|  |  |
| --- | --- |
| 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} |
|  | 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  -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(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** | |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |