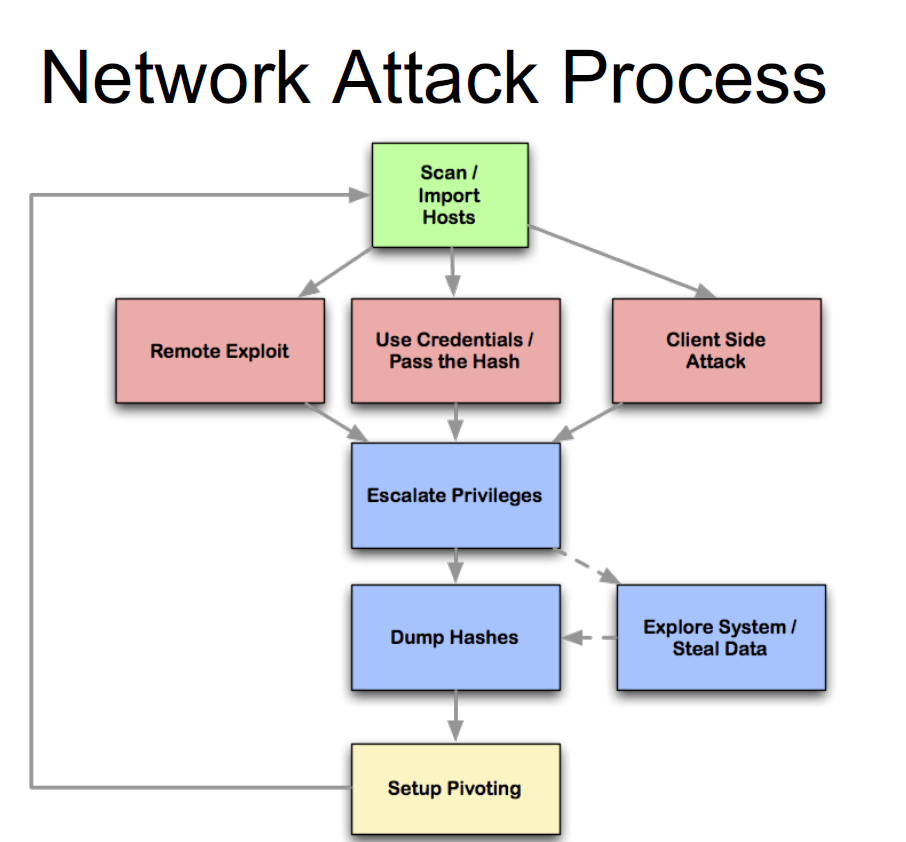
# 3809ICT Assignment

Step 1:- Network Exploration, as per the network attack process:



A broad scan

My IP: 192.168.34.4/24

The first step is to find all the live hosts within the range of 192.168.34.121 to 192.168.34.254

sudo nmap -sP -PI 192.168.34.0/24

|  |  |
| --- | --- |
| Operation | IP addresses |
| sudo nmap 192.168.34.0/24 -F | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243 |
| sudo nmap 192.168.34.0/24 -sV -O | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sP | 192.168.34.14  192.168.34.86  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sA | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sS | 192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sF | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sX | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sN | 192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -sT | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -PM | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
| sudo nmap 192.168.34.0/24 -PP | 192.168.34.14  192.168.34.86  192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243  192.168.34.4 |
|  |  |

|  |  |  |
| --- | --- | --- |
| My IP Address | Friendly IP Address | Target IP addresses |
| 192.168.34.4 | 192.168.34.14  192.168.34.86 | 192.168.34.145  192.168.34.188  192.168.34.209  192.168.34.237  192.168.34.243 |

Port Analysis of target IP Addresses:

|  |  |  |
| --- | --- | --- |
| Target IP addresses | Port Info | Traceroute |
| 192.168.34.145 | PORT STATE SERVICE VERSION  135/tcp open msrpc Microsoft Windows RPC  139/tcp open netbios-ssn Microsoft Windows netbios-ssn  445/tcp open microsoft-ds Mic192  2022/tcp open down?  MAC Address: 00:50:56:AE:07:8F (VMware)  Device type: firewall  Running (JUST GUESSING): Fortinet embedded (87%)  OS CPE: cpe:/h:fortinet:fortigate\_100d  Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)  No exact OS matches for host (test conditions non-ideal).  Network Distance: 1 hop  Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp | traceroute to 192.168.34.145 (192.168.34.145), 30 hops max, 60 byte packets  1 \* \* \*  2 192.168.34.145 (192.168.34.145) 0.313 ms 0.091 ms 0.086 ms |
| 192.168.34.188 | PORT STATE SERVICE VERSION  2022/tcp closed down  MAC Address: 00:50:56:AE:3B:13 (VMware)  Too many fingerprints match this host to give specific OS details  Network Distance: 1 hop  -----------------------------------------------------------------------------  2022/tcp closed down | traceroute to 192.168.34.188 (192.168.34.188), 30 hops max, 60 byte packets  1 \* \* \*  2 \* \* \*  3 \* \* \*  4 \* \* \*  5 \* \* \*  6 \* \* \*  7 \* \* \*  8 \* \* \*  9 \* \* \*  10 \* \* \*  11 \* \* \*  12 \* \* \*  13 \* \* \*  14 \* \* \*  15 \* \* \*  16 \* \* \*  17 \* \* \*  18 \* \* \*  19 \* \* \*  20 \* \* \*  21 \* \* \*  22 \* \* \*  23 \* \* \*  24 \* \* \*  25 \* \* \*  26 \* \* \*  27 \* \* \*  28 \* \* \*  29 \* \* \*  30 \* \* \* |
| 192.168.34.209 | PORT STATE SERVICE VERSION  80/tcp open http Apache httpd 2.4.18 ((Ubuntu))  MAC Address: 00:50:56:AE:85:98 (VMware)  Device type: general purpose  Running: Linux 3.X|4.X  OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4  OS details: Linux 3.2 - 4.9  Network Distance: 1 hop  -----------------------------------------------------------------------------  /tcp open|filtered http | traceroute to 192.168.34.209 (192.168.34.209), 30 hops max, 60 byte packets  1 192.168.34.209 (192.168.34.209) 0.271 ms 0.121 ms 0.103 ms |
| 192.168.34.237 | PORT STATE SERVICE VERSION  21/tcp open ftp ProFTPD 1.3.4c  22/tcp open ssh OpenSSH 8.4p1 Debian 5 (protocol 2.0)  53/tcp open domain ISC BIND 9.16.27 (Debian Linux)  80/tcp open http Apache httpd 2.4.10 ((Unix) OpenSSL/1.0.1i PHP/5.4.31 mod\_perl/2.0.8-dev Perl/v5.16.3)  443/tcp open ssl/https Apache/2.4.10 (Unix) OpenSSL/1.0.1i PHP/5.4.31 mod\_perl/2.0.8-dev Perl/v5.16.3  MAC Address: 00:50:56:AE:04:AC (VMware)  Device type: general purpose  Running: Linux 4.X|5.X  OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5  OS details: Linux 4.15 - 5.6  Network Distance: 1 hop  Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel  ----------------------------------------------------------------------------------  21/tcp open|filtered ftp  22/tcp open|filtered ssh  53/tcp open|filtered domain  80/tcp open|filtered http  443/tcp open|filtered https | traceroute to 192.168.34.237 (192.168.34.237), 30 hops max, 60 byte packets  1 192.168.34.237 (192.168.34.237) 0.358 ms 0.168 ms 0.104 ms |
| 192.168.34.243 | Nmap scan report for 192.168.34.243  Host is up (0.00029s latency).  Not shown: 999 filtered ports  PORT STATE SERVICE VERSION  9090/tcp closed zeus-admin  MAC Address: 00:50:56:AE:2F:07 (VMware)  Too many fingerprints match this host to give specific OS detailss  Network Distance: 1 hop | traceroute to 192.168.34.243 (192.168.34.243), 30 hops max, 60 byte packets  1 192.168.34.243 (192.168.34.243) 0.424 ms !X 0.365 ms !X 0.301 ms !X |

Port Information

|  |  |
| --- | --- |
| Port No. | Info  Service Name ------Port Number ------Transport Protocol ------Description ------Assignment Notes |
| 21 | ftp 21 tcp File Transfer Protocol [Control] Defined TXT keys: u=<username> p=<password> path=<path>  ftp 21 udp File Transfer Protocol [Control] Defined TXT keys: u=<username> p=<password> path=<path>  ftp 21 sctp FTP Defined TXT keys: u=<username> p=<password> path=<path> |
| 22 | ssh 22 tcp The Secure Shell (SSH) Protocol Defined TXT keys: u=<username> p=<password>  ssh 22 udp The Secure Shell (SSH) Protocol Defined TXT keys: u=<username> p=<password>  ssh 22 sctp SSH Defined TXT keys: u=<username> p=<password> |
| 53 | domain 53 udp Domain Name Server |
| 80 |  |
| 135 | epmap 135 tcp DCE endpoint resolution  epmap 135 udp DCE endpoint resolution |
| 139 | netbios-ssn 139 tcp NETBIOS Session Service  netbios-ssn 139 udp NETBIOS Session Service |
| 443 | https 443 tcp http protocol over TLS/SSL  https 443 udp http protocol over TLS/SSL  https 443 sctp HTTPS |
| 445 | microsoft-ds 445 tcp Microsoft-DS  microsoft-ds 445 udp Microsoft-DS |
| 2022 | down 2022 tcp  xinuexpansion2 2022 udp |
| 9090 | websm 9090 tcp WebSM  websm 9090 udp WebSM |

Vulnerability Exploration

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Command | Results | Comments |
| 192.168.34.243 | sudo nmap --script vuln <IP\_address> | $ sudo nmap --script vuln 192.168.34.188  [sudo] password for kali:  Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-17 00:21 AEST  Nmap scan report for 192.168.34.188  Host is up (0.00034s latency).  Not shown: 999 filtered ports  PORT STATE SERVICE  2022/tcp closed down  MAC Address: 00:50:56:AE:3B:13 (VMware)  Nmap done: 1 IP address (1 host up) scanned in 29.95 seconds |  |
| 192.168.34.237 | sudo nmap --script vuln <IP\_address> | sudo nmap --script vuln 192.168.34.209  [sudo] password for kali:  Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-17 00:21 AEST  Nmap scan report for 192.168.34.209  Host is up (0.000041s latency).  Not shown: 999 closed ports  PORT STATE SERVICE  80/tcp open http  http-csrf:  Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.34.209  Found the following possible CSRF vulnerabilities:    Path: http://192.168.34.209:80/  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/user/login  Form id: user-login-form  Form action: /user/login    Path: http://192.168.34.209:80/user/login  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node/help  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/user/register  Form id: user-register-form  Form action: /user/register    Path: http://192.168.34.209:80/user/register  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/user/password  Form id: user-pass  Form action: /user/password    Path: http://192.168.34.209:80/user/password  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/user/login  Form id: user-login-form  Form action: /user/login    Path: http://192.168.34.209:80/user/login  Form id: search-block-form  Form action: /search/node    Path: http://192.168.34.209:80/search/node/  Form id: search-form  Form action: /search/node/    Path: http://192.168.34.209:80/search/node/  Form id: search-block-form  \_ Form action: /search/node  \_http-dombased-xss: Couldn't find any DOM based XSS.  http-enum:  /rss.xml: RSS or Atom feed  /robots.txt: Robots file  /: Drupal version 8  /README.txt: Interesting, a readme.  \_ /contact/: Potentially interesting folder  http-fileupload-exploiter:    Failed to upload and execute a payload.    Failed to upload and execute a payload.    Failed to upload and execute a payload.    \_ Failed to upload and execute a payload.  http-slowloris-check:  VULNERABLE:  Slowloris DOS attack  State: LIKELY VULNERABLE  IDs: CVE:CVE-2007-6750  Slowloris tries to keep many connections to the target web server open and hold  them open as long as possible. It accomplishes this by opening connections to  the target web server and sending a partial request. By doing so, it starves  the http server's resources causing Denial Of Service.    Disclosure date: 2009-09-17  References:  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  \_ http://ha.ckers.org/slowloris/  \_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  MAC Address: 00:50:56:AE:85:98 (VMware)  Nmap done: 1 IP address (1 host up) scanned in 334.76 seconds |  |
| 192.168.34.145 | sudo nmap --script vuln <IP\_address> | ????$ sudo nmap --script vuln 192.168.34.145  [sudo] password for kali:  Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-17 00:22 AEST  Nmap scan report for 192.168.34.145  Host is up (0.000049s latency).  Not shown: 996 closed ports  PORT STATE SERVICE  135/tcp open msrpc  139/tcp open netbios-ssn  445/tcp open microsoft-ds  2022/tcp open down  MAC Address: 00:50:56:AE:07:8F (VMware)  Host script results:  \_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED  smb-vuln-ms08-067:  VULNERABLE:  Microsoft Windows system vulnerable to remote code execution (MS08-067)  State: VULNERABLE  IDs: CVE:CVE-2008-4250  The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,  Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary  code via a crafted RPC request that triggers the overflow during path canonicalization.    Disclosure date: 2008-10-23  References:  https://technet.microsoft.com/en-us/library/security/ms08-067.aspx  \_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250  \_smb-vuln-ms10-054: false  \_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)  smb-vuln-ms17-010:  VULNERABLE:  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)  State: VULNERABLE  IDs: CVE:  Risk factor: HIGH  A critical remote code execution vulnerability exists in Microsoft SMBv1  servers (ms17-010).    Disclosure date: 2017-03-14  References:  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx  \_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/    Nmap done: 1 IP address (1 host up) scanned in 53.25 seconds |  |
| 192.168.34.209 | sudo nmap --script vuln <IP\_address> | ????$ sudo nmap --script vuln 192.168.34.237  [sudo] password for kali:  Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-17 00:22 AEST  Nmap scan report for 192.168.34.237  Host is up (0.000084s latency).  Not shown: 995 closed ports  PORT STATE SERVICE  21/tcp open ftp  \_sslv2-drown:  22/tcp open ssh  53/tcp open domain  80/tcp open http  \_http-csrf: Couldn't find any CSRF vulnerabilities.  \_http-dombased-xss: Couldn't find any DOM based XSS.  http-enum:  /icons/: Potentially interesting folder w/ directory listing  \_ /img/: Potentially interesting folder w/ directory listing  \_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  \_http-trace: TRACE is enabled  443/tcp open https  \_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  \_http-csrf: Couldn't find any CSRF vulnerabilities.  \_http-dombased-xss: Couldn't find any DOM based XSS.  http-slowloris-check:  VULNERABLE:  Slowloris DOS attack  State: LIKELY VULNERABLE  IDs: CVE:CVE-2007-6750  Slowloris tries to keep many connections to the target web server open and hold  them open as long as possible. It accomplishes this by opening connections to  the target web server and sending a partial request. By doing so, it starves  the http server's resources causing Denial Of Service.    Disclosure date: 2009-09-17  References:  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  \_ http://ha.ckers.org/slowloris/  \_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  ssl-dh-params:  VULNERABLE:  Diffie-Hellman Key Exchange Insufficient Group Strength  State: VULNERABLE  Transport Layer Security (TLS) services that use Diffie-Hellman groups  of insufficient strength, especially those using one of a few commonly  shared groups, may be susceptible to passive eavesdropping attacks.  Check results:  WEAK DH GROUP 1  Cipher Suite: TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA  Modulus Type: Safe prime  Modulus Source: RFC2409/Oakley Group 2  Modulus Length: 1024  Generator Length: 8 Public Key Length: 1024  References:  \_ https://weakdh.org  ssl-poodle:  VULNERABLE:  SSL POODLE information leak  State: VULNERABLE  IDs: BID:70574 CVE:CVE-2014-3566  The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other  products, uses nondeterministic CBC padding, which makes it easier  for man-in-the-middle attackers to obtain cleartext data via a  padding-oracle attack, aka the "POODLE" issue.  Disclosure date: 2014-10-14  Check results:  TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA  References:  https://www.imperialviolet.org/2014/10/14/poodle.html  https://www.securityfocus.com/bid/70574  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566  \_ https://www.openssl.org/~bodo/ssl-poodle.pdf  \_sslv2-drown:  MAC Address: 00:50:56:AE:04:AC (VMware)  Nmap done: 1 IP address (1 host up) scanned in 57.20 seconds |  |
| 192.168.34.188 | sudo nmap --script vuln <IP\_address> | $ sudo nmap --script vuln 192.168.34.243  [sudo] password for kali:  Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-17 00:23 AEST  Nmap scan report for 192.168.34.243  Host is up (0.00029s latency).  Not shown: 999 filtered ports  PORT STATE SERVICE  9090/tcp closed zeus-admin  MAC Address: 00:50:56:AE:2F:07 (VMware)  Nmap done: 1 IP address (1 host up) scanned in 29.10 seconds |  |

Sources:

<https://www.youtube.com/watch?v=22ob1JjpzR4>

<https://www.youtube.com/watch?v=3U1pJ-eJrAU>

Scan for ports and weaknesses:

<https://linuxhint.com/nmap-port-scanning-security/>

Checkout:

<https://www.youtube.com/watch?v=qxbaBZxYygU>

<https://www.youtube.com/watch?v=6gHOUjpzesw>

SSL Analysis:

<https://www.youtube.com/watch?v=4VQH3Au5g-Q>

Downgrade attack:

<https://www.youtube.com/watch?v=iHiyYOxgisA>

Virtual Hosts:

<https://www.youtube.com/watch?v=fCN0QNZkYHM>

<https://systemweakness.com/metasploit-pivoting-to-hack-segregated-virtualbox-virtual-machines-b722213d667f>

Wireshark Config:

<https://www.youtube.com/watch?v=wJlIL3R9eO8>

Kali Linux tools - XSSER Cross-site scripting attack

<https://youtu.be/POLeVgtx0ps>

<https://www.facebook.com/CrewHackers00/videos/how-to-scan-variability-and-hack-website-with-xsser/1551766655143794/>

SSH Attack:

<https://www.youtube.com/watch?v=FKVsz_2IWJs>

<https://github.com/jeanphorn/wordlist>

Brute Force Attack:

<https://www.youtube.com/watch?v=FKVsz_2IWJs>

Default Gateway:

<https://www.youtube.com/watch?v=9YUv8aZiHK0>

Port 80:

Other:

<https://www.youtube.com/watch?v=8irLItrFNdM>