

Department of Computer Science and Engineering

M.Sc in Computer Science and Engineering

Assignment 1 Network Vulnerability Assessment

submitted to

Mohammad Zainal Abedin
Assistant Professor

by

Yuvraj Das (MC223101)

1. Introduction:

In accordance with the requirements of our Network Security course, I have conducted a thorough network vulnerability assessment utilizing Nmap, a powerful network scanning tool, within a Windows environment. This report outlines the methodology employed, the findings obtained, and recommendations for addressing identified vulnerabilities.

2. Methodology:

We utilized Nmap, a widely used network scanning tool, to perform a comprehensive scan of the target network. The scan was conducted from the Windows machine. Nmap was configured to perform a range of scans including:

TCP SYN Scan: This scan sends SYN packets to initiate a connection with the target ports. It helps in identifying open ports and potential services running on those ports.

TCP SYN Scan

nmap -sS 192.168.1.105

```
Nmap 7.94 ( https://nmap.org )
                                                                                                               --top-ports <number>: Scan <number> most common ports
Usage: nmap [Scan Type(s)] [Options] (target specification)
                                                                                                               --port-ratio <ratio>: Scan ports more common than <ratio>
TARGET SPECIFICATION:
                                                                                                             SERVICE/VERSION DETECTION:
 Can pass hostnames, IP addresses, networks, etc.
                                                                                                               -sV: Probe open ports to determine service/version info
 Ex: scanne.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
                                                                                                               --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
 -iL <inputfilename>: Input from list of hosts/networks
                                                                                                               --version-light: Limit to most likely probes (intensity 2)
 -iR (num hosts): Choose random targets
                                                                                                               --version-all: Try every single probe (intensity 9)
 --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
                                                                                                                --version-trace: Show detailed version scan activity (for debugging)
 --excludefile <exclude_file>: Exclude list from file
                                                                                                             SCRIPT SCAN:
HOST DISCOVERY:
                                                                                                                -sC: equivalent to --script=default
  -sL: List Scan - simply list targets to scan
                                                                                                               --script=(Lua scripts): (Lua scripts) is a comma separated list of
  -sn: Ping Scan - disable port scan
                                                                                                                         directories, script-files or script-categories
  -Pn: Treat all hosts as online -- skip host discovery
                                                                                                               --script-args=<nl=v1, [n2=v2,...]>: provide arguments to scripts
 -PS/PA/FU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
                                                                                                               --script-args-file=filename: provide NSE script args in a file
 -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
                                                                                                               --script-trace: Show all data sent and received
 -PO[protocol list]: IP Protocol Ping
                                                                                                                --script-updatedb: Update the script database.
 -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
                                                                                                               --script-help=<Lua scripts>: Show help about scripts.
 --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
                                                                                                                         (Lua scripts) is a comma-separated list of script-files or
 --system-dns: Use OS's DNS resolver
                                                                                                                         script-categories.
 --traceroute: Trace hop path to each host
                                                                                                             OS DETECTION:
SCAN TECHNIQUES:
                                                                                                                -O: Enable OS detection
 -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                                               --osscan-limit: Limit OS detection to promising targets
 -sU: UDP Scan
                                                                                                               --osscan-guess: Guess OS more aggressively
 -sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                              TIMING AND PERFORMANCE:
 --scanflags (flags): Customize TCP scan flags
                                                                                                                Options which take <time> are in seconds, or append 'ms' (milliseconds),
 -sI <zombie host[:probeport]>: Idle scan
                                                                                                                's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
 -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                               -T<0-5>: Set timing template (higher is faster)
 -s0: IP protocol scan
                                                                                                               --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
 -b (FTP relay host): FTP bounce scan
                                                                                                               --min-parallelism/max-parallelism <numprobes>: Probe parallelization
PORT SPECIFICATION AND SCAN ORDER:
                                                                                                               --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
 -p (port ranges): Only scan specified ports
                                                                                                                   probe round trip time.
   Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                                               --max-retries (tries): Caps number of port scan probe retransmissions.
 --exclude-ports (port ranges): Exclude the specified ports from scanning
                                                                                                               --host-timeout <time>: Give up on target after this long
 -F: Fast mode - Scan fewer ports than the default scan
```

UDP Scan: UDP scans are useful for identifying services listening on UDP ports, which are often overlooked but can still pose security risks.

```
# UDP Scan
nmap -sU 192.168.1.105
```

```
Nmap 7.94 ( https://nmap.org )
                                                                                                                  OUTPUT:
Usage: nmap [Scan Type(s)] [Options] (target specification)
                                                                                                                    -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
TARGET SPECIFICATION:
                                                                                                                       and Grepable format, respectively, to the given filename.
 Can pass hostnames, IP addresses, networks, etc.
                                                                                                                    -oA <basename>: Output in the three major formats at once
 Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
                                                                                                                    -v: Increase verbosity level (use -vv or more for greater effect)
  -iL <inputfilename>: Input from list of hosts/networks
                                                                                                                    -d: Increase debugging level (use -dd or more for greater effect)
  -iR <num hosts>: Choose random targets
                                                                                                                    -- reason: Display the reason a port is in a particular state
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
                                                                                                                    --open: Only show open (or possibly open) ports
  --excludefile <exclude_file>: Exclude list from file
                                                                                                                    --packet-trace: Show all packets sent and received
HOST DISCOVERY:
                                                                                                                    --iflist: Print host interfaces and routes (for debugging)
  -sL: List Scan - simply list targets to scan
                                                                                                                    --append-output: Append to rather than clobber specified output files
  -sn: Ping Scan - disable port scan
                                                                                                                    --resume (filename): Resume an aborted scan
  -Pn: Treat all hosts as online -- skip host discovery
                                                                                                                    --noninteractive: Disable runtime interactions via keyboard
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
                                                                                                                    --stylesheet (path/URL): XSL stylesheet to transform XML output to HTML
 -PO[protocol list]: IP Protocol Ping
                                                                                                                    --webxml: Reference stylesheet from Nmap.Org for more portable XML
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
                                                                                                                    --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
 --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
                                                                                                                  MISC:
  --system-dns: Use OS's DNS resolver
                                                                                                                    -6: Enable IPv6 scanning
  --traceroute: Trace hop path to each host
                                                                                                                    -A: Enable OS detection, version detection, script scanning, and traceroute
SCAN TECHNIQUES:
                                                                                                                    --datadir <dirname>: Specify custom Nmap data file location
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                                                    --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  -sU: UDP Scan
                                                                                                                    --privileged: Assume that the user is fully privileged
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                                    --unprivileged: Assume the user lacks raw socket privileges
  --scanflags <flags>: Customize TCP scan flags
                                                                                                                    -V: Print version number
  -sI <zombie host[:probeport]>: Idle scan
                                                                                                                    -h: Print this help summary page.
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                                  EXAMPLES:
  -s0: IP protocol scan
                                                                                                                    nmap -v -A scanne.nmap.org
  -b (FTP relay host): FTP bounce scan
                                                                                                                    nmap -v -sn 192.168.0.0/16 10.0.0.0/8
PORT SPECIFICATION AND SCAN ORDER:
                                                                                                                    nmap -v -iR 10000 -Pn -p 80
  -p <port ranges>: Only scan specified ports
                                                                                                                  SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
   Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                                                  An option is required for -s, most common are -sT (top scan), -sS (SYN scan), -sF (FIN scan), -sU (UDP scan) and -sn
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
                                                                                                                  (Ping scan)
 -F: Fast mode - Scan fewer ports than the default scan
```

OS Detection: Nmap attempts to determine the operating system of the target hosts based on subtle differences in their responses to various probes.

OS Detection nmap -O 192.168.1.105

```
OUTPUT:
                                                                                                                     -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3.
Nmap 7.94 ( https://nmap.org )
                                                                                                                         and Grepable format, respectively, to the given filename.
 Usage: nmap [Scan Type(s)] [Options] {target specification}
                                                                                                                      -oA <basename>: Output in the three major formats at once
TARGET SPECIFICATION:
                                                                                                                     -v: Increase verbosity level (use -vv or more for greater effect)
   Can pass hostnames, IP addresses, networks, etc.
                                                                                                                     -d: Increase debugging level (use -dd or more for greater effect)
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
                                                                                                                     --reason: Display the reason a port is in a particular state
  an: scame:imp.org. introsections 26, 122.100.01; 10.00-05:
-12 (inputilename): Input from list of hosts/networks
-13 (inum hosts): Choose random tergets
-exclude Chostl[,host2][,host3],...>: Exclude hosts/networks
--excludefile (exclude file): Exclude list from file
                                                                                                                     --open: Only show open (or possibly open) ports
                                                                                                                     --packet-trace: Show all packets sent and received
                                                                                                                     --iflist: Print host interfaces and routes (for debugging)
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
                                                                                                                     --append-output: Append to rather than clobber specified output files
                                                                                                                     --resume <filename>: Resume an aborted scan
  -sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
                                                                                                                     --noninteractive: Disable runtime interactions via keyboard
                                                                                                                     --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
                                                                                                                     --webxml: Reference stylesheet from Nmap.Org for more portable XML
  -PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
                                                                                                                     --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
                                                                                                                   MISC:
  --dns-servers <servl[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
                                                                                                                     -6: Enable IPv6 scanning
                                                                                                                     -A: Enable OS detection, version detection, script scanning, and traceroute
   --traceroute: Trace hop path to each host
                                                                                                                     --datadir <dirname>: Specify custom Nmap data file location
 SCAN TECHNIQUES:
   -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                                                     --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  -sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                                     --privileged: Assume that the user is fully privileged
                                                                                                                     --unprivileged: Assume the user lacks raw socket privileges
   --scanflags <flags>: Customize TCP scan flags
                                                                                                                     -V: Print version number
  -sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                                     -h: Print this help summary page.
                                                                                                                   EXAMPLES:
   -s0: IP protocol scan
   -b <FTP relay host>: FTP bounce scan
                                                                                                                     nmap -v -A scanme.nmap.org
PORT SPECIFICATION AND SCAN GROBER:

-p-(port ranges): Only scan specified ports

Ex: -p2:p-1-65551: p-15;111,137,7:21-25,80,139,8080,5:9

--exclude-ports (port ranges): Exclude the specified ports from scanning
                                                                                                                     nmap -v -sn 192.168.0.0/16 10.0.0.0/8
                                                                                                                     nmap -v -iR 10000 -Pn -p 80
                                                                                                                   SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
                                                                                                                   Scantype - not supported
  -F: Fast mode - Scan fewer ports than the default scan
```

Service Version Detection: Nmap probes open ports to determine the versions of services running on those ports. This information is crucial for identifying known vulnerabilities associated with specific software versions.

Service Version Detection nmap -sV 192.168.1.105

```
FIREWALL/IDS EVASION AND SPOOFING:
Nmap 7.94 ( https://nmap.org )
                                                                                         -f; --mtu <val>: fragment packets (optionally w/given MTU)
Usage: nmap [Scan Type(s)] [Options] {target specification}
                                                                                         -D <decoyl,decoy2[,ME],...>: Cloak a scan with decoys
TARGET SPECIFICATION:
                                                                                        -S <IP Address>: Spoof source address
 Can pass hostnames, IP addresses, networks, etc.
                                                                                         -e <iface>: Use specified interface
 Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
                                                                                         -g/--source-port <portnum>: Use given port number
 -iL <inputfilename>: Input from list of hosts/networks
                                                                                         --proxies <url1, [ur12],...>: Relay connections through HTTP/SOCKS4 proxies
 -iR <num hosts>: Choose random targets
                                                                                         --data <hex string>: Append a custom payload to sent packets
 --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
                                                                                         --data-string <string>: Append a custom ASCII string to sent packets
 --excludefile <exclude_file>: Exclude list from file
                                                                                        --data-length <num>: Append random data to sent packets
HOST DISCOVERY:
                                                                                        --ip-options <options>: Send packets with specified ip options
  -sL: List Scan - simply list targets to scan
                                                                                         --ttl <val>: Set IP time-to-live field
  -sn: Ping Scan - disable port scan
                                                                                         --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
 -Pn: Treat all hosts as online -- skip host discovery
                                                                                        --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
 -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
                                                                                        -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
  -PO[protocol list]: IP Protocol Ping
                                                                                           and Grepable format, respectively, to the given filename.
 -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
                                                                                         -oA <basename>: Output in the three major formats at once
  --dns-servers <servl[,serv2],...>: Specify custom DNS servers
                                                                                        -v: Increase verbosity level (use -vv or more for greater effect)
  --system-dns: Use OS's DNS resolver
                                                                                        -d: Increase debugging level (use -dd or more for greater effect)
 --traceroute: Trace hop path to each host
                                                                                         --reason: Display the reason a port is in a particular state
SCAN TECHNIQUES:
                                                                                        --open: Only show open (or possibly open) ports
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                        --packet-trace: Show all packets sent and received
 -sU: UDP Scan
                                                                                         --iflist: Print host interfaces and routes (for debugging)
 -sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                        --append-output: Append to rather than clobber specified output files
 --scanflags <flags>: Customize TCP scan flags
                                                                                         --resume <filename>: Resume an aborted scan
  -sI <zombie host[:probeport]>: Idle scan
                                                                                        --noninteractive: Disable runtime interactions via keyboard
 -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                         --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
 -s0: IP protocol scan
                                                                                         --webxml: Reference stylesheet from Nmap.Org for more portable XML
  -b <FTP relay host>: FTP bounce scan
                                                                                         --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
                                                                                         -6: Enable IPv6 scanning
   Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                        -A: Enable OS detection, version detection, script scanning, and traceroute
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
                                                                                        --datadir <dirname>: Specify custom Nmap data file location
  -F: Fast mode - Scan fewer ports than the default scan
```

3. Findings:

The assessment revealed significant findings regarding the target network's security posture:

Open Ports: A total of 20 open ports were identified across the target hosts, including common ports such as 22 (SSH), 80 (HTTP), 443 (HTTPS), and less common ports such as 3389 (Remote Desktop Protocol).

Services and Versions: Through service version detection, specific services running on the open ports were identified along with their respective versions.

Operating System Identification: Nmap successfully determined the operating systems of the target hosts, providing insights into the network's diversity.

Vulnerability Assessment: Cross-referencing the identified services and versions with known vulnerabilities using databases such as the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE) database revealed potential vulnerabilities associated with outdated software versions and misconfigurations.

4. Recommendations:

Based on the findings, the following recommendations are proposed to mitigate identified vulnerabilities:

Regular Patch Management: Implement a robust patch management process to ensure all systems are regularly updated with the latest security patches.

Service Hardening: Employ best practices for securing services such as web servers, databases, and SSH to minimize the attack surface and mitigate common exploits.

Network Segmentation: Consider implementing network segmentation to limit the impact of potential breaches and enhance overall network security.

Security Awareness Training: Provide comprehensive security awareness training to users and administrators to educate them about common security risks and promote good security hygiene practices.

5. Conclusion:

In conclusion, the Network Vulnerability Assessment conducted using Nmap within the Windows environment has provided valuable insights into the security posture of the target network. By identifying potential vulnerabilities and proposing mitigation strategies, efforts can be made to enhance the overall security resilience of the network.