Department of Computer Science and Engineering International Islamic University Chittagong

M.Sc in Computer Science and Engineering



Assignment 1 Network Vulnerability Assessment

submitted to

Mohammad Zainal Abedin
Assistant Professor

by

Redoan Ahmed (MC223107)

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 192.168.1.100

```
probe round trip time.
Nmap 7.94 ( https://nmap.org )
                                                                                                     --max-retries <tries>: Caps number of port scan probe retransmissions.
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
                                                                                                     --host-timeout (time): Give up on target after this long
 Can pass hostnames, IP addresses, networks, etc.
                                                                                                     --scan-delay/--max-scan-delay <time>: Adjust delay between probes
 Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
                                                                                                       --min-rate <number>: Send packets no slower than <number> per second
 -iL <inputfilename>: Input from list of hosts/networks
                                                                                                       --max-rate <number>: Send packets no faster than <number> per second
 -iR <num hosts>: Choose random targets
                                                                                                   FIREWALL/IDS EVASION AND SPOOFING:
 --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
                                                                                                      -f; --mtu <val>: fragment packets (optionally w/given MTU)
 --excludefile <exclude file>: Exclude list from file
                                                                                                       -D <decoyl,decoy2[,ME],...>: Cloak a scan with decoys
HOST DISCOVERY:
                                                                                                       -S <IP Address>: Spoof source address
 -sL: List Scan - simply list targets to scan
                                                                                                        -e <iface>: Use specified interface
 -sn: Ping Scan - disable port scan
                                                                                                       -g/--source-port <portnum): Use given port number
  -Pn: Treat all hosts as online -- skip host discovery
 -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
                                                                                                      --proxies <url1, [url2],...>: Relay connections through HTTP/SOCKS4 proxies
 -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
                                                                                                     --data <hex string>: Append a custom payload to sent packets
 -PO[protocol list]: IP Protocol Ping
                                                                                                       --data-string <string>: Append a custom ASCII string to sent packets
 -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
                                                                                                       --data-length <num>: Append random data to sent packets
 --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
                                                                                                       --ip-options <options>: Send packets with specified ip options
 --system-dns: Use OS's DNS resolver
                                                                                                      --ttl <val>: Set IP time-to-live field
  --traceroute: Trace hop path to each host
                                                                                                        --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
SCAN TECHNIQUES:
                                                                                                        --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
 -sU: UDP Scan
                                                                                                       -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
 -sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                          and Grepable format, respectively, to the given filename.
  --scanflags <flags>: Customize TCP scan flags
 -sI <zombie host[:probeport]>: Idle scan
                                                                                                       -oA (basename): Output in the three major formats at once
 -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                       -v: Increase verbosity level (use -vv or more for greater effect)
 -s0: IP protocol scan
                                                                                                        -d: Increase debugging level (use -dd or more for greater effect)
 -b <FTP relay host>: FTP bounce scan
                                                                                                       --reason: Display the reason a port is in a particular state
PORT SPECIFICATION AND SCAN ORDER:
                                                                                                       --open: Only show open (or possibly open) ports
  -p (port ranges): Only scan specified ports
                                                                                                       --packet-trace: Show all packets sent and received
   Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                                        --iflist: Print host interfaces and routes (for debugging)
 --exclude-ports (port ranges): Exclude the specified ports from scanning
                                                                                                        --append-output: Append to rather than clobber specified output files
 -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 192.168.1.100
```

```
Nmap 7.94 ( https://nmap.org )
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
                                                                                                                  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  -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
                                                                                                                   --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <servl[,serv2],...>: Specify custom DNS servers
                                                                                                                  -6: Enable IPv6 scanning
  --system-dns: Use OS's DNS resolver
                                                                                                                   -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:
                                                                                                                   --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                                                  --privileged: Assume that the user is fully privileged
  -sU: UDP Scan
                                                                                                                   --unprivileged: Assume the user lacks raw socket privileges
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                                  -V: Print version number
  --scanflags <flags>: Customize TCP scan flags
                                                                                                                  -h: Print this help summary page.
  -sI <zombie host[:probeport]>: Idle scan
                                                                                                                EXAMPLES:
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                                  nmap -v -A scanme.nmap.org
  -s0: IP protocol scan
                                                                                                                  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  -b <FTP relay host>: FTP bounce scan
                                                                                                                  nmap -v -iR 10000 -Pn -p 80
PORT SPECIFICATION AND SCAN ORDER:
                                                                                                                 SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
  -p <port ranges>: Only scan specified ports
                                                                                                                An option is required for -s, most common are -sT (tcp scan), -sS (SYN scan), -sF (FIN scan), -sU (UDF scan) and -sn
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                                                (Ping scan)
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -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 192.168.1.100

```
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
                                                                                                                                     -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.
                                                                                                                                         and Grepable format, respectively, to the given filename.
                                                                                                                                      -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 -iL <inputfilename>: Input from list of hosts/networks
                                                                                                                                     -v: Increase verbosity level (use -vv or more for greater effect)
                                                                                                                                     -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
--excludefile <exclude file>: Exclude list from file
                                                                                                                                      --open: Only show open (or possibly open) ports
                                                                                                                                      --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
  -sn: Ping Scan - disable port scan
                                                                                                                                      --append-output: Append to rather than clobber specified output files
  -Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
                                                                                                                                     --resume <filename>: Resume an aborted scan
                                                                                                                                     --noninteractive: Disable runtime interactions via keyboard
  -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 <servl[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
                                                                                                                                  MISC:
                                                                                                                                     -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
-sN/sF/sX: TCP Null, FIN, and Xmas scans
                                                                                                                                     --privileged: Assume that the user is fully privileged
   --scanflags <flags>: Customize TCP scan flags
                                                                                                                                      --unprivileged: Assume the user lacks raw socket privileges
  -sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                                                                     -V: Print version number
                                                                                                                                      -h: Print this help summary page.
  -s0: IP protocol scan
                                                                                                                                  EXAMPLES:
  -b <FTP relay host>: FTP bounce scan
                                                                                                                                     nmap -v -A scanme.nmap.or
PORT SPECIFICATION AND SCAN ORDER:
                                                                                                                                     nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  -p <pr
                                                                                                                                     nmap -v -iR 10000 -Pn -p 80
                                                                                                                                  SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
   --exclude-ports <port ranges>: Exclude the specified ports from scanning
                                                                                                                                  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 192.168.1.100

```
Nmap 7.94 ( https://nmap.org )
                                                                                   FIREWALL/IDS EVASION AND SPOOFING:
NMap 7.94 { https://mmap.ozy /
<u>Usage:</u> nmap [Scan Type(s)] [Options] {target specification}
                                                                                     -f; --mtu <val>: fragment packets (optionally w/given MTU)
TARGET SPECIFICATION:
                                                                                      -D <decoyl,decoy2[,ME],...>: Cloak a scan with decoys
                                                                                -S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
  Can pass hostnames, IP addresses, networks, etc.
 Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
                                                                                -g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <nex string>: Append a custom payload to sent packets
 -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
                                                                                      --data-string <string>: Append a custom ASCII string to sent packets
  -sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
                                                                                      --data-length <num>: Append random data to sent packets
                                                                                      --ip-options <options>: Send packets with specified ip options
  -Pn: Treat all hosts as online -- skip host discovery
                                                                                     --ttl <val>: Set IP time-to-live field
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
                                                                                    --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
                                                                                      --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
                                                                                       -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
  --system-dns: Use OS's DNS resolver
                                                                                         and Grepable format, respectively, to the given filename.
  --traceroute: Trace hop path to each host
                                                                                       -oA <basename>: Output in the three major formats at once
SCAN TECHNIQUES:
                                                                                      -v: Increase verbosity level (use -vv or more for greater effect)
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
                                                                                      -d: Increase debugging level (use -dd or more for greater effect)
  -sU: UDP Scan
                                                                                      --reason: Display the reason a port is in a particular state
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
                                                                                      --open: Only show open (or possibly open) ports
  -sI <zombie host[:probeport]>: Idle scan
                                                                                      --packet-trace: Show all packets sent and received
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
                                                                                      --iflist: Print host interfaces and routes (for debugging)
  -s0: IP protocol scan
                                                                                      --append-output: Append to rather than clobber specified output files
  -b <FTP relay host>: FTP bounce scan
                                                                                      --resume <filename>: Resume an aborted scan
PORT SPECIFICATION AND SCAN ORDER:
                                                                                      --noninteractive: Disable runtime interactions via keyboard
  -p <port ranges>: Only scan specified ports
   Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
                                                                                      --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
                                                                                      --webxml: Reference stylesheet from Nmap.Org for more portable XML
   -exclude-ports <port ranges>: Exclude the specified ports from scanning
 -F: Fast mode - Scan fewer ports than the default scan
                                                                                      --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

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.

6. References:

- Nmap Documentation: https://nmap.org/book/
- National Vulnerability Database (NVD): https://nvd.nist.gov/
- Common Vulnerabilities and Exposures (CVE) Database: https://cve.mitre.org/