

CompTIA Network+ Exam N10-008

Lesson 19



Applying Network Hardening Techniques

Objectives

- Compare and contrast types of attacks
- Apply network hardening techniques

Lesson 19

Topic 19A

Compare and Contrast Types of Attacks

General Attack Types

- Understanding attacker types and their motivations
- Footprinting and fingerprinting
 - Discover how the network and its security systems are configured
- Spoofing
 - Any type of attack where the attacker disguises his or her identity
- Denial of Service Attacks
 - Any attack that causes a service to become unavailable to users
 - May be purely destructive or may allow attacker to spoof the legitimate service

On-path Attacks

- Threat actor intercepts communication path
 - “Man-in-the-Middle (MitM)”
- MAC spoofing and IP spoofing
 - Arbitrarily change address value in packet
- ARP spoofing
 - Broadcast unsolicited/gratuitous ARP replies
 - Masquerade as MAC address of default gateway
- Rogue DHCP
 - Configure clients with malicious default gateway/DNS server IP

No.	Time	Source	Destination	Protocol	Length	Info
6	10.022521400	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.102 is at 00:15:5d:01:ca:76
7	10.032593900	Microsof_01:ca:4a	Microsof_01:ca:77	ARP	42	10.1.0.2 is at 00:15:5d:01:ca:77
8	10.032605300	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.101 is at 00:15:5d:01:ca:76
9	18.219200600	10.1.0.101	10.1.0.2	TCP	66	1702 → 80 [SYN] Seq=0 win=65535
10	18.220473400	10.1.0.101	10.1.0.2	TCP	66	[TCP Out-Of-Order] 1702 → 80
11	18.223616200	10.1.0.2	10.1.0.101	TCP	66	80 → 1702 [SYN, ACK] Seq=0 Ack=1702
12	18.228456800	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 80 → 1702
13	18.228797700	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1702
14	18.229264100	10.1.0.101	10.1.0.2	HTTP	433	GET / HTTP/1.1
15	18.238162600	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1702
16	18.238250400	10.1.0.101	10.1.0.2	TCP	433	[TCP Retransmission] 1702 → 80
17	18.239342200	10.1.0.2	10.1.0.101	HTTP	412	HTTP/1.1 302 Redirect (text/html)
18	18.244530700	10.1.0.2	10.1.0.101	TCP	412	[TCP Retransmission] 80 → 1702
19	18.245021200	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=380 Ack=1702
20	18.252481800	10.1.0.101	10.1.0.2	TCP	54	[TCP Dup ACK 19#1] 1702 → 80
21	18.255190400	10.1.0.101	10.1.0.2	TCP	66	1703 → 443 [SYN] Seq=0 win=0
22	18.260503200	10.1.0.101	10.1.0.2	TCP	66	[TCP Retransmission] 1703 → 443
23	18.261065300	10.1.0.2	10.1.0.101	TCP	66	443 → 1703 [SYN, ACK] Seq=0 Ack=1703
24	18.268454300	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 443 → 1703

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microsof_01:ca:77 (00:15:5d:01:ca:77), Dst: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
Destination: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
Source: Microsof_01:ca:77 (00:15:5d:01:ca:77)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2
Transmission Control Protocol, Src Port: 1702, Dst Port: 80, Seq: 0, Len: 0

```
0000 00 15 5d 01 ca 4a 00 15 5d 01 ca 77 08 00 45 00  ..J...].w..E.
0010 00 34 1c ca 40 00 80 06 c9 91 0a 01 00 65 0a 01  .4.@.....e..
0020 00 02 06 a5 00 50 dc 52 ee 41 00 00 00 00 80 02  ....P.R.A.....
0030 ff ff 89 1d 00 00 02 04 05 b4 01 03 03 08 01 01  ....
0040 04 02 ..
```

Destination Hardware Address (eth.dst), 6 bytes Packets: 286 · Displayed: 286 (100.0%) Profile: Default

DNS Poisoning Attacks

- Spoofing trusted hosts/sites (pharming)
- Denial of Service (DoS)
- Client-side attacks
 - Change/intercept resolver traffic
 - Modify HOSTS
- Server-side attacks
 - Hack server and change name records
 - Pollute server cache

```
HOSTNAME www.web.local yes Hostname to hijack
INTERFACE no The name of the interface
NEWADDR 192.168.2.192 yes New address for hostname
RECONS 192.168.2.254 yes The nameserver used for reconnaissance
RHOST 192.168.1.1 yes The target address
SNAPLEN 65535 yes The number of bytes to capture
SRCADDR Real yes The source address to use for sending t
he queries (Accepted: Real, Random)
SRCPORT 0 yes The target server's source query port (
0 for automatic)
TIMEOUT 500 yes The number of seconds to wait for new d
ata
TTL 46348 yes The TTL for the malicious host entry
XIDS 0 yes The number of XIDS to try for each quer
y (0 for automatic)

msf auxiliary(bailliwicked_host) > run

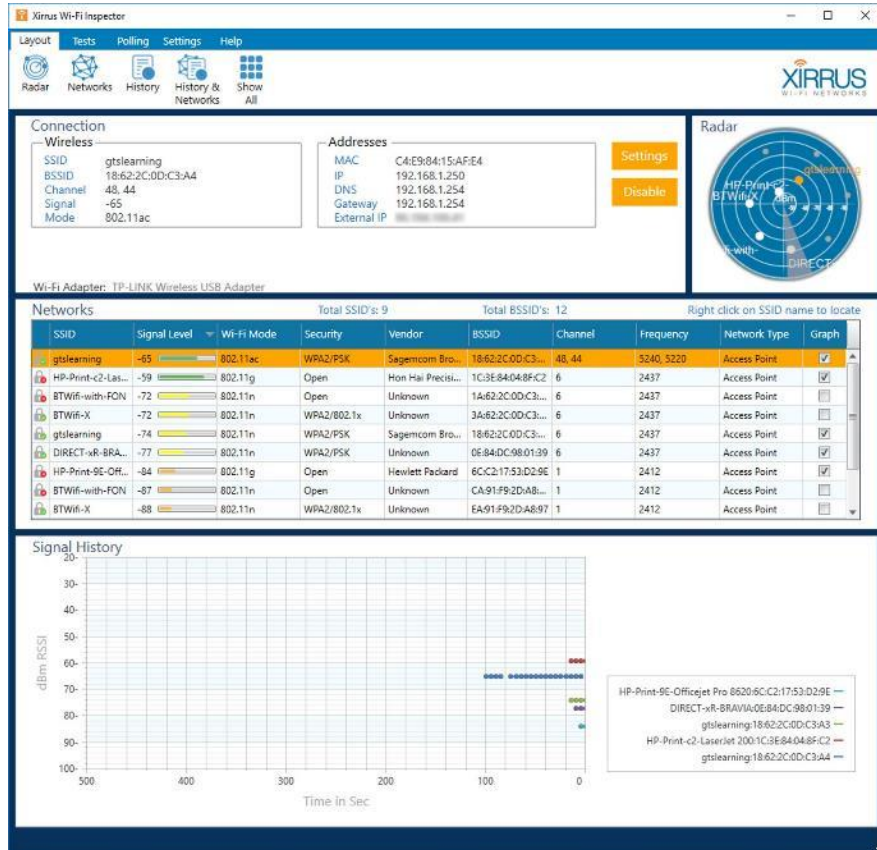
[-] Failure: This hostname is already in the target cache: www.web.local
[-] Cache entry expires on 2017-09-17 09:08:17 -0700... sleeping.
^C[-] Auxiliary interrupted by the console user
[*] Auxiliary module execution completed
msf auxiliary(bailliwicked_host) > set hostname updates.web.local
hostname => updates.web.local
msf auxiliary(bailliwicked_host) > run

[*] Targeting nameserver 192.168.1.1 for injection of updates.web.local. as 192.
168.2.192
[*] Querying recon nameserver for web.local.'s nameservers...
[*] Got an NS record: web.local. 604800 IN NS ns.web.lo
cal.
[*] Querying recon nameserver for address of ns.web.local....
[*] Got an A record: ns.web.local. 604800 IN A 192.168.
1.1
[*] Checking Authoritativeness: Querying 192.168.1.1 for web.local....
[*] ns.web.local. is authoritative for web.local., adding to list of nameser
vers to spoof as
[*] Calculating the number of spoofed replies to send per query...
[*] race calc: 100 queries | min/max/avg time: 0.0/0.0/0.0 | min/max/avg repli
es: 0/1/0
[*] The server did not reply, giving up.
[*] Auxiliary module execution completed
msf auxiliary(bailliwicked_host) > |
```

VLAN Hopping Attacks

- Send traffic to VLAN that would not normally be accessible
 - Double tag exploit against weakly configured native VLANs
 - Masquerade as trunk

Wireless Network Attacks



- Rogue access points
 - Potential backdoor
 - Risks from shadow IT
- Evil twins
 - Spoofs SSID and BSSID (MAC) of legitimate AP
- Deauthentication attacks
 - Cause client(s) to disconnect from AP

Distributed DoS Attacks and Botnets

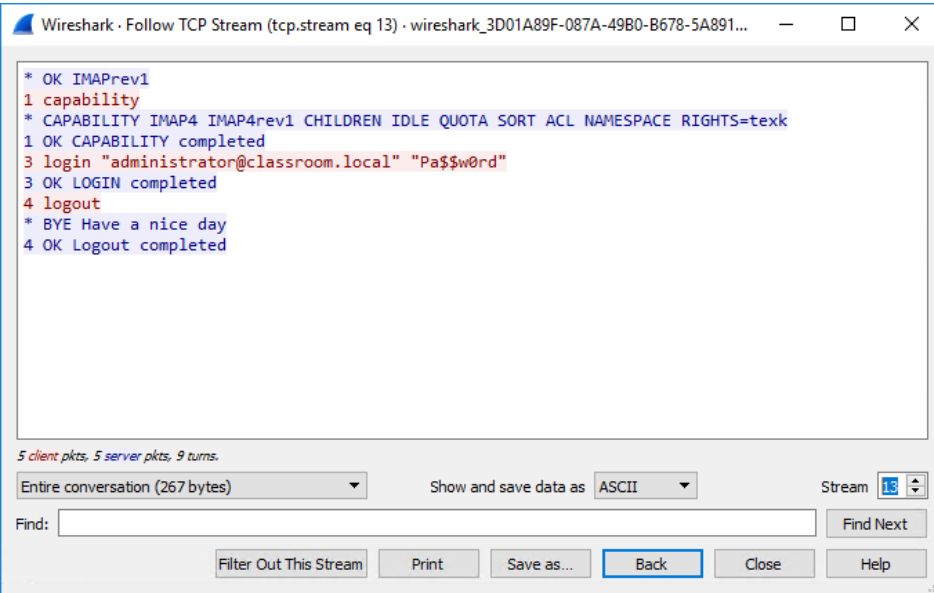
- Co-ordinated attacks launched by multiple hosts simultaneously
 - Overwhelm bandwidth
 - Overwhelm processing resource (flood state table)
- Distributed reflection DoS
 - Amplification attack
 - Spoof victim IP to overwhelm it with responses
- Botnets
 - Group of compromised hosts used to perpetrate DDoS/DRDoS)
 - Handler/herders versus bots
 - Command and control (C&C/C2) network

Malware and Ransomware Attacks

- Malware classification by vector
 - Viruses and worms
 - Trojan
 - Potentially unwanted programs (PUPs)/Potentially unwanted applications (PUAs)
- Malware classification by payload
 - Spyware, rootkit, remote access Trojan (RAT), ransomware, ...
- Ransomware
 - Spoof shell/dialogs/notifications
 - Crypto-malware



Password Attacks



The image shows a Wireshark window titled "Wireshark · Follow TCP Stream (tcp.stream eq 13) · wireshark_3D01A89F-087A-49B0-B678-5A891...". The main pane displays the following IMAP session transcript:

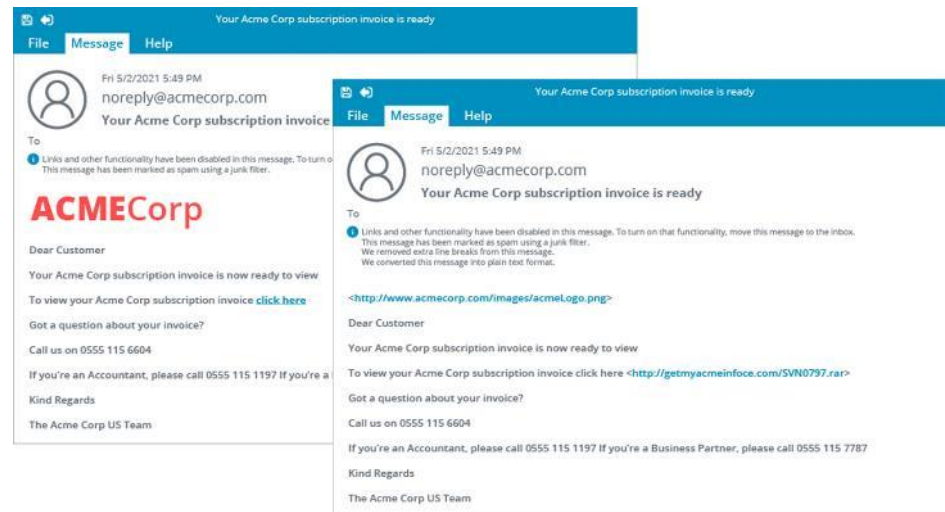
```
* OK IMAPrev1
1 capability
* CAPABILITY IMAP4 IMAP4rev1 CHILDREN IDLE QUOTA SORT ACL NAMESPACE RIGHTS=texk
1 OK CAPABILITY completed
3 login "administrator@classroom.local" "Pa$$w0rd"
3 OK LOGIN completed
4 logout
* BYE Have a nice day
4 OK Logout completed
```

Below the transcript, it says "5 client pkts, 5 server pkts, 9 turns." The "Show and save data as" dropdown is set to "ASCII". The "Stream" dropdown is set to "13". The "Find:" field is empty. At the bottom, there are buttons for "Filter Out This Stream", "Print", "Save as...", "Back", "Close", and "Help".

- Password capture
 - Plaintext storage and transmission
 - Password hashes
- Password hash cracking
 - Dictionary
 - Brute force
- Protecting password hashes

Human and Environmental Attacks


- Social engineering or hacking the human
 - Reasons for effectiveness
- Phishing
 - Social engineering over email
 - Also uses spoofed resource (website)
- Shoulder surfing
 - Observing password/PIN entry
- Tailgating and piggybacking
 - Gaining unauthorized entry to premises



Review Activity: Types of Attacks

- Footprinting, Spoofing, and Denial of Service Attacks
- On-path Attacks
- DNS Poisoning Attacks
- VLAN Hopping Attacks
- Wireless Network Attacks
- Distributed DoS Attacks and Botnets
- Malware and Ransomware Attacks
- Password Attacks
- Human and Environmental Attacks

Assisted Lab: Analyze an On-path Attack

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

Lesson 19

Topic 19B

Apply Network Hardening Techniques

Device and Service Hardening

- Hardening means applying a secure configuration to each network host or appliance
 - Change default passwords
 - Enforce password complexity/length requirements
 - Configure role-based access
 - Disable unneeded network services
 - Disable unsecure protocols

Endpoint Security and Switchport Protection

- Disable unneeded switchports
 - Restrict physical access/unplug patch cord
 - Administratively disable port
 - Assign to black hole VLAN
- Configure protection mechanisms
 - MAC Filtering and Dynamic ARP Inspection
 - DHCP Snooping
 - Neighbor Discovery (ND) Inspection and Router Advertisement (RA) Guard
 - Port Security (IEEE 802.1X Port-Based Network Access Control)

```
NYCORE1>
NYCORE1#
*Mar  1 00:02:27.991: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 00:02:46.287: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
NYCORE1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
NYCORE1(config)#ip arp inspection vlan 1,999
NYCORE1(config)#
*Mar  1 00:07:20.561: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/23, vlan 1.([0023.049
0.0000/192.168.16.21/00:07:20 UTC Mon Mar  1 1993])
```

VLAN and PVLAN Best Practices

- Private VLAN (PVLAN)
 - Further segment traffic within host/primary VLAN
 - Promiscuous, isolated, and community ports
- Default VLAN and native VLAN
 - VLAN ID 1 is default VLAN
 - Native VLAN contains untagged traffic on trunks
 - Native VLAN is also VLAN 1 by default
 - Change to unique value on both ends of trunk

Firewall Rules and ACL Configuration

Firewall: Rules: WAN

Select category ▾ Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
								Automatically generated rules	
	IPv4 *	<bogons>	*	*	*	*	*	Block bogon IPv4 networks from WAN	
	IPv6 *	<bogonsv6>	*	*	*	*	*	Block bogon IPv6 networks from WAN	
	IPv4 *	10.0.0.0/8,127.0.0.0/8,100.64.0.0/10,172.16.0.0/12,192.168.0.0/16	*	*	*	*	*	Block private networks from WAN	
	IPv6 *	fd0c::7	*	*	*	*	*	Block private networks from WAN	
	IPv4 ICMP	*	*	This Firewall	*	*	*	Allow ping to firewall interface	
	IPv4 TCP	*	*	SCREENED net	80 (HTTP)	*	*	Allow web access (unencrypted)	
	IPv4 TCP	MAILHOSTS	*	SCREENED net	25 (SMTP)	*	*	Allow SMTP access from secure mail gateway	
pass		block	reject		log		in	first match	
pass (disabled)		block (disabled)	reject (disabled)		log (disabled)		out	last match	
Active/Inactive Schedule (click to view/edit)									
Alias (click to view/edit)									

- Network access control list (ACL)
 - Top-to-bottom
 - Default block (implicit deny)
 - Explicit deny
 - Tuples
- iptables
 - Chains (INPUT, OUTPUT, and FORWARD)
 - Stateful rules

Control Plane Policing

- Control, data, and management planes
- Control and management require CPU resource
- Control and management must always be kept “open”
 - Sufficient bandwidth
 - Sufficient processing resource
- Control plane policing policy
 - Mitigate route processor vulnerabilities
 - ACL-based filters
 - Rate-limiting

Wireless Security

- Preshared keys (PSKs)
- Extensible Authentication Protocol
- Captive portal
- MAC filtering
- Geofencing
- Antenna placement and power levels
- Wireless client isolation
- Guest network isolation

IoT Access Considerations

- Audits to prevent use of shadow IT
- Secure administration interfaces
- Include IoT in patch and vulnerability management
- Isolate management and monitoring traffic for embedded systems
- Audit supplier security policies and procedures regularly


Patch and Firmware Management

- Monitor security and patch advisories
- Appliance firmware updates versus OS patches
- Firmware upgrade procedure
- Downgrading/rollback firmware
 - Configuration backup

Review Activity: Network Hardening Techniques

- Device and Service Hardening
- Endpoint Security and Switchport Protection
- VLAN and PVLAN Best Practices
- Firewall Rules and ACL Configuration
- Control Plane Policing
- Wireless Security
- IoT Access Considerations
- Patch and Firmware Management

Assisted Lab: Configure Port Security

- Lab types
 - Assisted labs guide you step-by-step through tasks
 - Applied labs set goals with limited guidance
- Complete lab
 - Submit all items for grading and check each progress box
 - Select “Grade Lab” from final page
- Save lab 
 - Select the hamburger menu and select “Save”
 - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
 - Select the hamburger menu and select “End”

CompTIA Network+ Exam N10-008

Lesson 19



Summary