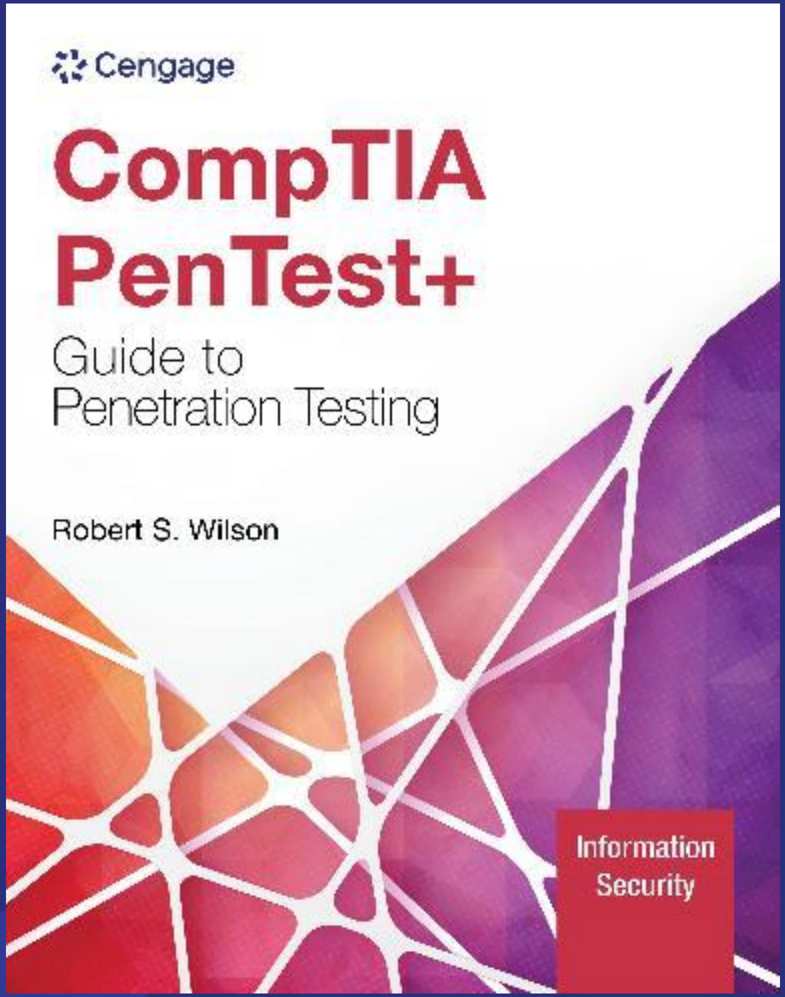


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 8: Wireless and Specialized Systems Attack Vectors and Attacks

Module Objectives (1 of 2)

By the end of this module, you should be able to:

1. Describe wireless attacks and attack vectors
2. Describe specialized systems attacks and attack vectors
3. Explain wireless network components, architecture, authentication, and encryption
4. Describe Radio-Frequency Identification (RFID) and Near Field Communication (NFC)
5. Explain how to acquire wireless hacking targets
6. Describe wardriving

Module Objectives (2 of 2)

By the end of this module, you should be able to:

7. Explain the tools and methods used to compromise WPS, WEP, WPA, WPA2, and WPA3 wireless security protocols
8. Describe the tools and methods used to compromise Bluetooth, RFID, and NFC technologies
9. Describe specialized systems and their vulnerabilities and attack vectors
10. Describe mobile device vulnerabilities and attack vectors

Wireless Attacks and Attack Vectors (1 of 29)

Understanding Wireless Networks

- Wireless generally refers to equipment and technologies using radio frequency (RF) between 3Hz and 300 GHz
- Many different types of wireless technologies and devices use them
  - Laptops
  - IoT devices
  - Cellular/Smartphones
  - Wireless network devices
  - Radar systems
  - AM/FM radios
- Wireless networking predominantly operates in 2.4GHz to 66GHz range
- Wireless networks are subject to as many attacks as wired networks
- Additional attack vectors and methods exist and are unique to wireless

Wireless Attacks and Attack Vectors (2 of 29)

Understanding Wireless Networks

Access Points (AP) / Wireless Access Point (WAP)

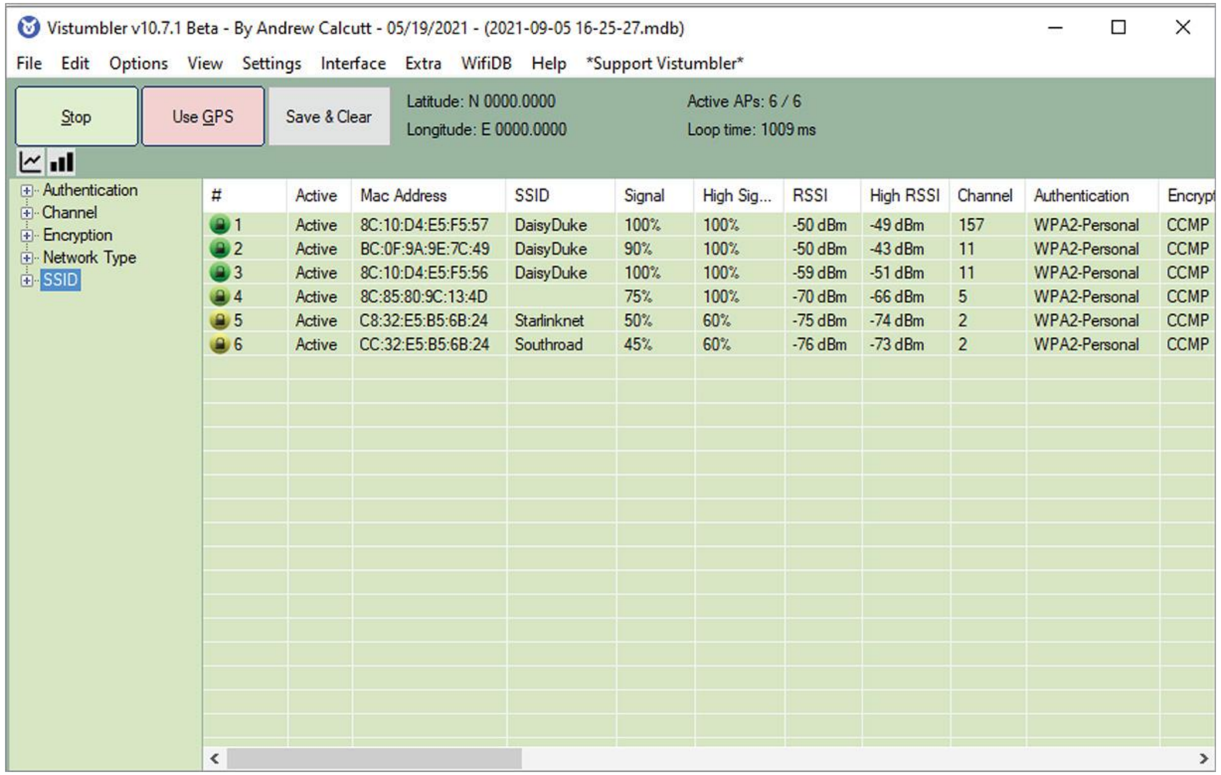
- Radio transceiver that connects to a wired network and bridges a wireless LAN (WLAN) with a wired network
- An AP is configured to use specific RF channels, or dedicated RF ranges, for wireless hosts to communicate with
- Wireless network interface cards (WNICs) transmit and receive wireless signals to APs

Wireless Attacks and Attack Vectors (3 of 29)

Understanding Wireless Networks

- Many tools exist to provide reconnaissance and enumeration of wireless APs

- Some tools provide detailed information about the security, channel and radio frequencies used, and even signal and noise measurements



Latitude: N 0000.0000
Longitude: E 0000.0000

Active APs: 6 / 6
Loop time: 1009 ms

#	Active	Mac Address	SSID	Signal	High Sig...	RSSI	High RSSI	Channel	Authentication	Encrypt
1	Active	8C:10:D4:E5:F5:57	DaisyDuke	100%	100%	-50 dBm	-49 dBm	157	WPA2-Personal	CCMP
2	Active	BC:0F:9A:9E:7C:49	DaisyDuke	90%	100%	-50 dBm	-43 dBm	11	WPA2-Personal	CCMP
3	Active	8C:10:D4:E5:F5:56	DaisyDuke	100%	100%	-59 dBm	-51 dBm	11	WPA2-Personal	CCMP
4	Active	8C:85:80:9C:13:4D		75%	100%	-70 dBm	-66 dBm	5	WPA2-Personal	CCMP
5	Active	C8:32:E5:B5:6B:24	Starlinknet	50%	60%	-75 dBm	-74 dBm	2	WPA2-Personal	CCMP
6	Active	CC:32:E5:B5:6B:24	Southroad	45%	60%	-76 dBm	-73 dBm	2	WPA2-Personal	CCMP

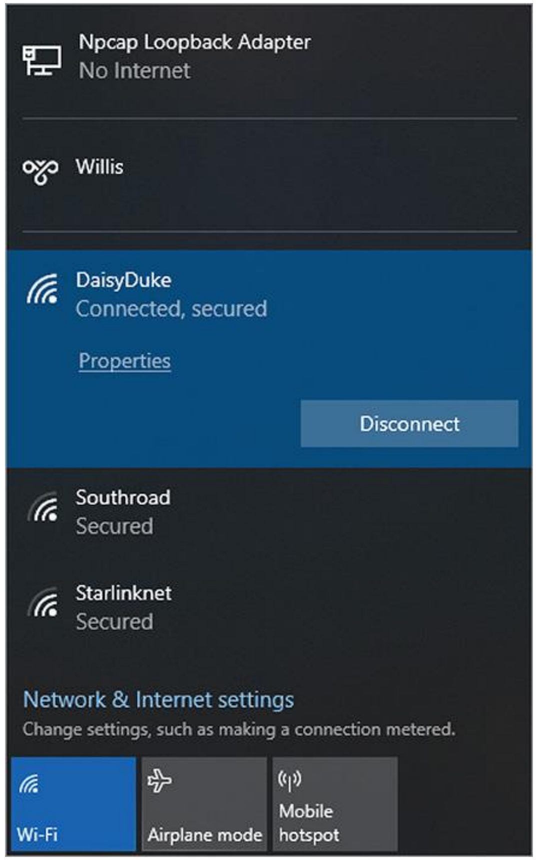
AP channels detected

Wireless Attacks and Attack Vectors (4 of 29)

Understanding Wireless Networks

Service Set Identifiers (SSID)

- A SSID is a name used to identify a WLAN
- Configured on APs as 1 - 32-character, case-sensitive alphanumeric name
- An AP will broadcast the SSID rapidly for potential wireless clients
- SSID broadcast and other types of Wi-Fi frames are unencrypted
- APs with default SSIDs may indicate default security



Npcap Loopback Adapter
No Internet

Willis

DaisyDuke
Connected, secured

Southroad
Secured

Starlinknet
Secured

Network & Internet settings
Change settings, such as making a connection metered.

SSIDs advertised to a Windows computer

Wireless Attacks and Attack Vectors (5 of 29)

Understanding Wireless Networks

Wireless NICs

- Systems wanting Wi-Fi access must have appropriate wireless NIC
- Many types exists, but must have right NIC to use latest Wi-Fi standards
- Specific models of wireless NICs better for security tools and testing use

The 802.11 Wireless Network Standard

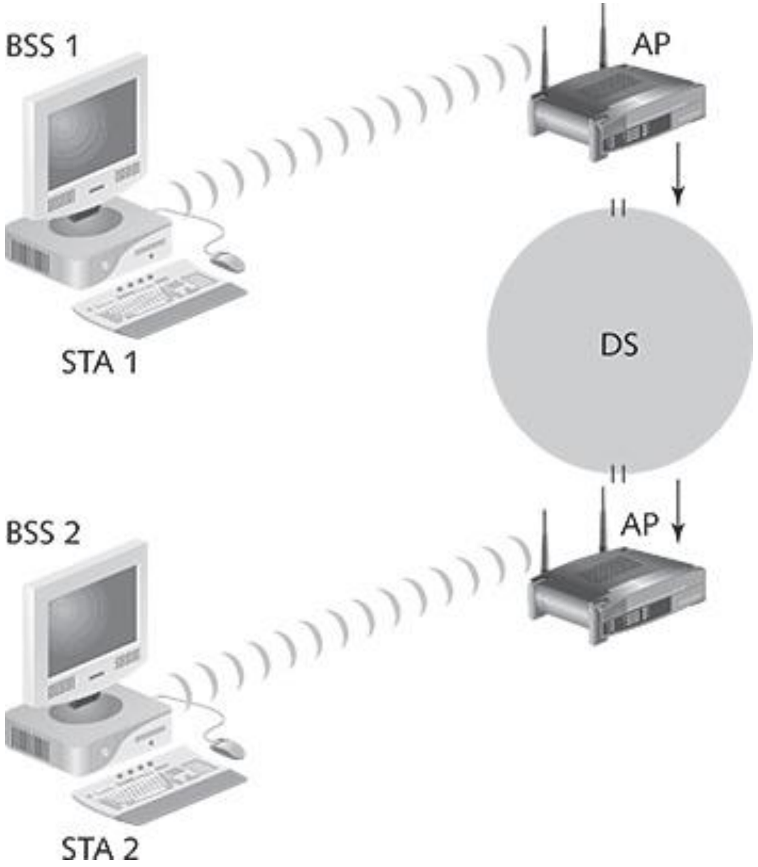
- IEEE created 802.11 family for wireless LAN standardization
- There are many specifications, varying underlying technologies, ranges, speeds, frequencies used, etc.

Wireless Attacks and Attack Vectors (6 of 29)

Understanding Wireless Networks

Basic Architecture of 802.11

- Basic service set (BSS) is collection of devices that make up a WLAN
- Devices within a BSS can communicate with other devices in same BSS
- Two BSSs connected requires distributed service set (DSS)



Connecting two wireless remote stations

Wireless Attacks and Attack Vectors (7 of 29)

Understanding Authentication

Authentication and security of wireless LANs present challenges not present in traditional wireless networks. Several standards and security frameworks have evolved to address this challenge:

The 802.1X Standard

- Defines process of authenticating and authorizing users on network
- Both wired and wireless networks can employ 802.1X

Point-to-Point Protocol (PPP)

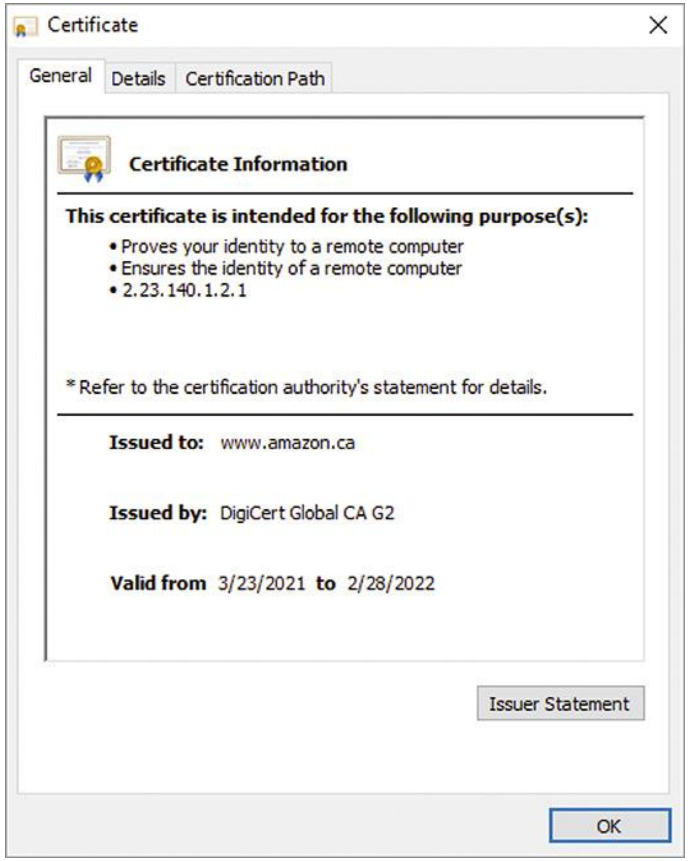
- Simple protocol authenticates users by username and password

Wireless Attacks and Attack Vectors (8 of 29)

Understanding Authentication

Extensible Authentication Protocol (EAP)

- Enhancement to PPP; allows selection of authentication method like Kerberos or digital certificates
- EAP offers methods to improve WLAN security
  - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  - Protected EAP (PEAP)
  - Microsoft PEAP



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

Issued to: www.amazon.ca

Issued by: DigiCert Global CA G2

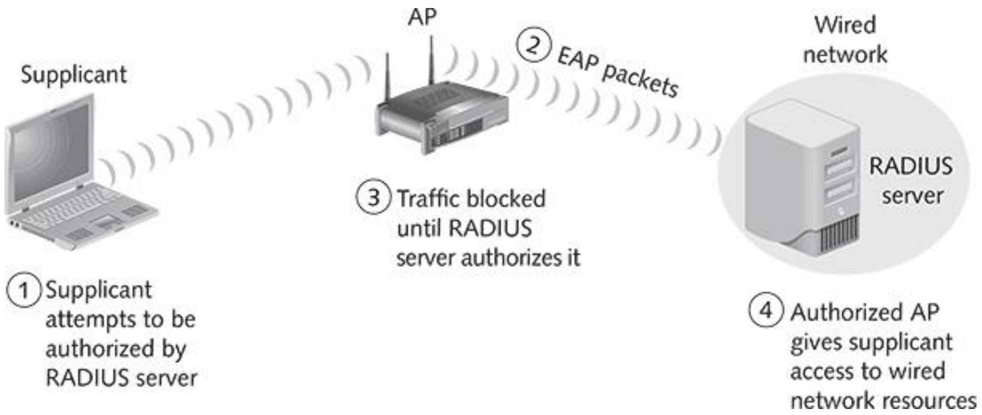
Valid from 3/23/2021 **to** 2/28/2022

Viewing information about an x.509 certificate

Wireless Attacks and Attack Vectors (9 of 29)

Understanding Authentication

- 802.1X uses following components to function:
  - Supplicant – wireless user seeking WLAN access
  - Authenticator – AP functions as entity allowing or denying supplicant access
  - Authentication Server – central component that authenticates and provides accounting functions
    - Commonly RADIUS


Supplicant
AP
② EAP packets
Wired network
RADIUS server
③ Traffic blocked until RADIUS server authorizes it
① Supplicant attempts to be authorized by RADIUS server
④ Authorized AP gives supplicant access to wired network resources

A supplicant connecting to an AP and a RADIUS server

Wireless Attacks and Attack Vectors (10 of 29)

Understanding Authentication

- Before 802.1x and EAP, Wi-Fi authentication was per device, not per user
- Wired Equivalent Privacy (WEP) is part of 802.11b standard to provide encryption for wireless network traffic
- WEP was soon plagued by serious security flaws, rendering encryption cracking within reach of attackers of varying skill levels
- Most well-known WEP flaw related to attacking encryption key through an initialization vector; short 24-bit string
- Wi-Fi Protected Access (WPA, WPA2, and WPA3) specified in 802.11i; greatly improved replacements for WEP

Wireless Attacks and Attack Vectors (11 of 29)

Understanding Authentication

- Wi-Fi Protected Setup (WPS) is another wireless authentication standard rendered insecure by security flaws
- WPS intent is to allow for easy connection by client device to AP
- Major vulnerability allows gaining access to WLAN without password

Wireless Attacks and Attack Vectors (12 of 29)

Understanding Authentication

Bluetooth

- IEEE 802.15 addresses wireless personal area network (WPAN)
- Various versions exist; newer providing better performance and security
- Version 5 uses 2.4 GHz for speeds up to 48 Mbps and 300 m distance

Radio-Frequency Identification (RFID)

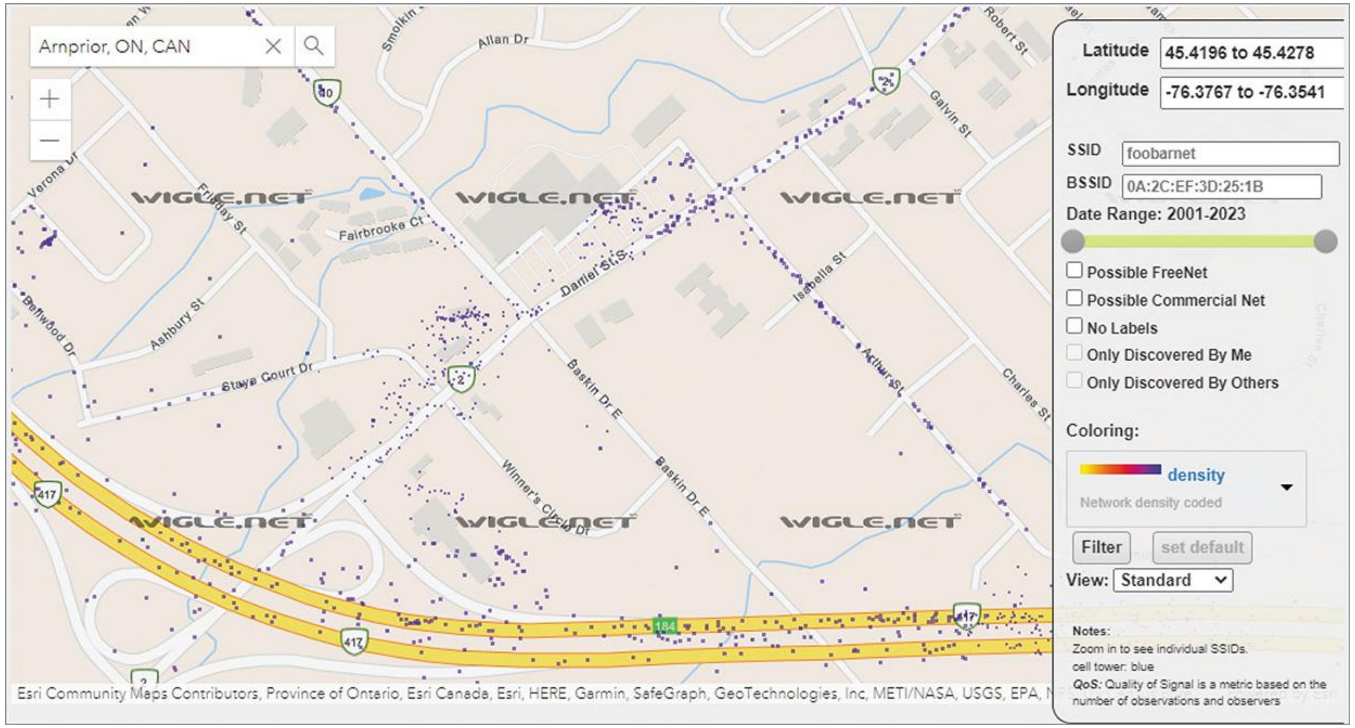
- Uses electromagnetic fields to identify and track objects with RFID “tags”
- Commonly used for employee badges, asset tagging, and pet tagging

Wireless Attacks and Attack Vectors (13 of 29)

Finding Targets

Understanding Wardriving

- Locating common starting point of access points
- Wardriving – act of scanning for wireless access points using tools that often map the location of discovered APs via GPS and map tools
- Smartphone app WiGLE is capable of this recon



Latitude 45.4196 to 45.4278
Longitude -76.3767 to -76.3541
SSID foobarnet
BSSID 0A:2C:EF:3D:25:1B
Date Range: 2001-2023

☐ Possible FreeNet
☐ Possible Commercial Net
☐ No Labels
☐ Only Discovered By Me
☐ Only Discovered By Others

Coloring: density
Network density coded

Filter set default

View: Standard

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Esri Community Maps Contributors, Province of Ontario, Esri Canada, Esri, HERE, Garmin, SafeGraph, GeoTechnologies, Inc, METI/NASA, USGS, EPA,

WiGLE Wi-Fi Map

Wireless Attacks and Attack Vectors (14 of 29)

Finding Targets

Understanding Wardriving

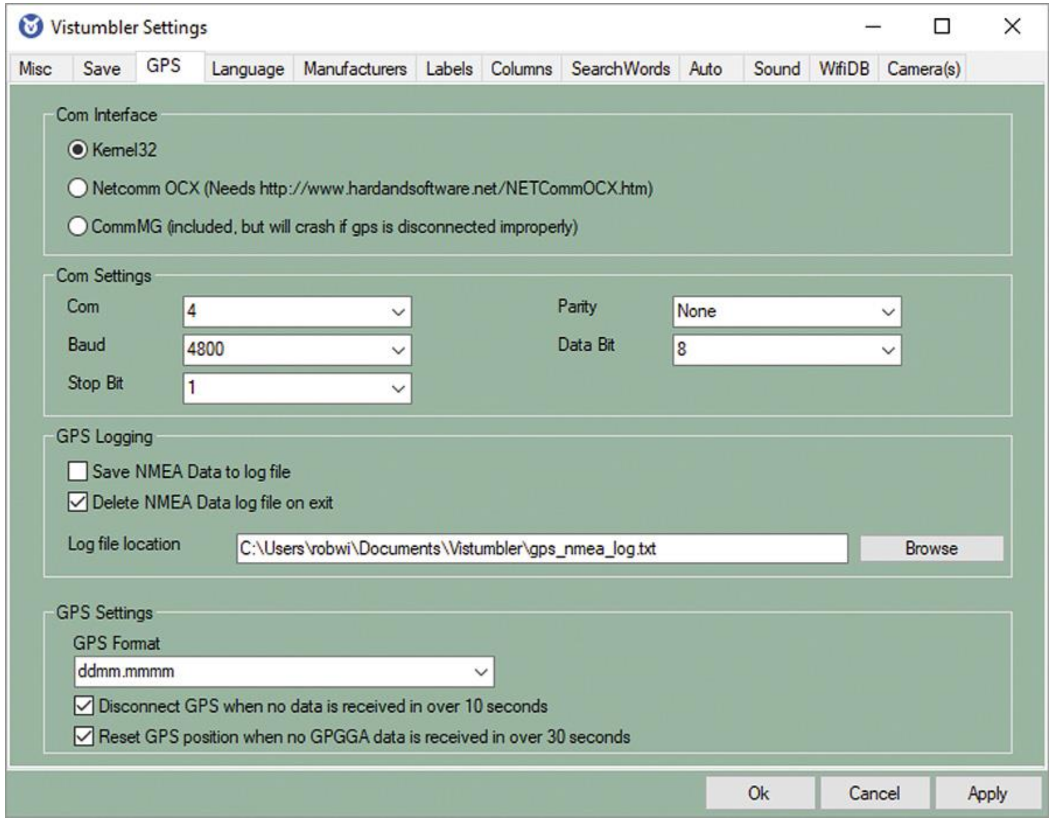
- Wardriving (or biking, or walking, or flying) can discover APs with lax security or no authentication and encryption protocols
- Wardriving is not illegal; using networks without authorizations likely is
- Certain wireless NICs perform better or are more compatible with tools
- Wardriving can determine security parameters and RF channels APs use

Wireless Attacks and Attack Vectors (15 of 29)

Finding Targets

Understanding Wardriving

- Vistumbler is one of several tools for wardriving or WLAN discovery
- Can interact with GPS to log location of APs and plot details on map
- Logs SSID, MAC of AP, manufacture, RF channel in use, signal strength, and encryption



Com Interface

● Kernel32

○ Netcomm OCX (Needs http://www.hardandsoftware.net/NETCommOCX.htm)

○ CommMG (included, but will crash if gps is disconnected improperly)

Com Settings

Com: 4

Baud: 4800

Stop Bit: 1

Parity: None

Data Bit: 8

GPS Logging

☐ Save NMEA Data to log file

☑ Delete NMEA Data log file on exit

Log file location: C:\Users\robwi\Documents\Vistumbler\gps_nmea_log.txt

GPS Settings

GPS Format: ddmm.mmmm

☑ Disconnect GPS when no data is received in over 10 seconds

☑ Reset GPS position when no GPGGA data is received in over 30 seconds

Configuring GPS settings in the Vistumbler Settings dialog box

Wireless Attacks and Attack Vectors (16 of 29)

Attack Methods

1. Eavesdropping – capturing data in transit using sniffer tools
2. Data modification attack – changing captured data like in MITM attack
3. Data corruption attack – corrupting WLAN traffic to enable other attacks, such as deauthentication attacks, knocking client offline
4. Relay attack – using intercepted wireless traffic, possibly analyzing and modifying before sending to intended destination
5. Spoofing Attacks – provide false protocol address or responses to allow attacker to impersonate a host

Wireless Attacks and Attack Vectors (17 of 29)

Attack Methods

6. Deauthentication attack – sending spoofed packets to attempt forcing targets to disconnect from an AP, allowing for follow up attacks
7. Jamming – denial-of-service attack to prevent legitimate wireless traffic due to RF spectrum overload of target or communicating AP
8. Capturing handshake messages - capturing traffic between hosts and APs; attackers can attempt to decrypt or attack via other methods
9. On-path attacks – attempting to trick target into sending traffic through malicious system controlled by threat actor

Wireless Attacks and Attack Vectors (18 of 29)

Eavesdropping, Rogues, Evil Twins, and Wireless On-Path Attacks

Eavesdropping

- The nature of wireless networks makes them inherently vulnerable to eavesdropping
- Eavesdropping requires that WNIC supports “monitor mode”
- WNIC supporting “packet injection” also required for other Wi-Fi attacks discussed later
- Eavesdropping is often precursor to follow-up attacks

Wireless Attacks and Attack Vectors (19 of 29)

Eavesdropping, Rogues, Evil Twins, and Wireless On-Path Attacks

Rogue Access Points

- Rogue AP is set up and connected to public or private network without authorization to do so
- Attacker who connects rogue AP hopes users will connect to it
- Eavesdropping, credential harvesting, and MITM attacks are then more likely to occur
- Users rather than attackers can install a rogue AP for reasons other than attacks
    - Internal user may setup own AP to bypass legitimate AP security

Wireless Attacks and Attack Vectors (20 of 29)

Eavesdropping, Rogues, Evil Twins, and Wireless On-Path Attacks

Evil Twin Access Point

- Evil twin AP is rogue AP masquerading as legitimate AP
- Typically uses same SSID as authorized APs of organization
- Users connecting can be subject to similar exploits as rogue AP
- New tools and techniques can protect organizations from evil twin AP

Downgrade Attacks

- Attacker controlled AP can initiate downgrade attack on target AP user
- Can direct user to use weaker security protocols than expected

Discussion Activity 8-1

Wireless 802.11-based LANs are subject to a variety of attacks that exploit the ease at which an access point can be provisioned and deployed by an attacker.

Discuss the differences in effect of attack for a rogue access point, evil twin access point, and downgrade attacks.

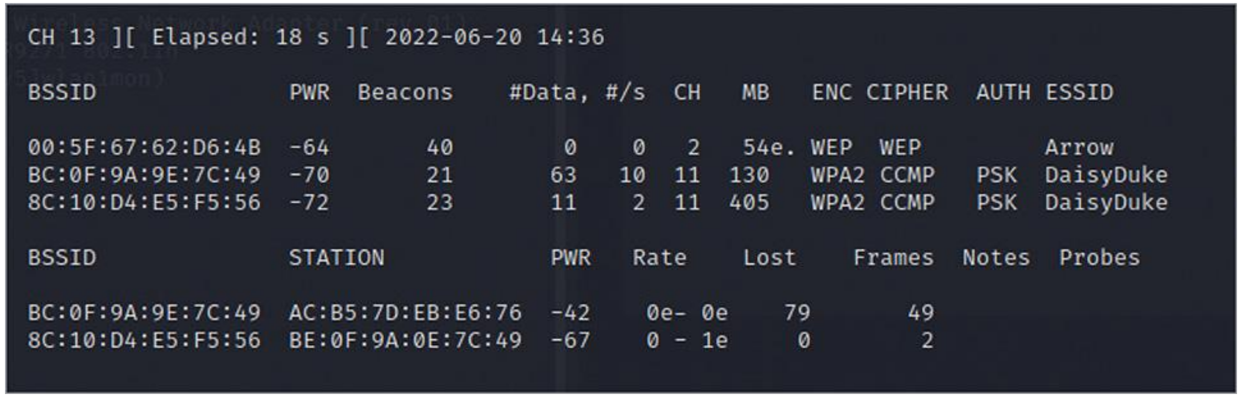
What are the intended results for each? Would these attacks be detectable by vigilant blue team members? Why or why not?

Wireless Attacks and Attack Vectors (21 of 29)

Attacking WEP and WPS

Attacking WEP

- Cracking WEP typically involves capturing and then analyzing traffic
- Using “packet injection” can speed up process but is more detectable
- Airodump-ng one of several Wi-Fi attack and observation tools
- Successful attack reveals WEP key and grants network access



```
CH 13 ][ Elapsed: 18 s ][ 2022-06-20 14:36

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:5F:67:62:D6:4B  -64       40        0    0   2   54e. WEP  WEP         Arrow
BC:0F:9A:9E:7C:49  -70       21       63   10  11  130   WPA2 CCMP   PSK  DaisyDuke
8C:10:D4:E5:F5:56  -72       23       11    2  11  405   WPA2 CCMP   PSK  DaisyDuke

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

BC:0F:9A:9E:7C:49  AC:B5:7D:EB:E6:76  -42    0e- 0e    79       49
8C:10:D4:E5:F5:56  BE:0F:9A:0E:7C:49  -67    0 - 1e     0        2
```

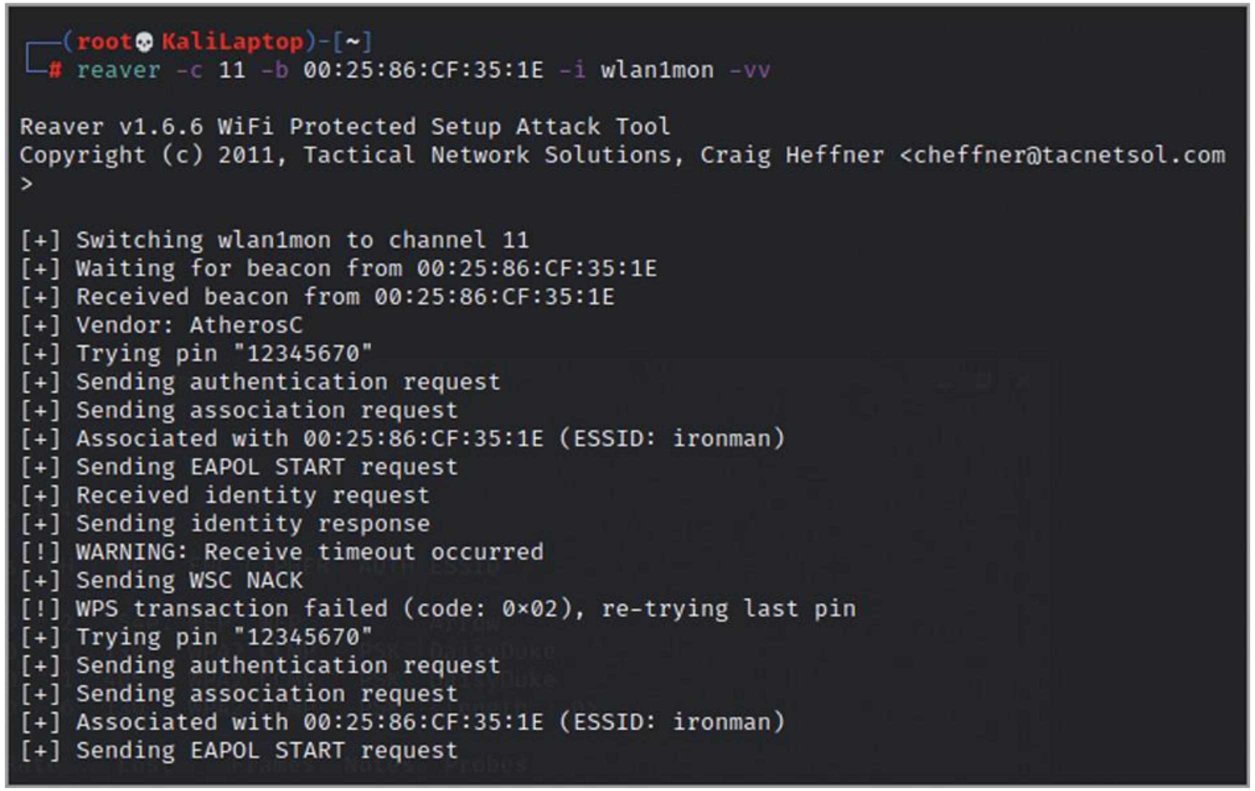
airodump-ng AP list

Wireless Attacks and Attack Vectors (22 of 29)

Attacking WEP and WPS

Attacking WPS

- WPS employs two four-digit PINs to make establishing connection easy
- These short PINs can be cracked relatively easily within a few hours using brute force attacks
- Several utilities exist in Kali and separately for attacking WPS



```
┌──(root💀KaliLaptop)-[~]
└─# reaver -c 11 -b 00:25:86:CF:35:1E -i wlan1mon -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com
>

[+] Switching wlan1mon to channel 11
[+] Waiting for beacon from 00:25:86:CF:35:1E
[+] Received beacon from 00:25:86:CF:35:1E
[+] Vendor: AtherosC
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 00:25:86:CF:35:1E (ESSID: ironman)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0×02), re-trying last pin
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 00:25:86:CF:35:1E (ESSID: ironman)
[+] Sending EAPOL START request
```

Using Reaver to brute force WPS

Wireless Attacks and Attack Vectors (23 of 29)

Attacking WPA, WPA2, and WPA3

Cracking WPA/WPA2 with Brute Force

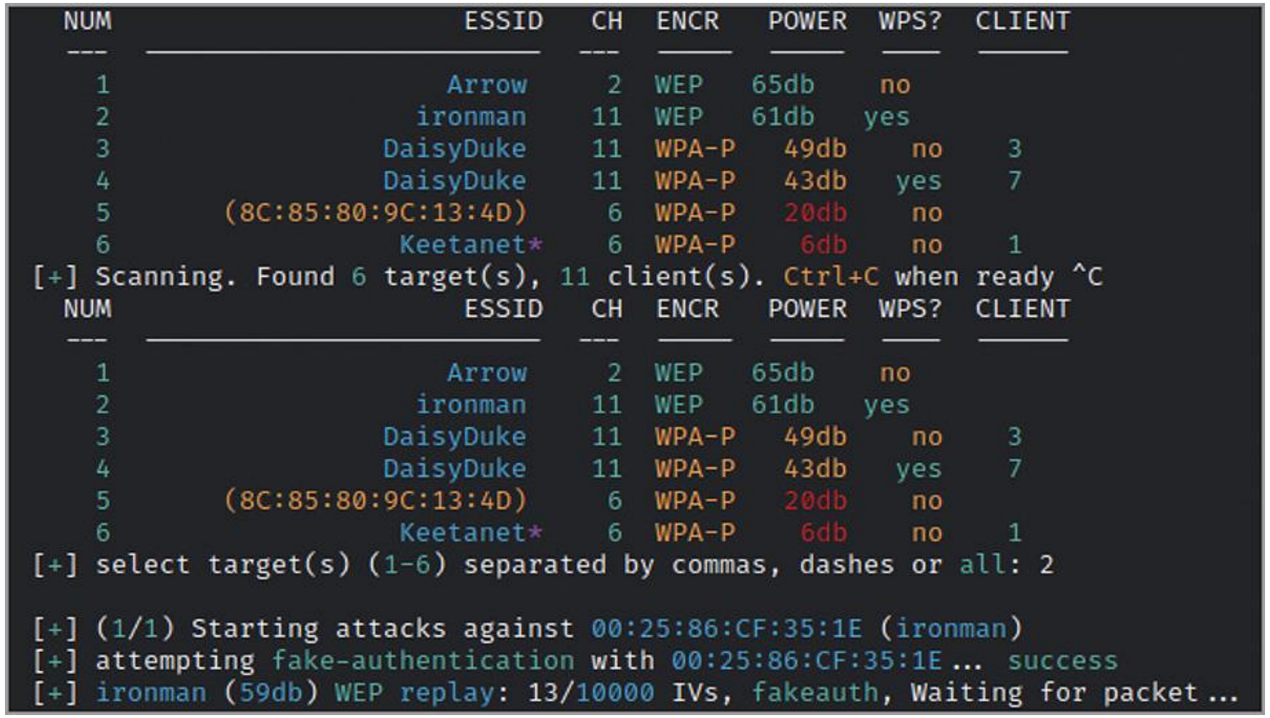
- All versions of WPA are substantially more secure than WEP and WPS
- WPA and WPA2 can be cracked using packet capturing and injection and brute force password attack on captured packets
- Wordlists or other sources can speed up password attacks
- WPA3 is much more resistant to password attacks
- The airodump-ng tool suite can perform WPA attacks

Wireless Attacks and Attack Vectors (24 of 29)

Attacking WPA, WPA2, and WPA3

Automating Wireless Attacks Using Wifite

- The Wifite tool in Kali can be used to automate WPA attacks
- Scans Wi-Fi networks and then guides users to select specific attacks
- Launches additional tools to conduct those attacks



```
  NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
  ---   ------------------------   --  -----  -----  ----  ------
    1                      Arrow    2  WEP   65db     no
    2                    ironman   11  WEP   61db    yes
    3                  DaisyDuke   11  WPA-P   49db     no      3
    4                  DaisyDuke   11  WPA-P   43db    yes      7
    5        (8C:85:80:9C:13:4D)    6  WPA-P   20db     no
    6                  Keetanet*    6  WPA-P    6db     no      1
[+] Scanning. Found 6 target(s), 11 client(s). Ctrl+C when ready ^C
  NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
  ---   ------------------------   --  -----  -----  ----  ------
    1                      Arrow    2  WEP   65db     no
    2                    ironman   11  WEP   61db    yes
    3                  DaisyDuke   11  WPA-P   49db     no      3
    4                  DaisyDuke   11  WPA-P   43db    yes      7
    5        (8C:85:80:9C:13:4D)    6  WPA-P   20db     no
    6                  Keetanet*    6  WPA-P    6db     no      1
[+] select target(s) (1-6) separated by commas, dashes or all: 2

[+] (1/1) Starting attacks against 00:25:86:CF:35:1E (ironman)
[+] attempting fake-authentication with 00:25:86:CF:35:1E... success
[+] ironman (59db) WEP replay: 13/10000 IVs, fakeauth, Waiting for packet...
```

Wifite attacking the ironman network

Wireless Attacks and Attack Vectors (25 of 29)

Attacking Bluetooth

- Bluetooth is a wireless personal area network (WPAN) technology with working exploits available, some within Kali
- Bluesnarfing – stealing info from Bluetooth-enabled devices
- Bluejacking – sending unsolicited messages using a victim’s Bluetooth device
- Bluetooth Low Energy (BLE) – variation used by some IoT and other lightweight devices
- Bluetooth Low Energy Spoofing Attack (BLESA) exploits protocol weakness not requiring reauthentication when devices reconnect

Knowledge Check Activity 8-1

What challenge makes attacking BLE, NFC, and RFID more potentially more difficult than performing attacks on traditional 802.11 wireless LANs?

a. Always-on encryption will prevent access to transmissions

b. Certificates for hosts and clients ensure strict authentication controls

c. Low transmission distances require close proximity of attacker to target

d. Hardcoded MAC addresses prevent spoofing of target systems

Knowledge Check Activity 8-1: Answer

What challenge makes attacking BLE, NFC, and RFID more potentially more difficult than performing attacks on traditional 802.11 wireless LANs?

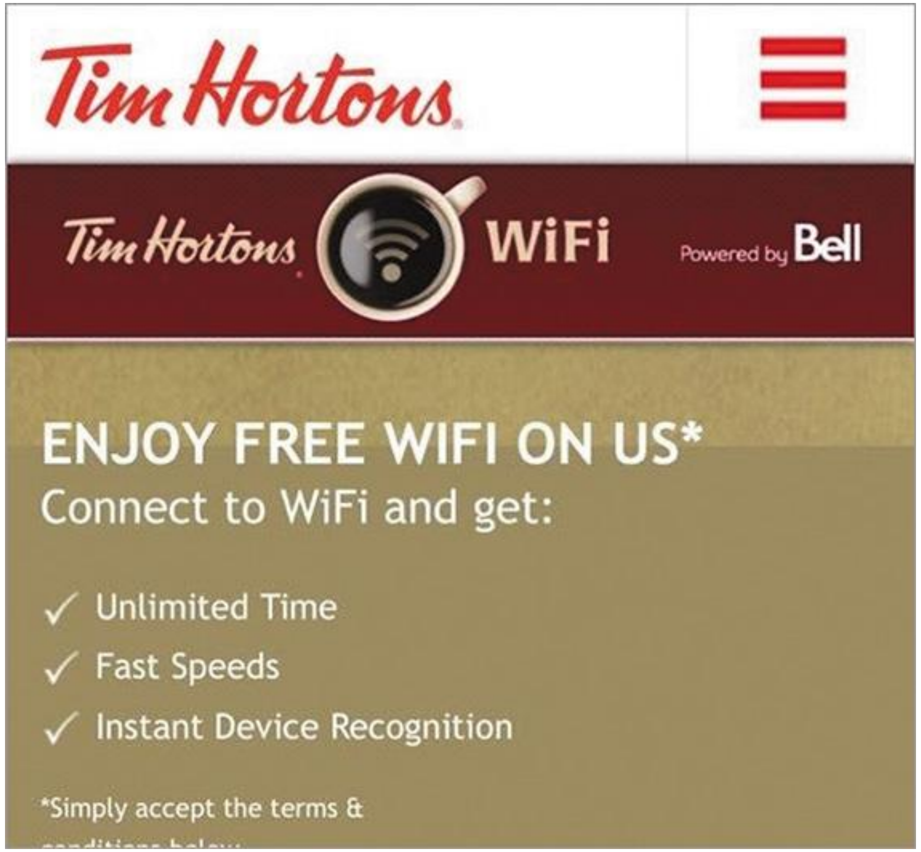
Answer: Low transmission distances require close proximity of attacker to target

With transmission distances ranging from a few centimeters for NFC to several meters for Bluetooth, an attacker will need to be close enough to successfully send and receive attack packets for a successful attack.

Wireless Attacks and Attack Vectors (26 of 29)

Attacking Captive Portals

- Captive portals are login pages providing entry points for access to a Wi-Fi network, often a public WLAN provided by a business
- Security on captive portal protected WLANs might be low as intent is to provide quick and easy Wi-Fi access
- Spoofing MAC address of authenticated client or other device may bypass captive portals



ENJOY FREE WIFI ON US*

Connect to WiFi and get:

✓ Unlimited Time

✓ Fast Speeds

✓ Instant Device Recognition

*Simply accept the terms &

Captive portal

Wireless Attacks and Attack Vectors (27 of 29)

NFC and Amplification Attacks

- NFC is only useful for very short ranges, 4cm or less, limits attacks
- Tap-to-pay services use NFC as do some ATMs
- Eavesdropping is possible but encryption may be used, rendering it difficult
- NFC relay attack more likely in a crowded location by two attackers
  - First attacker can hold phone near target’s NFC, phone in pocket
  - First attacker relays captured NFC credentials to second attacker which then presents to NFC access device to open secured door
- NFC can be amplified using hardware and software tools in amplification attack

Wireless Attacks and Attack Vectors (28 of 29)

RFID Cloning

- RFID tags are common in physical access control systems
- There are multiple types of RFID devices, employing different RF ranges and technology to enable
- RFID cloners can be purchase cheaply
- Obtaining access to RFID tag, even for a short time, can allow cloning, just like copying a spare key

lidiasilva/Shutterstock.com

RFID cloner and tags

Wireless Attacks and Attack Vectors (29 of 29)

Jamming and Repeating

- Jamming is a wireless DoS attack, prevents communication to target
- May be illegal depending on jurisdiction and methods; not advisable
- Repeating wireless traffic in relay attack can be used in on-path scenarios
  - WEP, WPA, WPA2, WPA3 and NFC can be attacked via relay
- Wireless repeater is device that can be used to amplify target wireless device signal to transmit it further than is intended by target
  - Can allow attacker access to WLAN from outside normal physical proximity

Specialized System Attacks and Attack Vectors (1 of 5)

Attacking Specialized Systems

- Many types of specialized and embedded systems are employed by organizations and may be subject to various attack methods
  - IoT devices
  - Industrial Control Systems (ICS)
  - Cellular/Smartphones
  - Industrial IoT (IIoT)
  - SCADA systems
  - Intelligent Platform Management Interface (IPMI) systems
- Because these systems may be used in factory environments or industrial applications to control powerful machines or other dangerous processes, extra care must be taken by pen tester
- Make sure any specialized systems are within SOW and ROE

Specialized System Attacks and Attack Vectors (2 of 5)

Attacking Specialized Systems

- Bluetooth Low Energy attacks – MITM, sniffing, MAC address spoofing, jamming, and device-pairing attacks
- Insecure default settings and hard-coded configurations – default settings may be more likely found on specialized systems; some may not be able to be changed
- Use of insecure or outdated software, hardware, and firmware – includes outdated OSs; more likely for specialized systems to be difficult or impossible to apply certain security patches or protections
- Cleartext communication – HTTP, FTP, Telnet or other unencrypted protocols may be in use

Specialized System Attacks and Attack Vectors (3 of 5)

Attacking Mobile Devices

- Mobile devices are everywhere and connected to wide range of networks
- Vulnerable when connected to public network, may be vulnerable when connected to enterprise network
- Personally-owned devices used for business present unique challenges
- Reverse engineering – analyzing source code or mobile applications to locate vulnerabilities
- Sandbox analysis – running mobile code in controlled environment to determine how it works and what it accesses
- Spamming – user tricked to launch code via spam text, email, calls

Specialized System Attacks and Attack Vectors (4 of 5)

Attacking Mobile Devices - Vulnerabilities

- Insecure storage – removable MicroSD cards, cloud services, unencrypted info, and other weak application storage mechanisms may be subject to attacker access
- Passcode vulnerabilities – include bypass techniques for lock screen or passcode, biometric access, or email resets to reset passcodes
- Certificate pinning – changing X.509 certificate paired to device to gain access
- Vulnerable components – premade components such as communication modules; other processors and firmware may have vulnerabilities

Specialized System Attacks and Attack Vectors (5 of 5)

Attacking Mobile Devices - Vulnerabilities

- Root level access – Jailbreaking or other methods or tools to provide root access to device can require considerable effort or be trivial to perform
- Biometric vulnerabilities – spoofing fingerprints or circumventing facial recognition for biometric access controls possible, especially on lower quality biometric components
- Business logic vulnerabilities – compromising mobile app flaws to gain access to device
- Personally owned devices not likely in scope of pen test

Discussion Activity 8-2

Modern organizations and their networks are more likely to host non-traditional devices than in years prior. List five different types of specialized systems discussed in this module. Explain each, and discuss the challenges associated with securing and with pen testing these types of devices.

Summary (1 of 2)

By the end of this module, you should be able to:

1. Describe wireless attacks and attack vectors
2. Describe specialized systems attacks and attack vectors
3. Explain wireless network components, architecture, authentication, and encryption
4. Describe Radio-Frequency Identification (RFID) and Near Field Communication (NFC)
5. Explain how to acquire wireless hacking targets
6. Describe wardriving

Summary (2 of 2)

By the end of this module, you should be able to:

7. Explain the tools and methods used to compromise WPS, WEP, WPA, WPA2, and WPA3 wireless security protocols
8. Describe the tools and methods used to compromise Bluetooth, RFID, and NFC technologies
9. Describe specialized systems and their vulnerabilities and attack vectors
10. Describe mobile device vulnerabilities and attack vectors