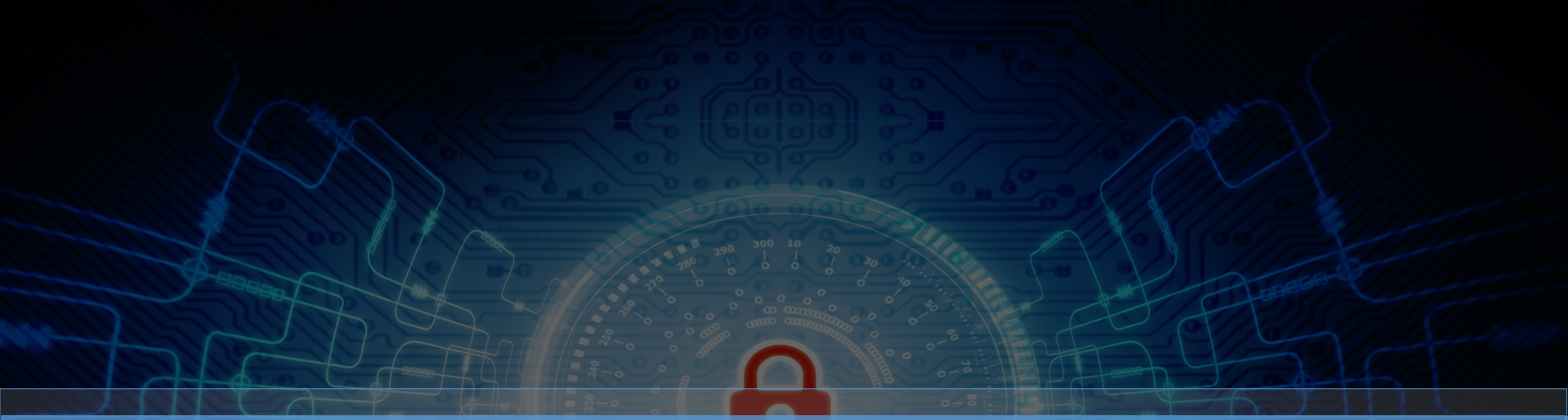
CHAPTER 4

Wireless and RF Attacks



Episode 4.01 - Wireless Exploits, Part 1

Objective 3.2 Given a scenario, research attack vectors and perform wireless attacks

WIRELESS AND RF VULNERABILITIES

- Wireless and RF vulnerabilities
  - Broadcast is wide open
  - aircrack-ng
- Evil twin – rogue WAP used to eavesdrop
  - Karma attack (Karma Attacks Radio Machines Automatically)
  - Downgrade attack – attempt to negotiate a more insecure protocol
- Deauthentication attacks
  - DoS attacks, disrupt communication between user and WAP

WIRELESS AND RF VULNERABILITIES

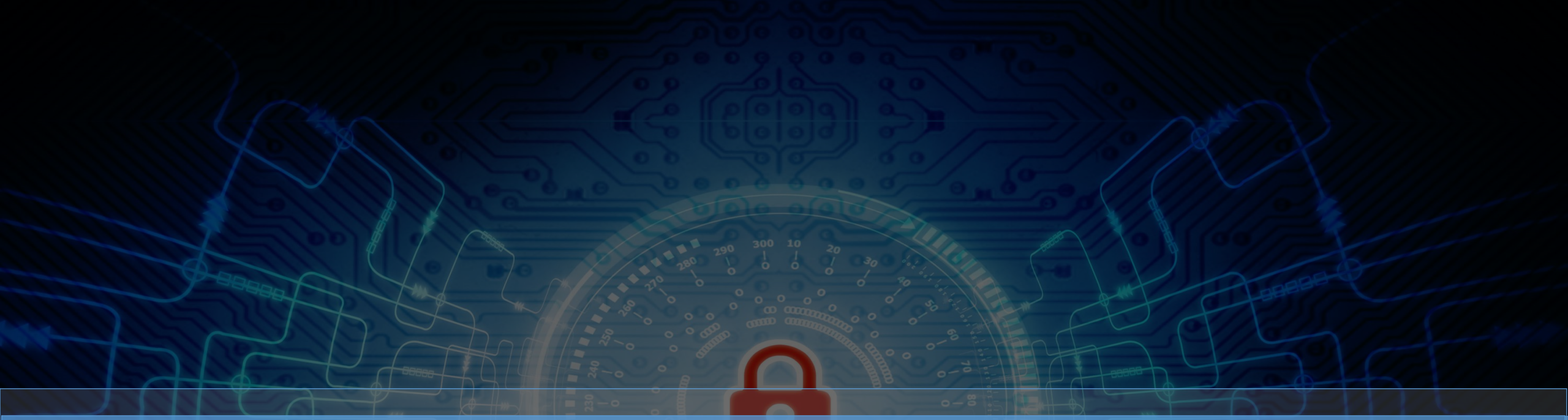
- Fragmentation attacks
  - DoS attack, floods a network with datagram fragments
- Credential harvesting
  - Process of capturing or discovering valid login
  - Social engineering, etc
- WPS implementation weaknesses
  - Several consumer grade WAPs could allow an attacker to learn the WPS PIN

OTHER WIRELESS VULNERABILITIES

- Bluejacking
  - Unsolicited messages to a Bluetooth-enabled device
- Bluesnarfing
  - Stealing information from Bluetooth-enabled device
- RFID Cloning
  - Unauthorized copy of device's RF signal
- Jamming
  - DoS attack, disables communication among devices
- Repeating
  - Receiving and retransmitting a signal to increase range

QUICK REVIEW

- Anyone can receive wireless traffic - unencrypted means anyone can read it
- Evil twin can trick users into using your access point instead of a valid one
- Multiple attacks emerging for Bluetooth devices
- IoT makes wireless vulnerabilities much more prevalent



Episode 4.02 – Wireless Exploits, Part 2

Objective 3.2 Given a scenario, research attack vectors and perform wireless attacks

WIRELESS EXPLOITS

- Data modification
  - Unauthorized wireless access to change actionable data
  - May focus on altering configuration to ease further access/attack
- Data corruption
  - Attack on availability
  - Targets may be valuable data and/or configuration settings
- Capture handshakes
  - Useful in replay and impersonation attacks
- On-path
  - Previously known as man-in-the-middle attacks

QUICK REVIEW

- Wireless attacks focus on key vulnerable areas including sessions, authentication, and blocking valid access
- Data corruption is an attack on availability
- Capturing handshakes is useful in replay and impersonation attacks

Episode 4.03 – Antennas

Objective 3.2 Given a scenario, research attack vectors and perform wireless attacks

WIRELESS ATTACK TOOLS

- Amplified antenna
  - Device to extend the effective range of attack platform
  - Allows an attacker to carry out attacks physically farther from victims

QUICK REVIEW

- Amplified antennas are devices used to extend the effective range of attack platform
- Amplified antennas allow an attacker to carry out attacks physically farther from victims