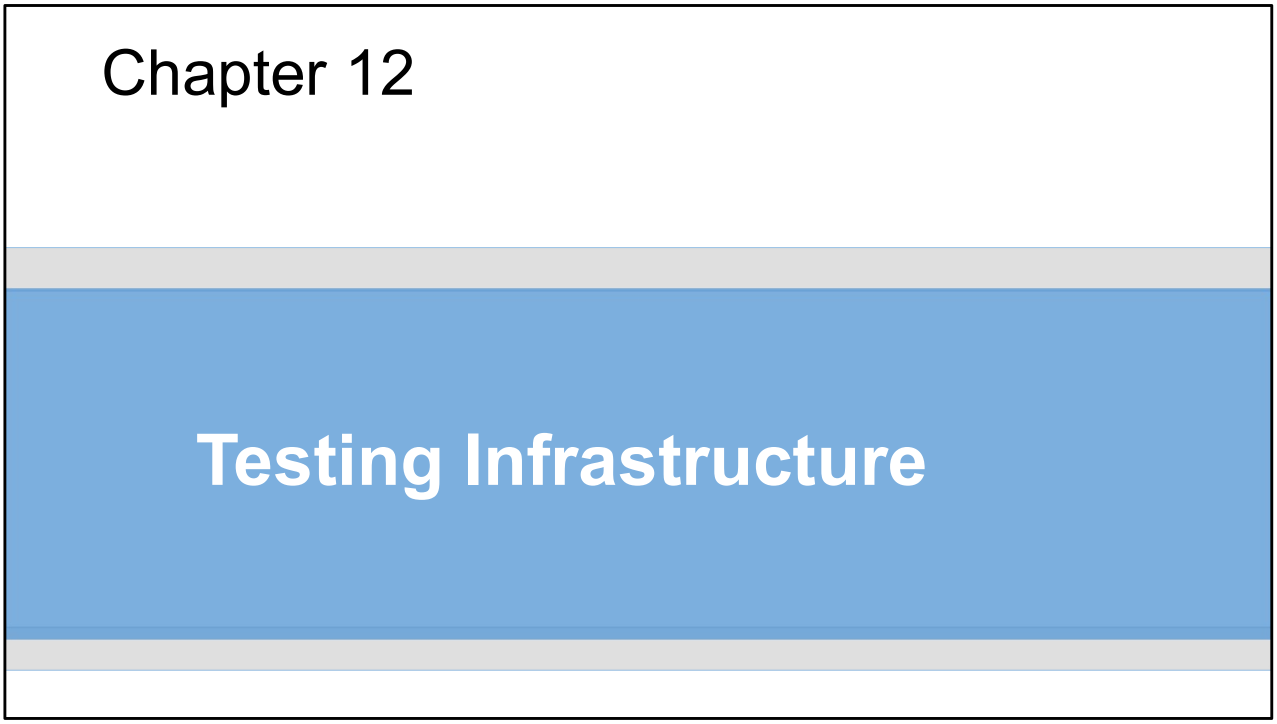
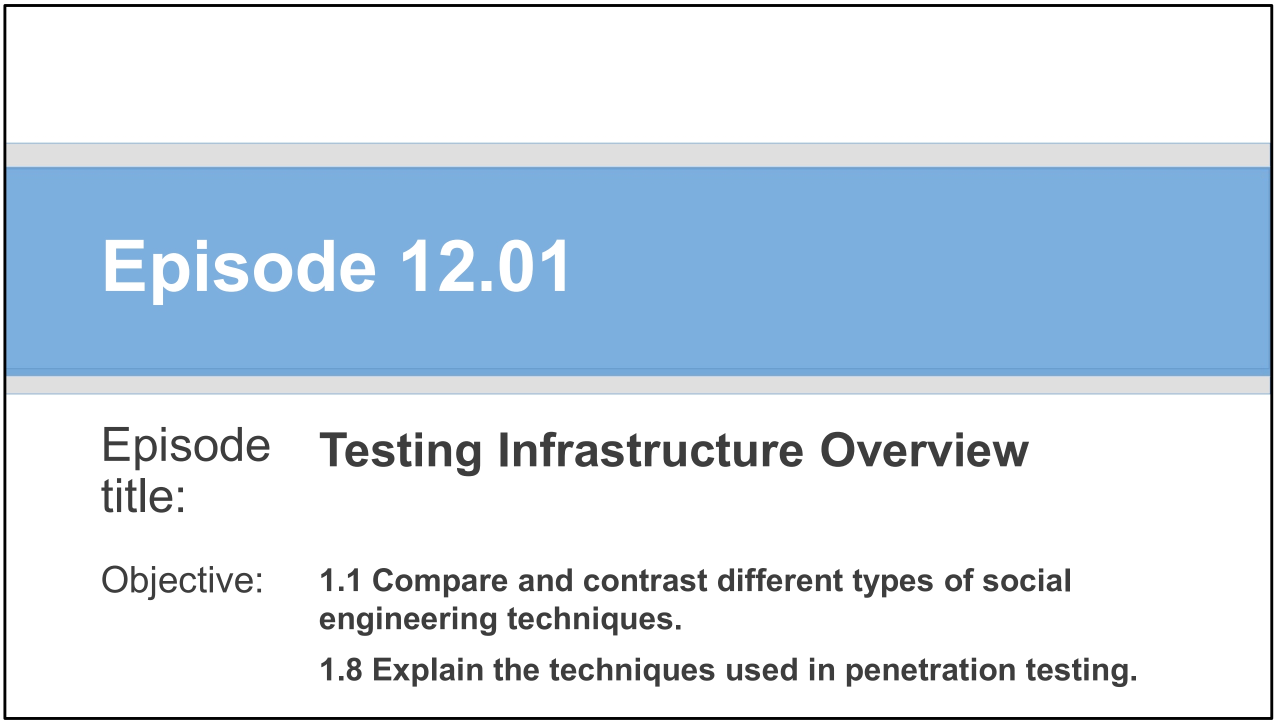


Chapter 12

Testing Infrastructure

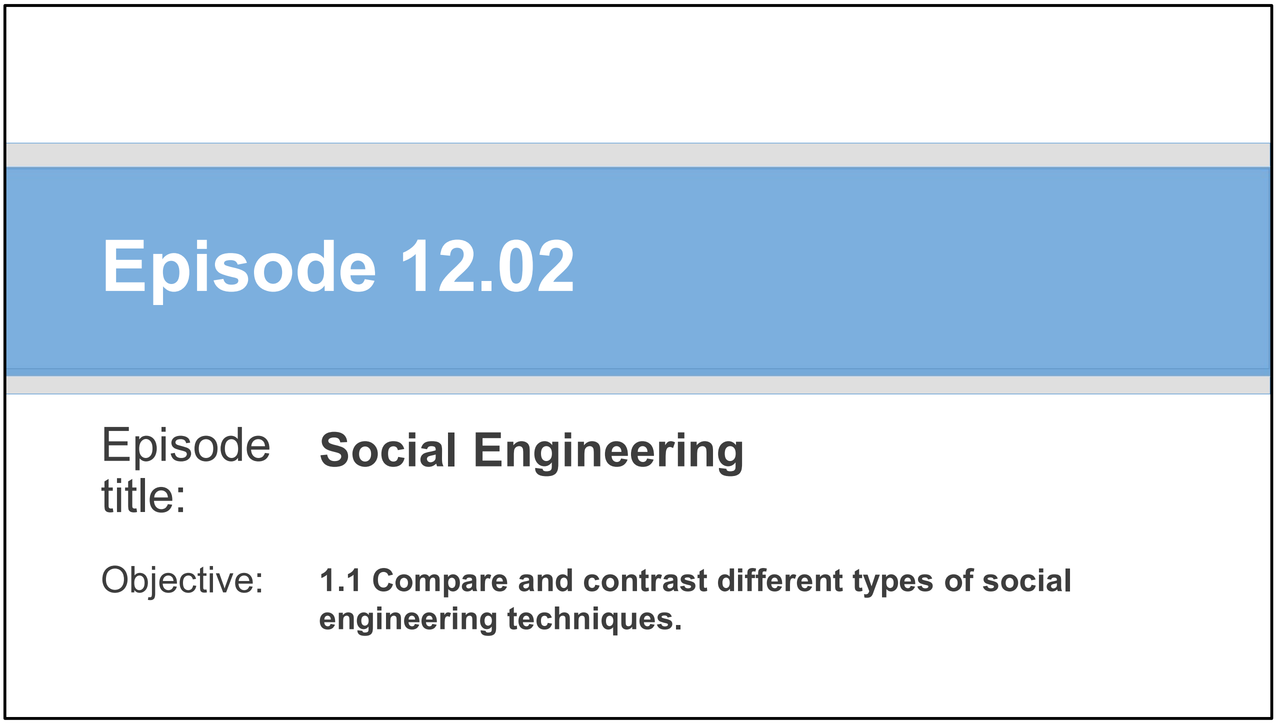


Episode 12.01

Episode title: **Testing Infrastructure Overview**

Objective: **1.1 Compare and contrast different types of social engineering techniques.**

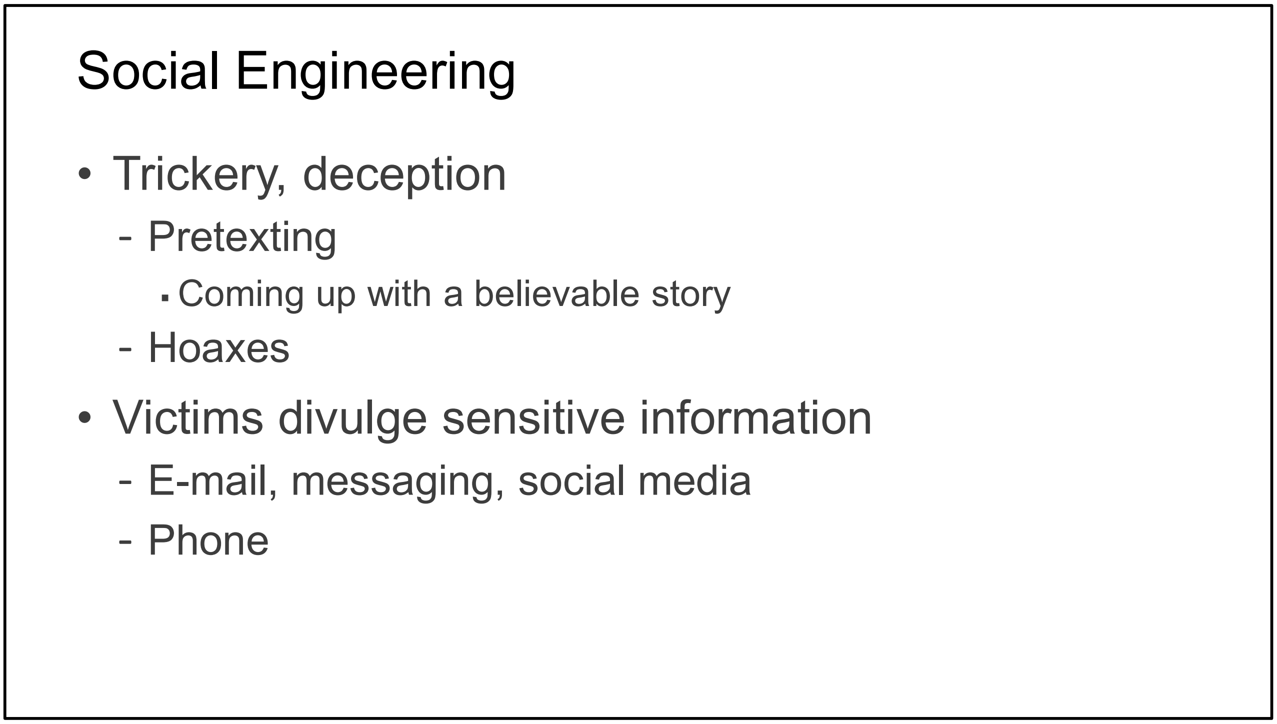
1.8 Explain the techniques used in penetration testing.



Episode 12.02

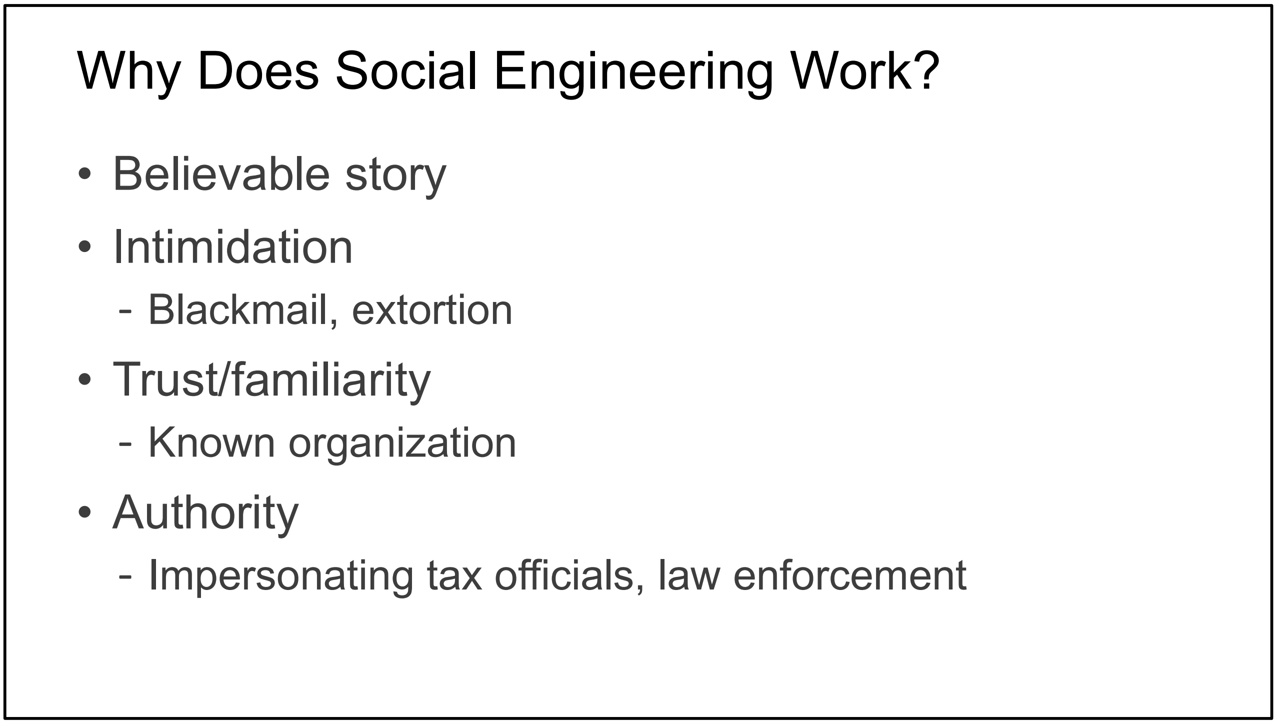
Episode title: **Social Engineering**

Objective: **1.1 Compare and contrast different types of social engineering techniques.**



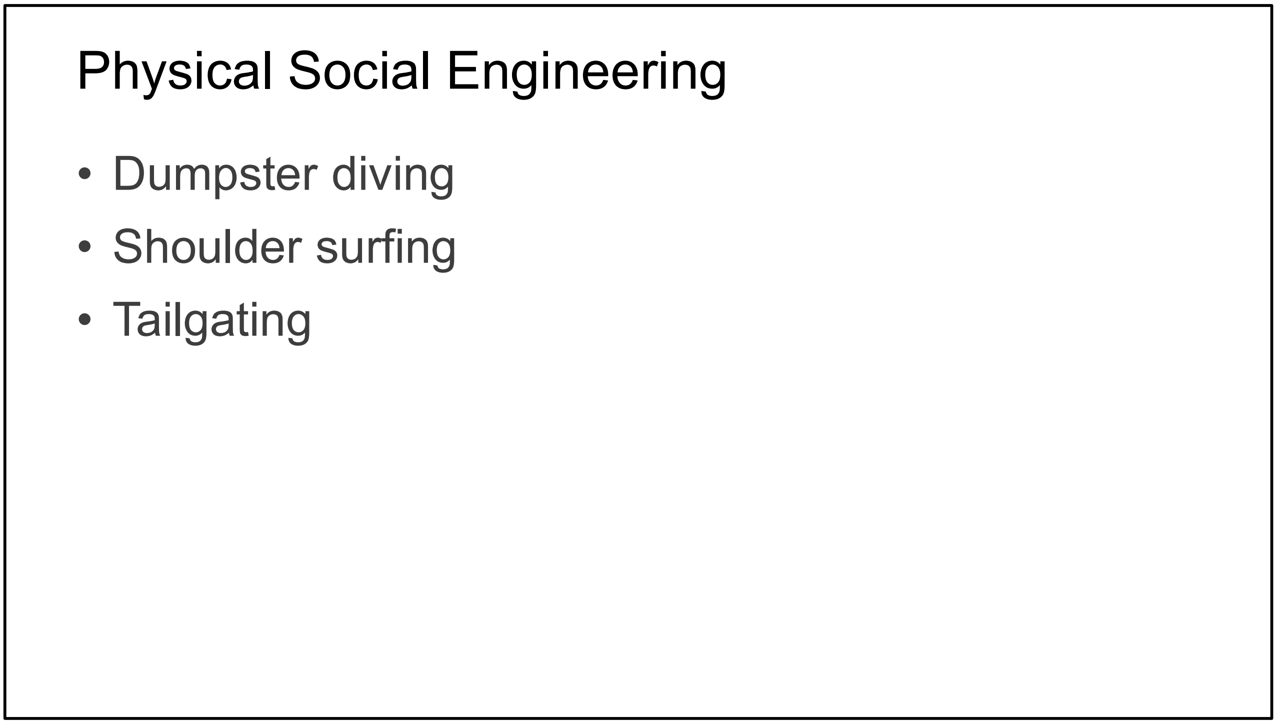
Social Engineering

- Trickery, deception
  - Pretexting
    - Coming up with a believable story
  - Hoaxes
- Victims divulge sensitive information
  - E-mail, messaging, social media
  - Phone



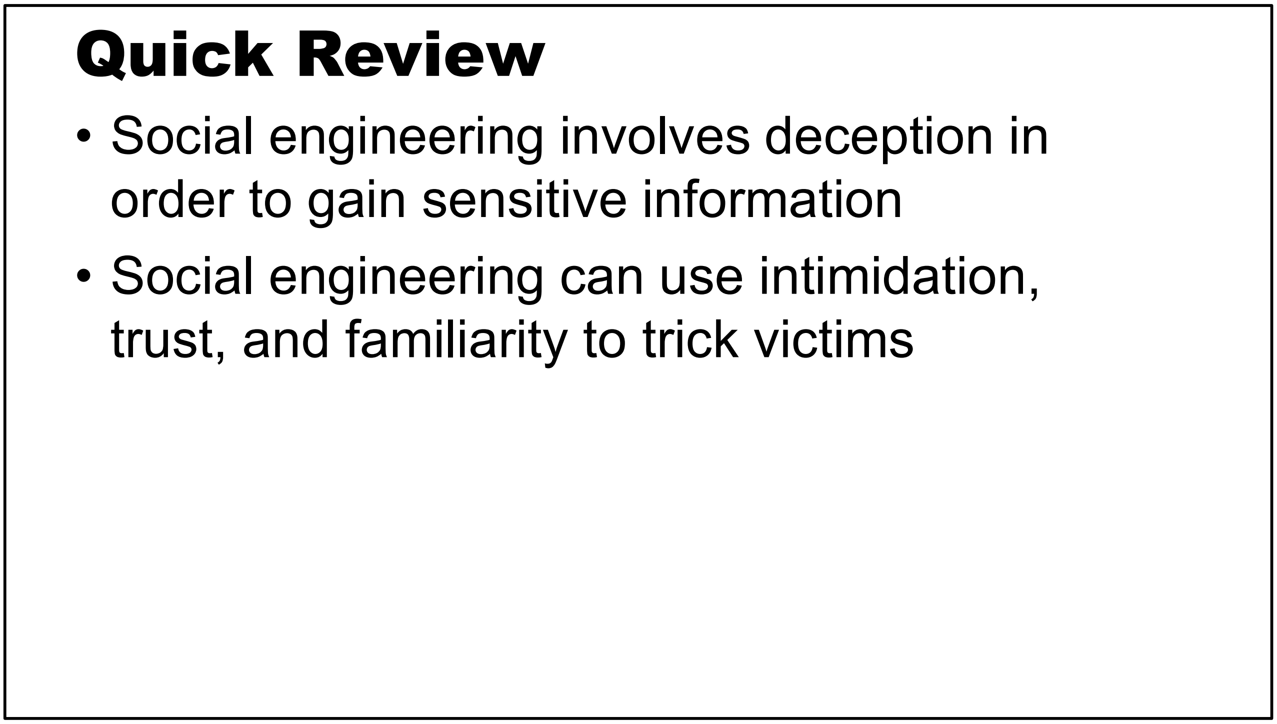
Why Does Social Engineering Work?

- Believable story
- Intimidation
  - Blackmail, extortion
- Trust/familiarity
  - Known organization
- Authority
  - Impersonating tax officials, law enforcement



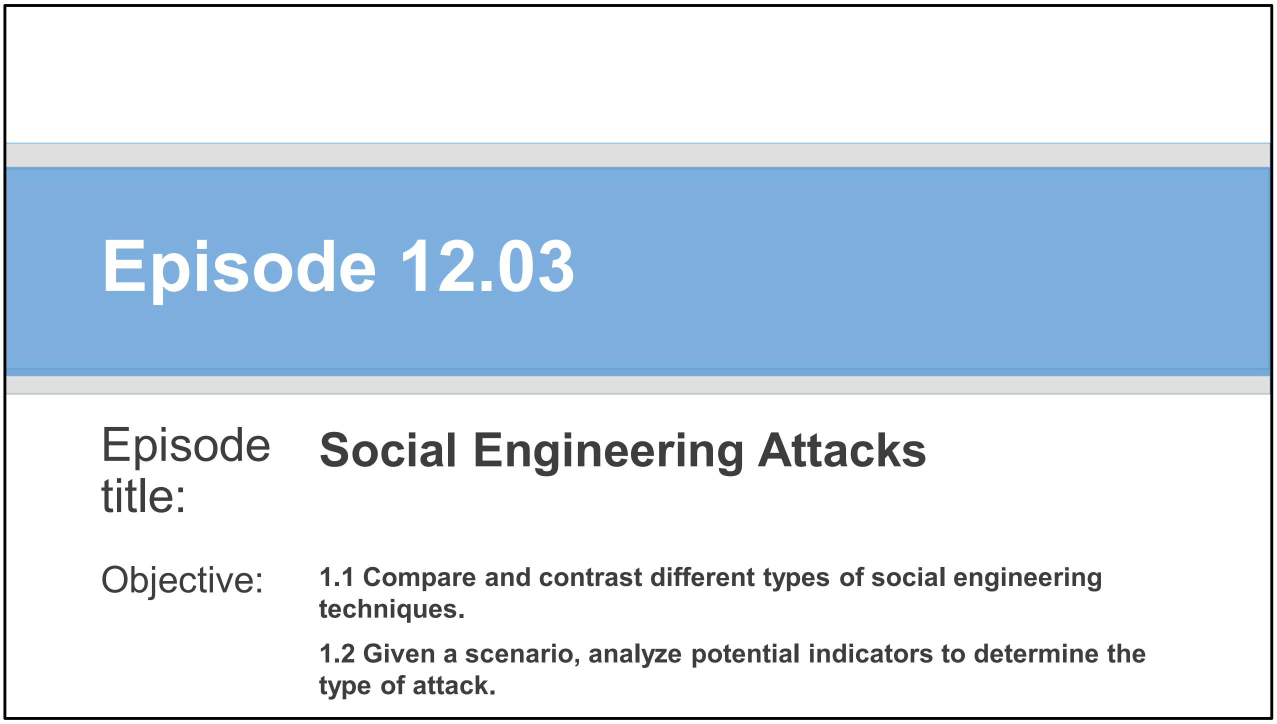
Physical Social Engineering

- Dumpster diving
- Shoulder surfing
- Tailgating



Quick Review

- Social engineering involves deception in order to gain sensitive information
- Social engineering can use intimidation, trust, and familiarity to trick victims

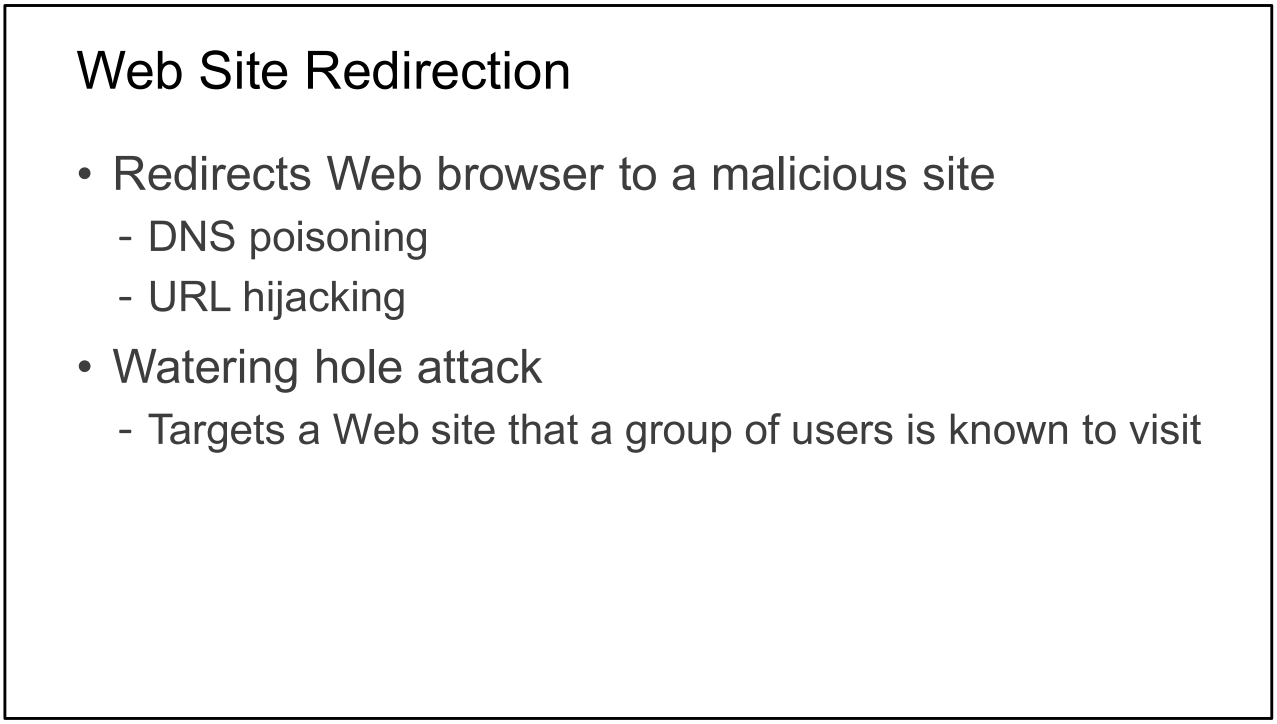


Episode 12.03

Episode title: **Social Engineering Attacks**

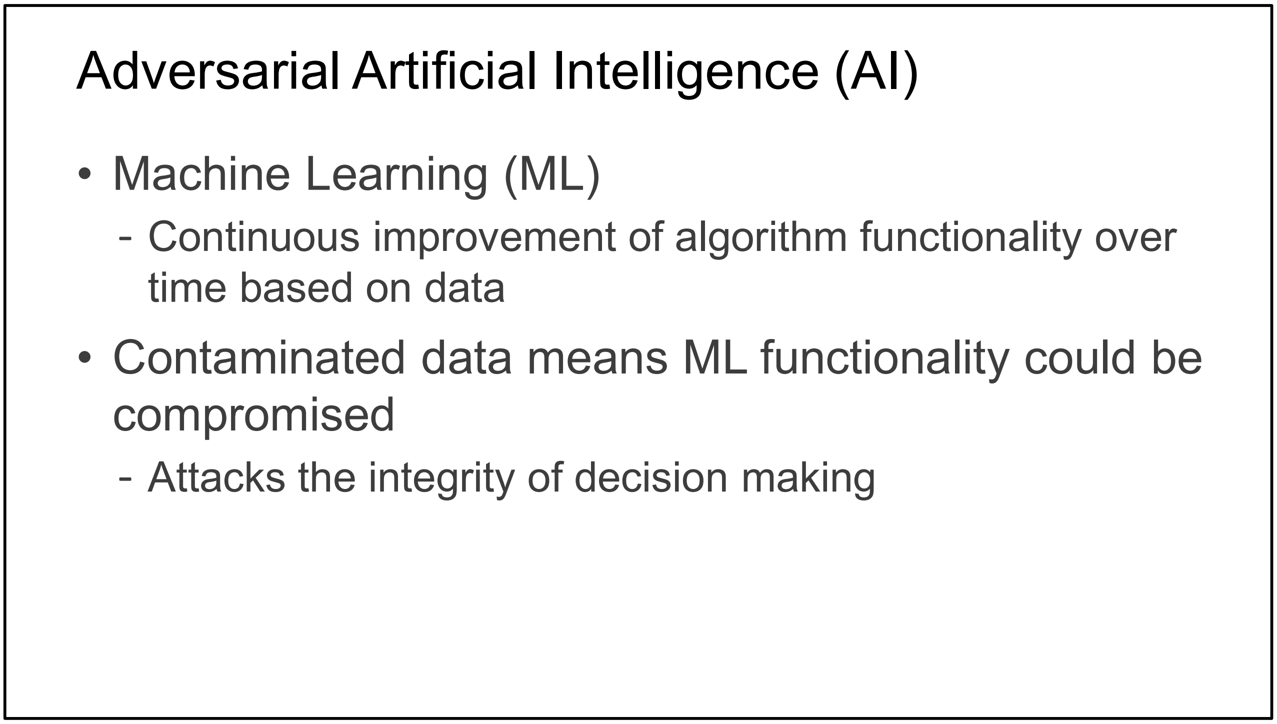
Objective: **1.1 Compare and contrast different types of social engineering techniques.**

1.2 Given a scenario, analyze potential indicators to determine the type of attack.



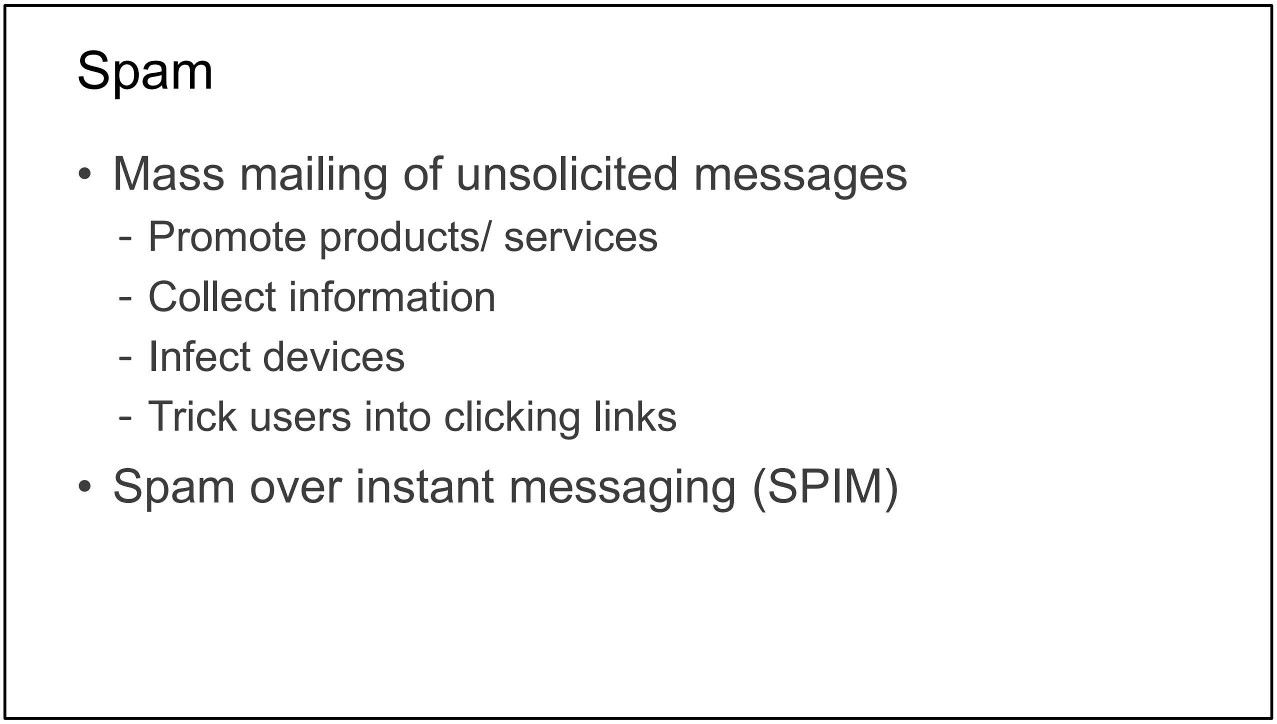
Web Site Redirection

- Redirects Web browser to a malicious site
  - DNS poisoning
  - URL hijacking
- Watering hole attack
  - Targets a Web site that a group of users is known to visit



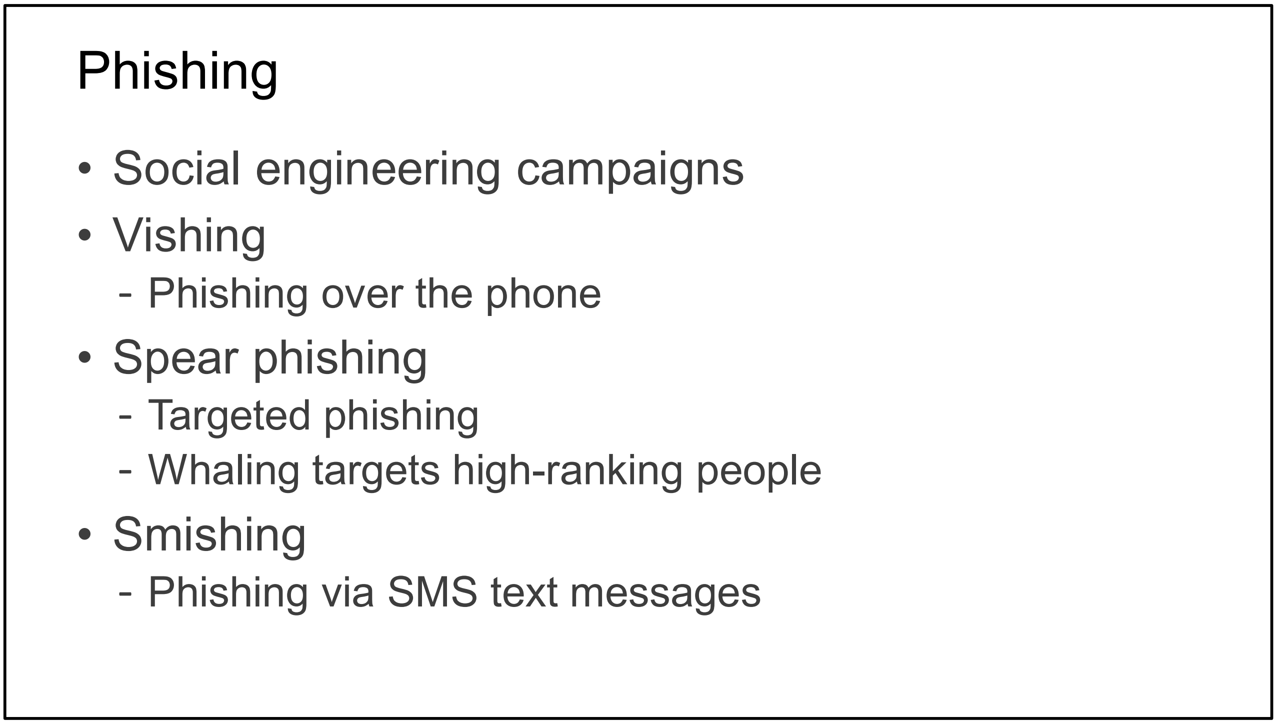
Adversarial Artificial Intelligence (AI)

- Machine Learning (ML)
  - Continuous improvement of algorithm functionality over time based on data
- Contaminated data means ML functionality could be compromised
  - Attacks the integrity of decision making



Spam

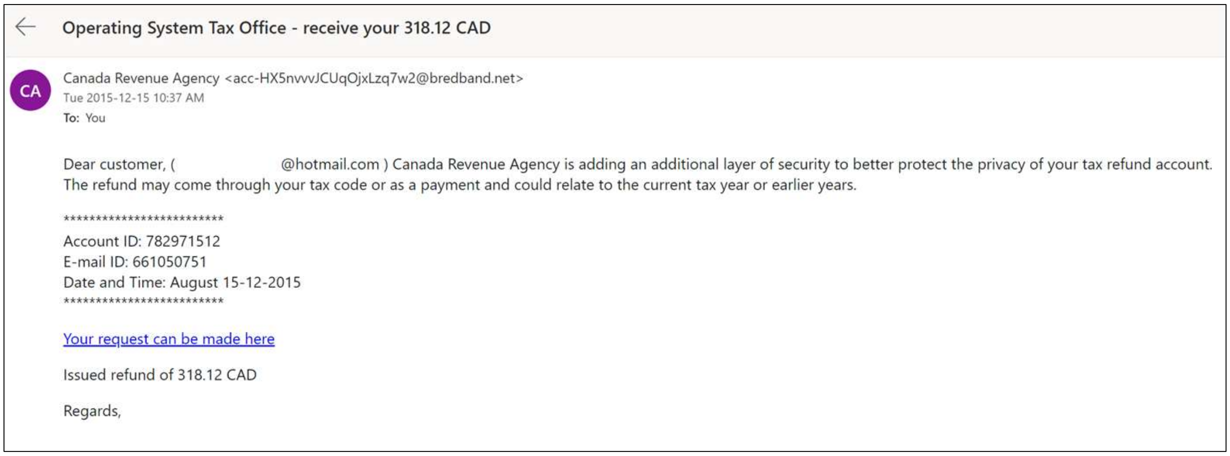
- Mass mailing of unsolicited messages
  - Promote products/ services
  - Collect information
  - Infect devices
  - Trick users into clicking links
- Spam over instant messaging (SPIM)



Phishing

- Social engineering campaigns
- Vishing
  - Phishing over the phone
- Spear phishing
  - Targeted phishing
  - Whaling targets high-ranking people
- Smishing
  - Phishing via SMS text messages

Income Tax Phishing Scam



Operating System Tax Office - receive your 318.12 CAD

Canada Revenue Agency <acc-HX5nvvvJCUqOjxLzq7w2@bredband.net>
Tue 2015-12-15 10:37 AM
To: You

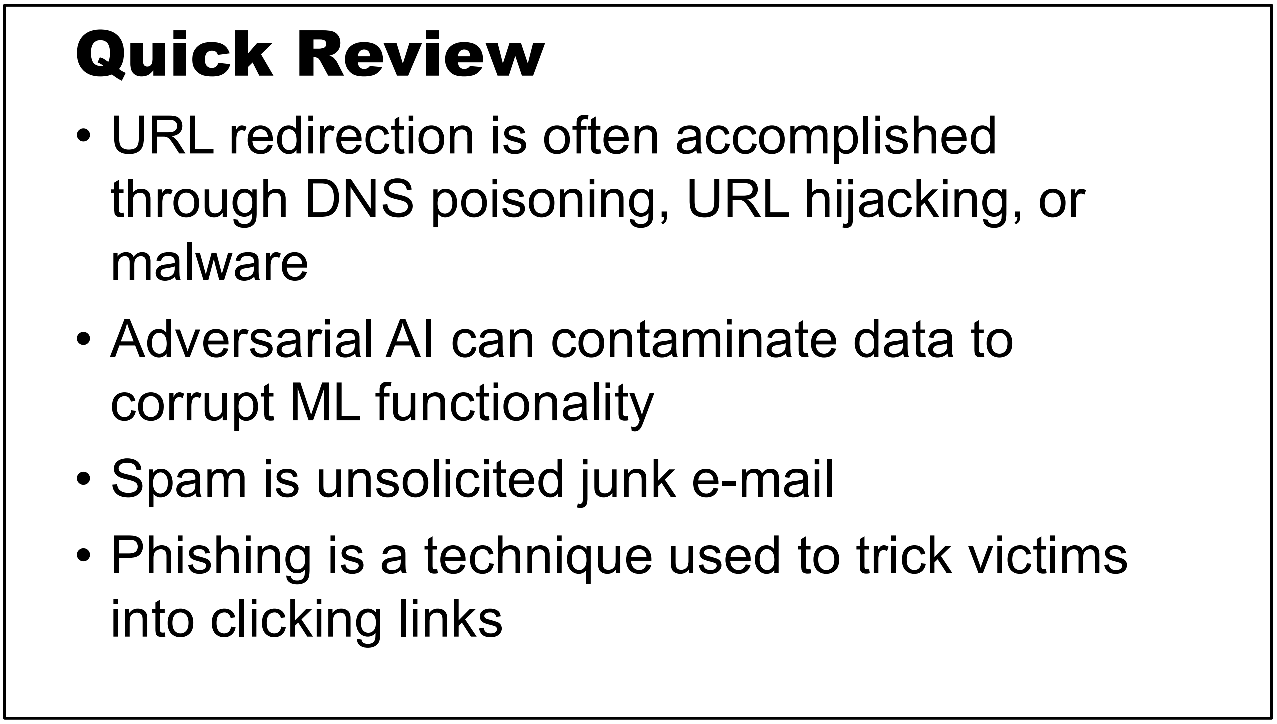
Dear customer, (@hotmail.com) Canada Revenue Agency is adding an additional layer of security to better protect the privacy of your tax refund account. The refund may come through your tax code or as a payment and could relate to the current tax year or earlier years.

****
Account ID: 782971512
E-mail ID: 661050751
Date and Time: August 15-12-2015
****

Your request can be made here

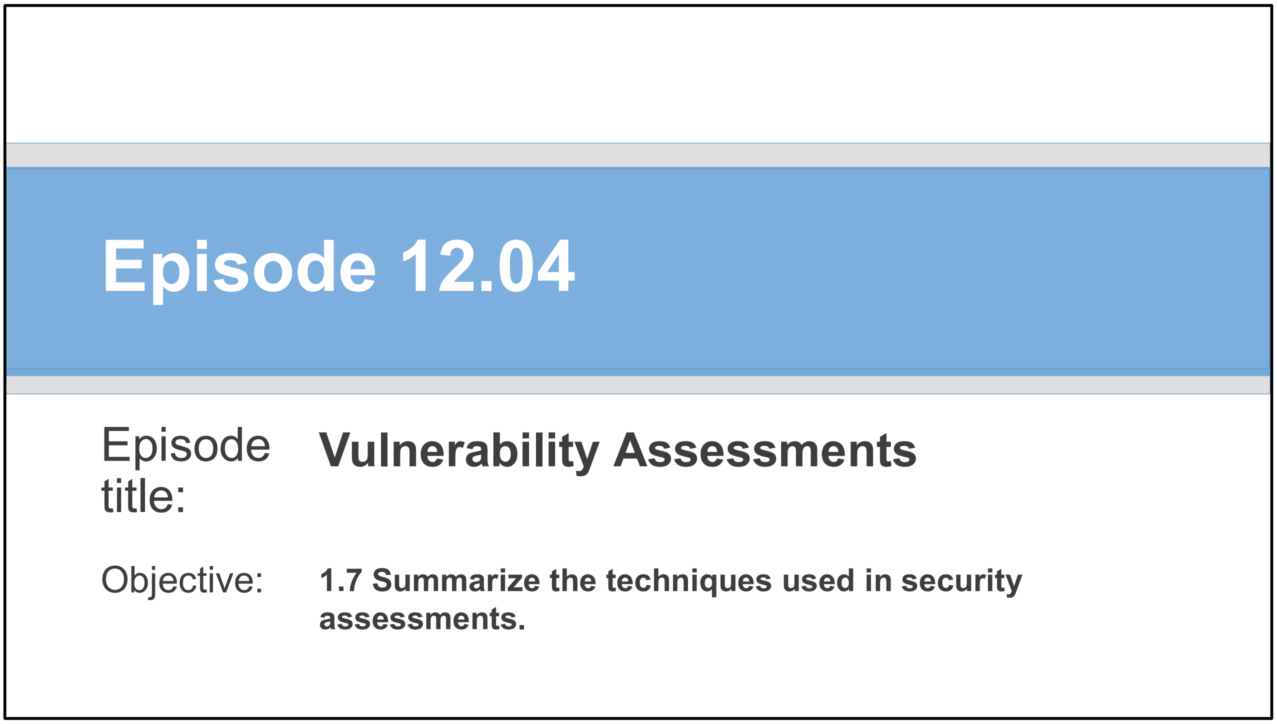
Issued refund of 318.12 CAD

Regards,



Quick Review

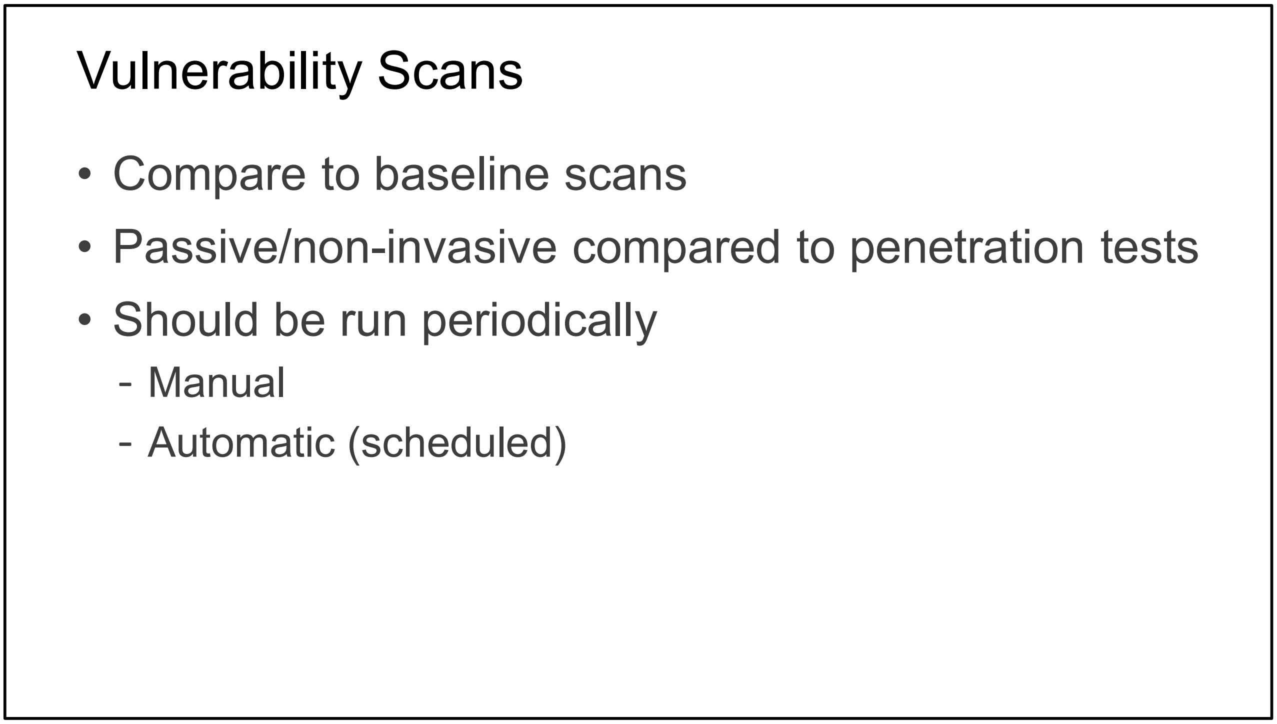
- URL redirection is often accomplished through DNS poisoning, URL hijacking, or malware
- Adversarial AI can contaminate data to corrupt ML functionality
- Spam is unsolicited junk e-mail
- Phishing is a technique used to trick victims into clicking links



Episode 12.04

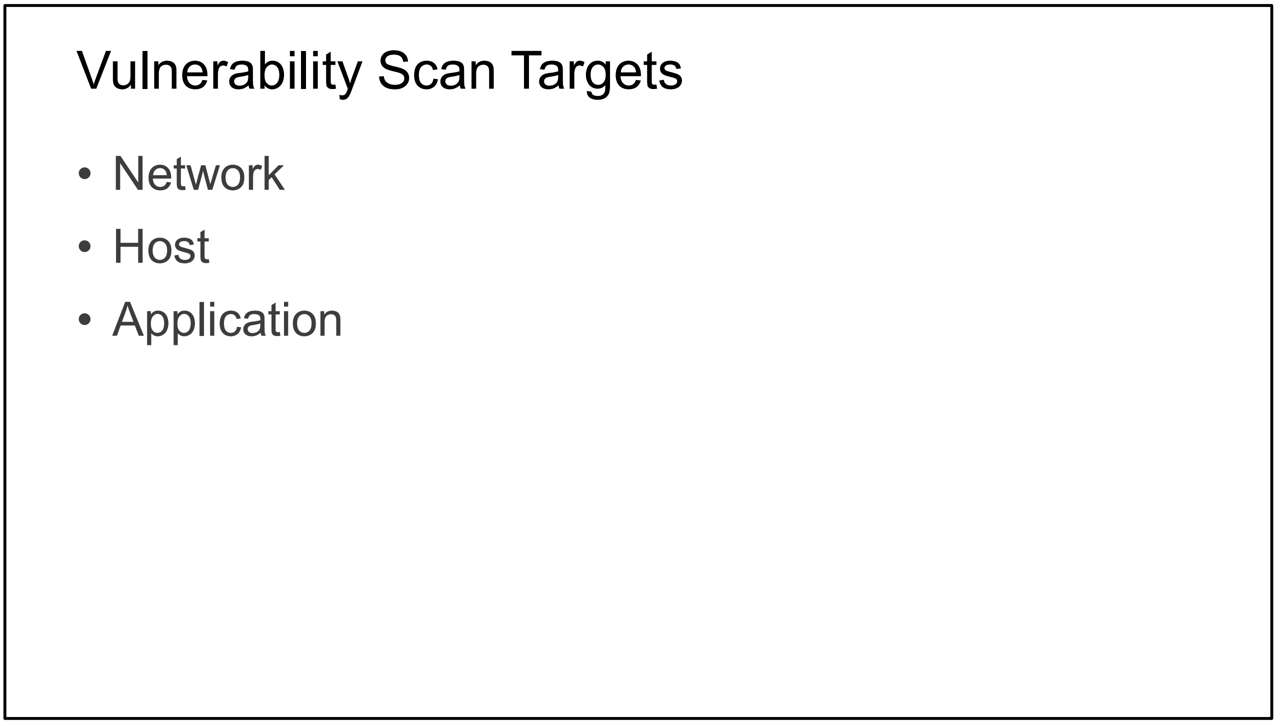
Episode title: **Vulnerability Assessments**

Objective: **1.7 Summarize the techniques used in security assessments.**



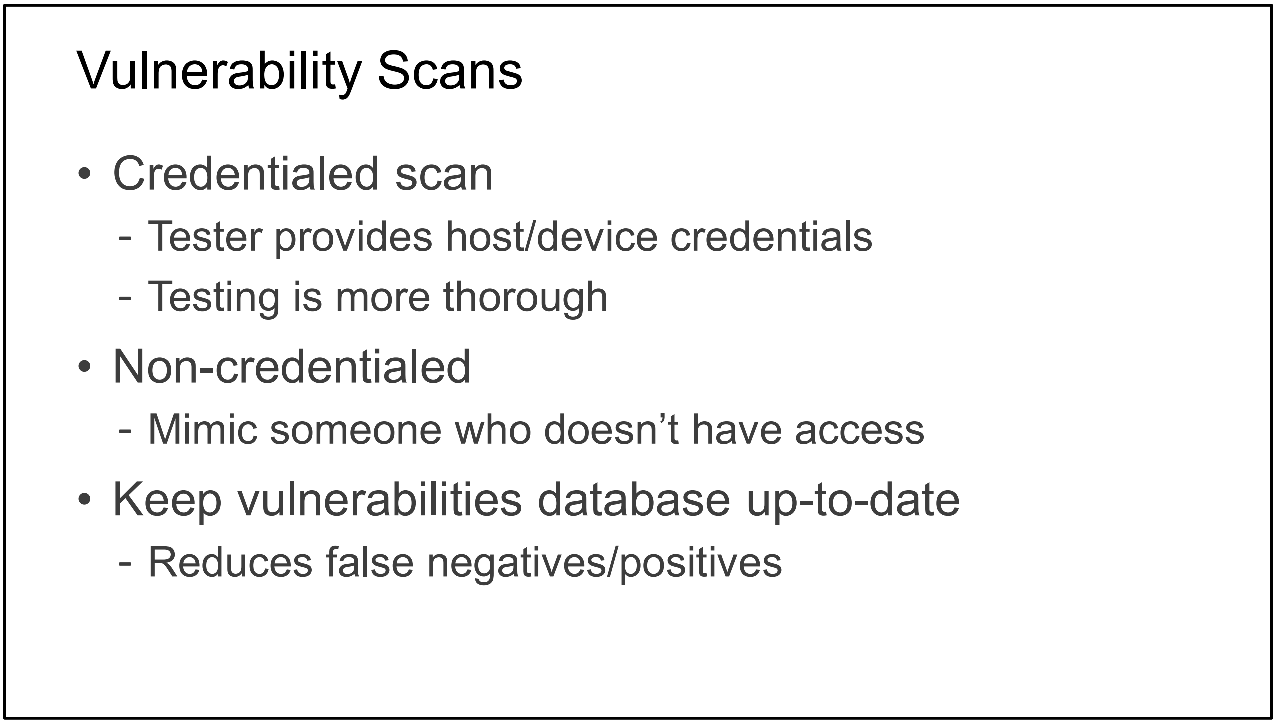
Vulnerability Scans

- Compare to baseline scans
- Passive/non-invasive compared to penetration tests
- Should be run periodically
  - Manual
  - Automatic (scheduled)



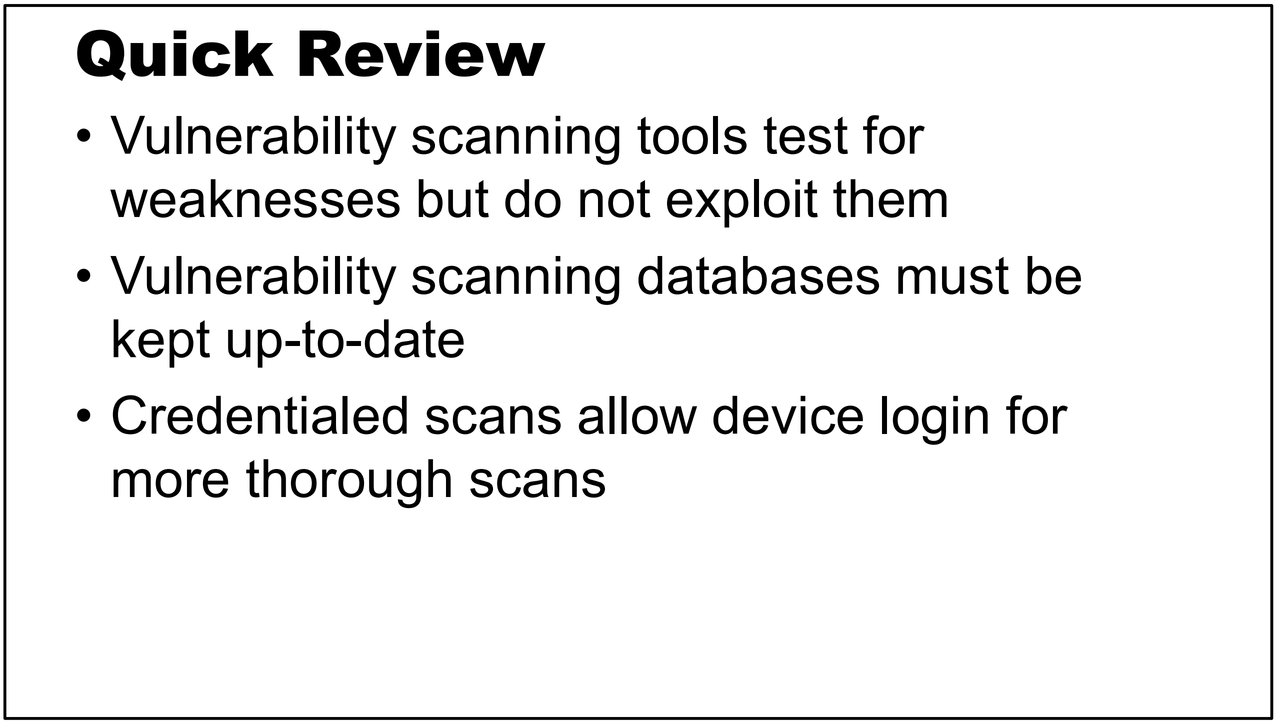
Vulnerability Scan Targets

- Network
- Host
- Application



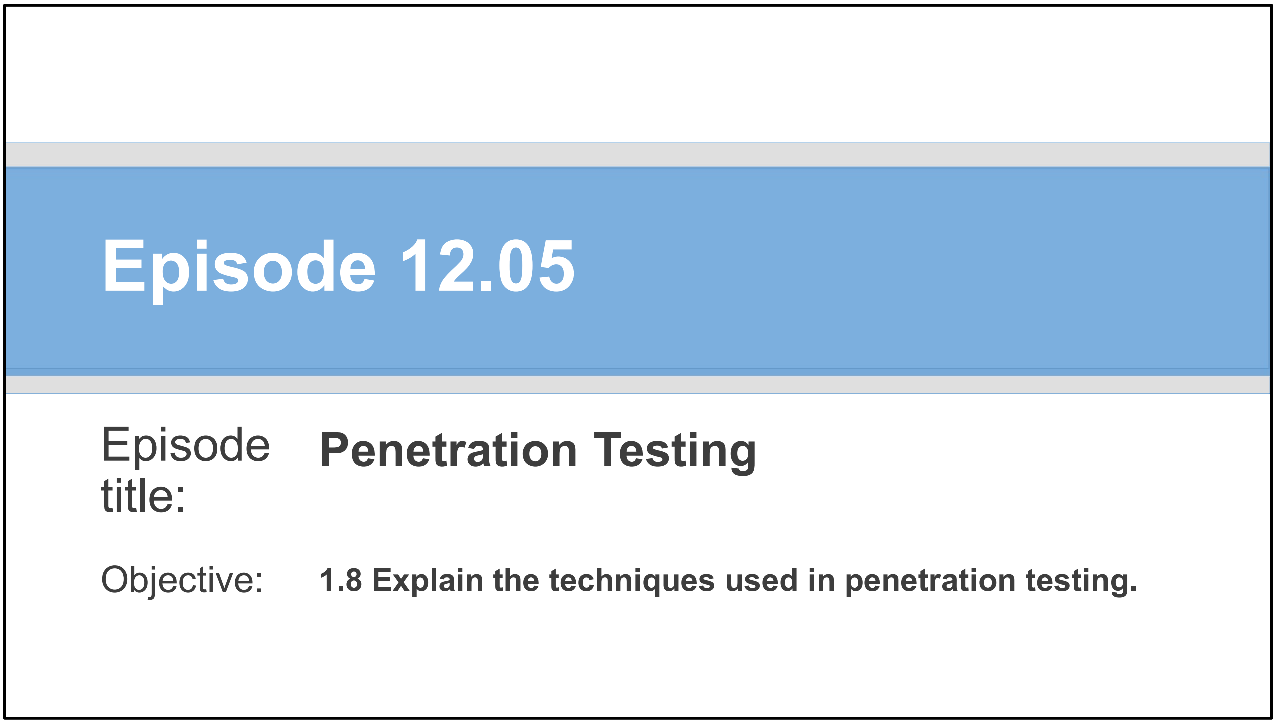
Vulnerability Scans

- Credentialed scan
  - Tester provides host/device credentials
  - Testing is more thorough
- Non-credentialed
  - Mimic someone who doesn’t have access
- Keep vulnerabilities database up-to-date
  - Reduces false negatives/positives



Quick Review

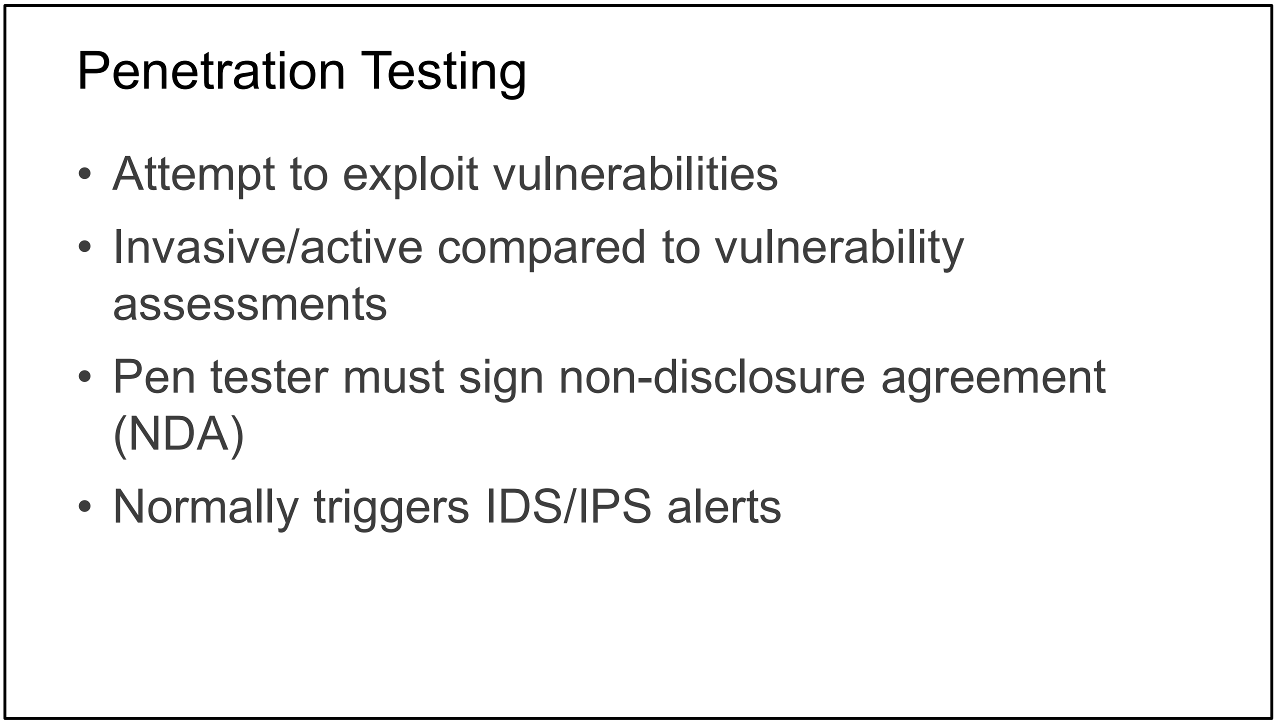
- Vulnerability scanning tools test for weaknesses but do not exploit them
- Vulnerability scanning databases must be kept up-to-date
- Credentialed scans allow device login for more thorough scans



Episode 12.05

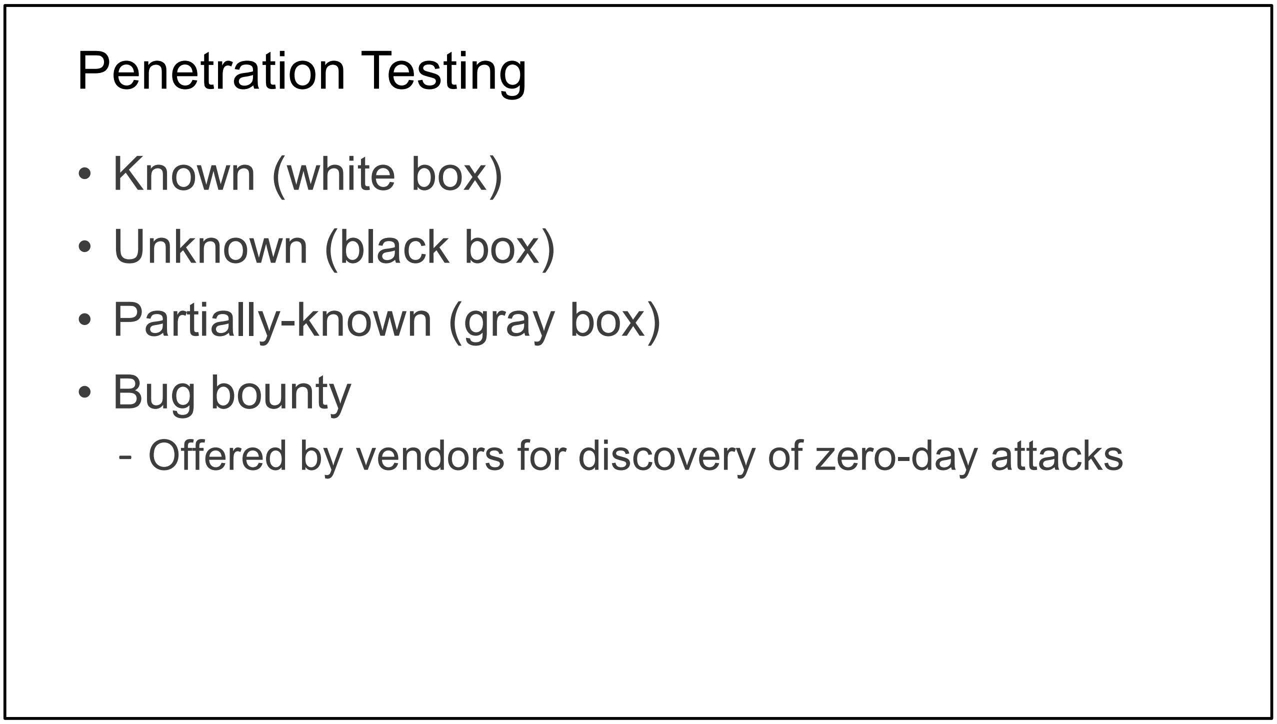
Episode title: **Penetration Testing**

Objective: **1.8 Explain the techniques used in penetration testing.**



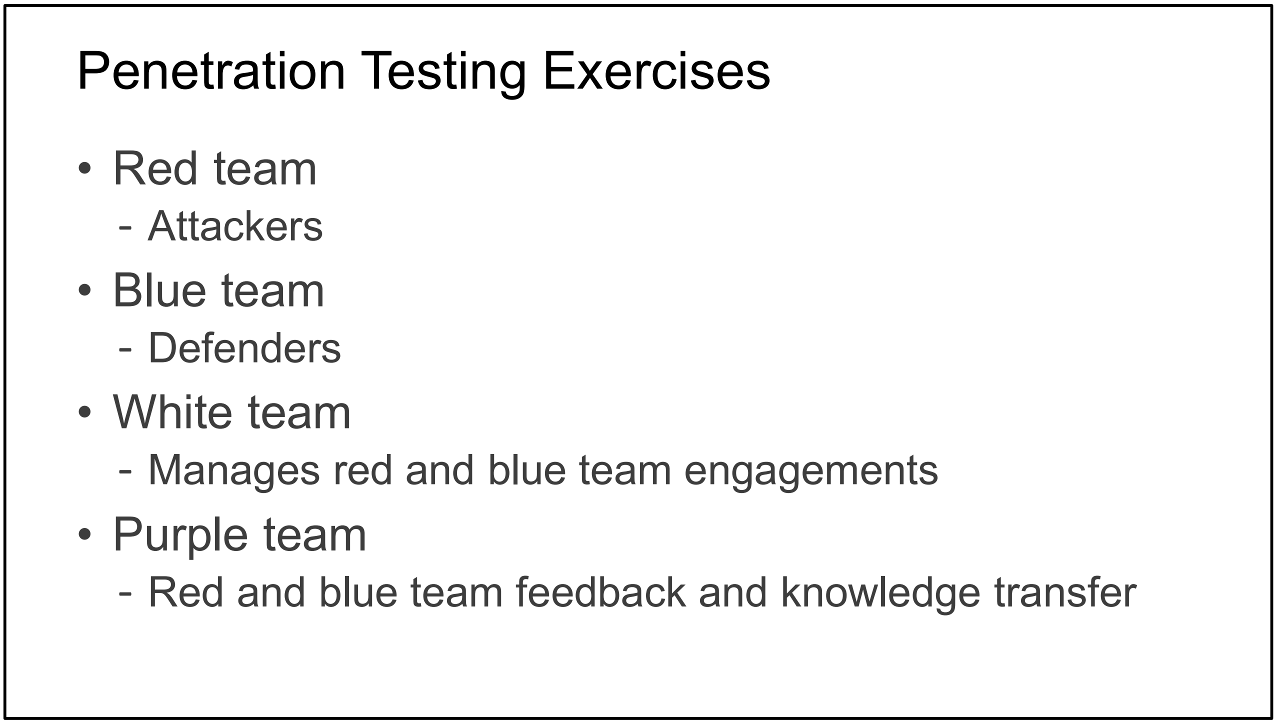
Penetration Testing

- Attempt to exploit vulnerabilities
- Invasive/active compared to vulnerability assessments
- Pen tester must sign non-disclosure agreement (NDA)
- Normally triggers IDS/IPS alerts



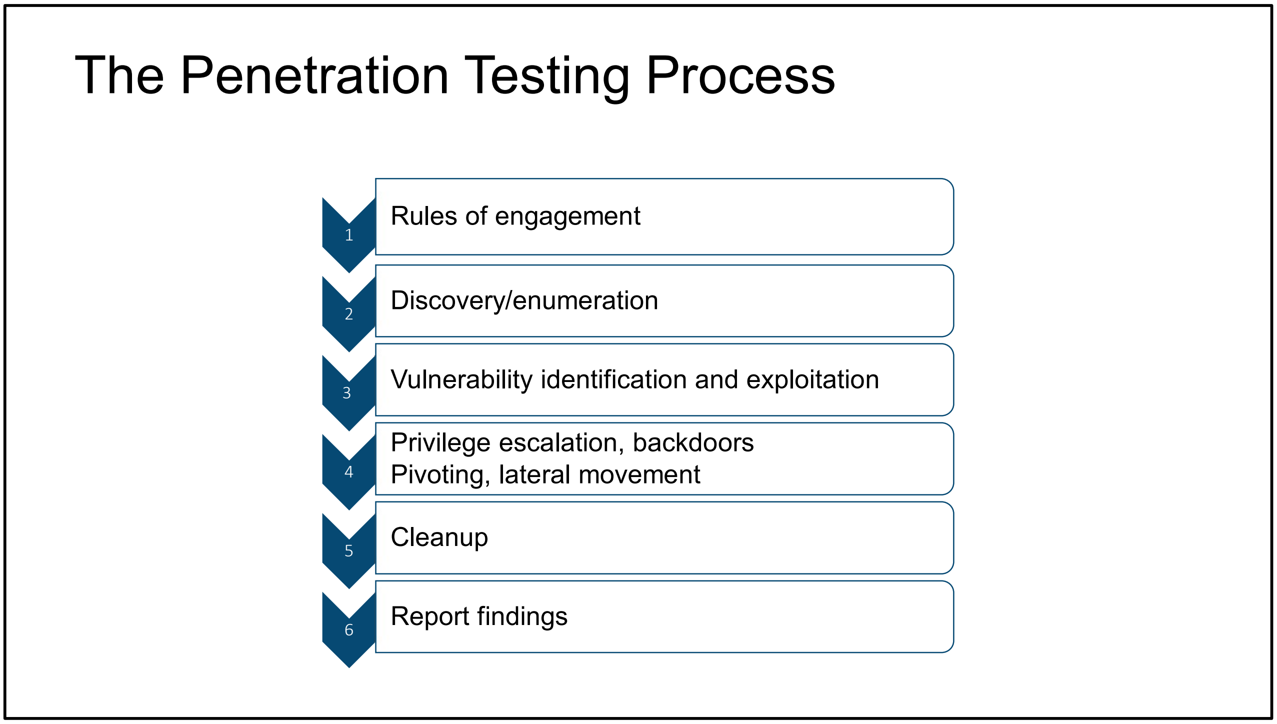
Penetration Testing

- Known (white box)
- Unknown (black box)
- Partially-known (gray box)
- Bug bounty
  - Offered by vendors for discovery of zero-day attacks



Penetration Testing Exercises

- Red team
  - Attackers
- Blue team
  - Defenders
- White team
  - Manages red and blue team engagements
- Purple team
  - Red and blue team feedback and knowledge transfer



The Penetration Testing Process

1 Rules of engagement

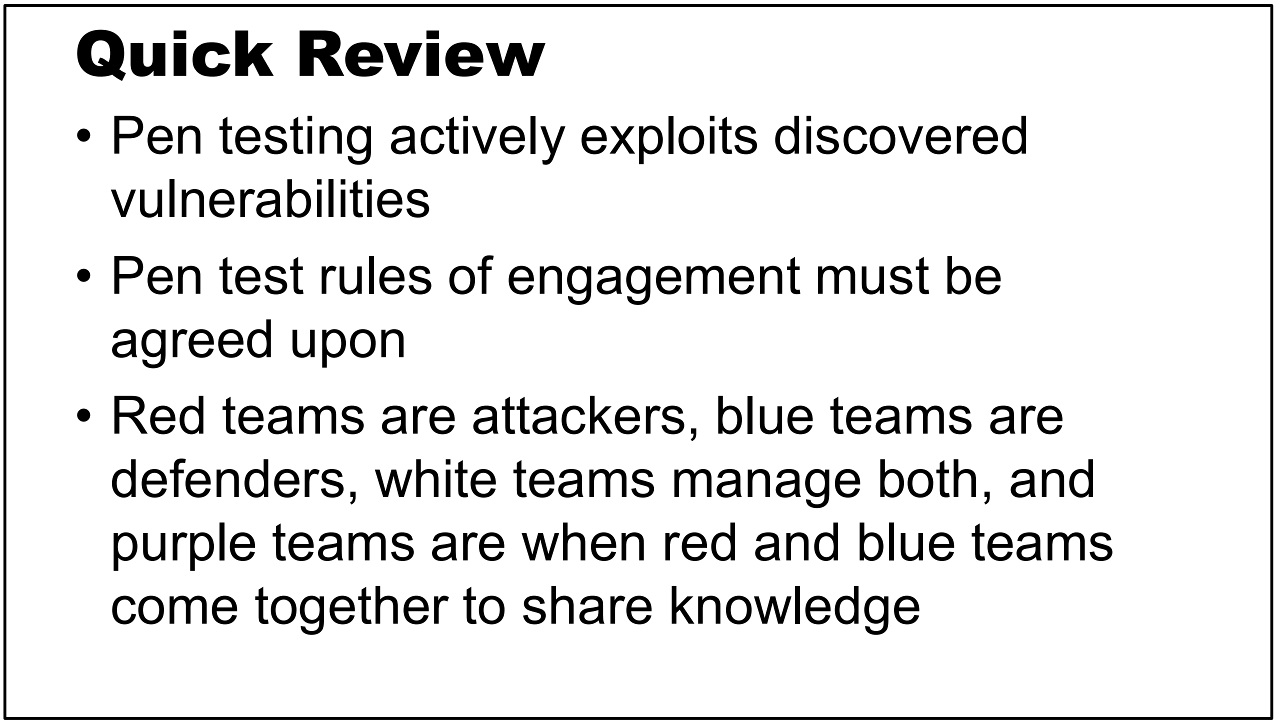
2 Discovery/enumeration

3 Vulnerability identification and exploitation

4 Privilege escalation, backdoors
Pivoting, lateral movement

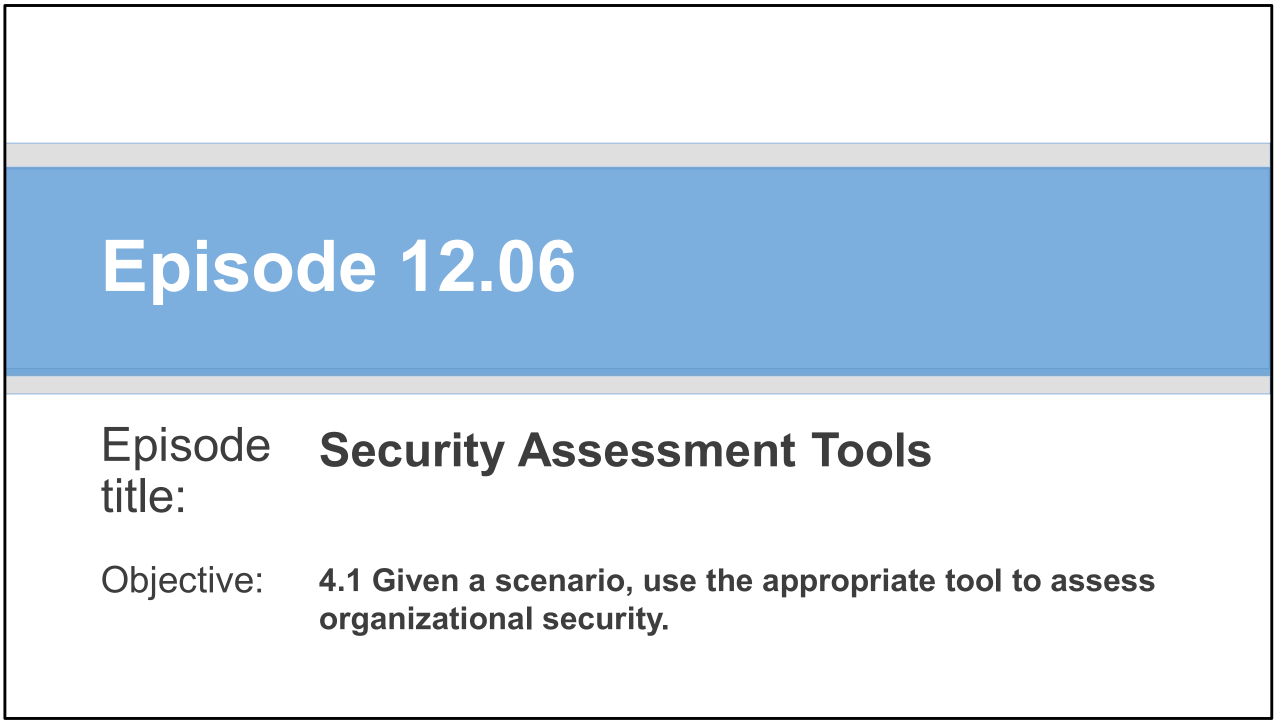
5 Cleanup

6 Report findings



Quick Review

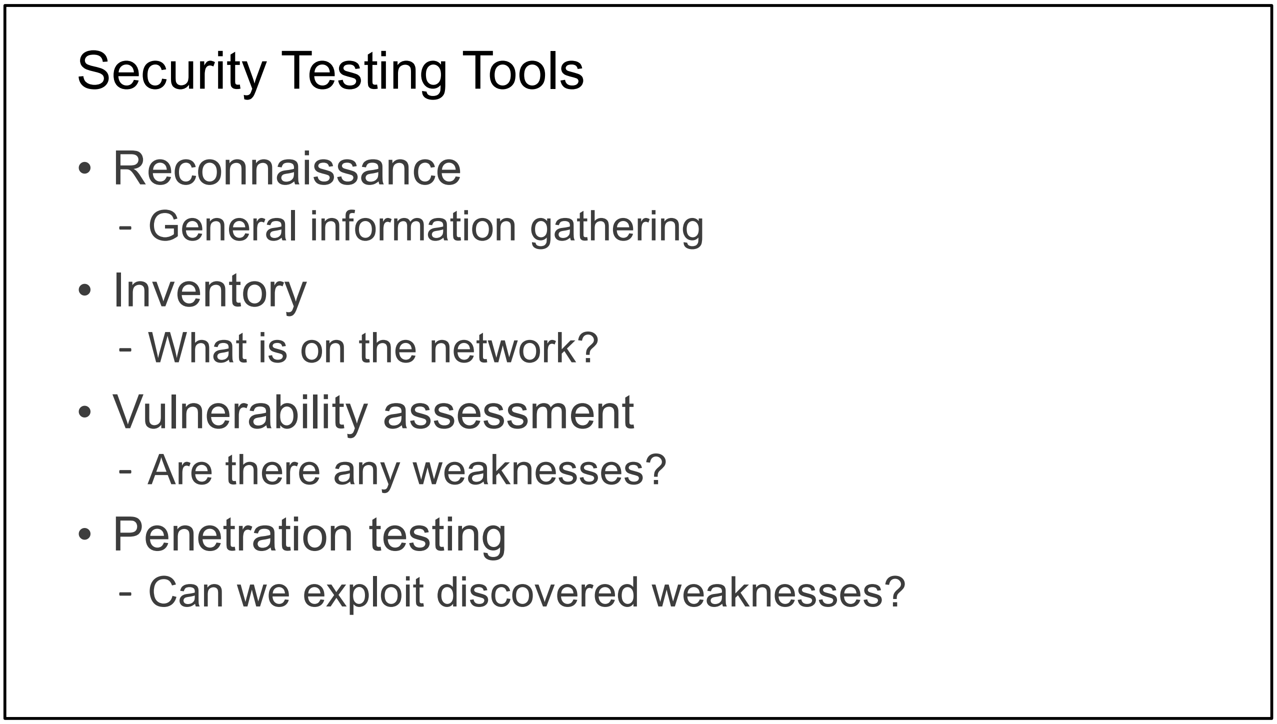
- Pen testing actively exploits discovered vulnerabilities
- Pen test rules of engagement must be agreed upon
- Red teams are attackers, blue teams are defenders, white teams manage both, and purple teams are when red and blue teams come together to share knowledge



Episode 12.06

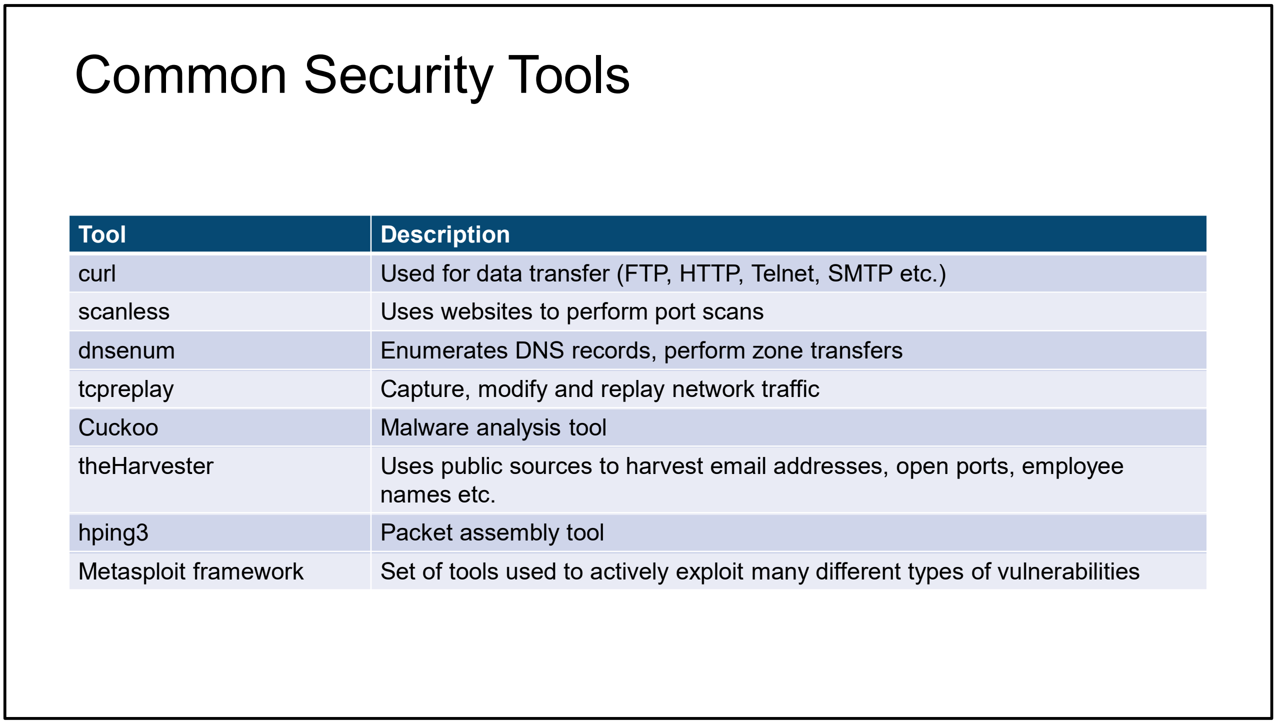
Episode title: **Security Assessment Tools**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**



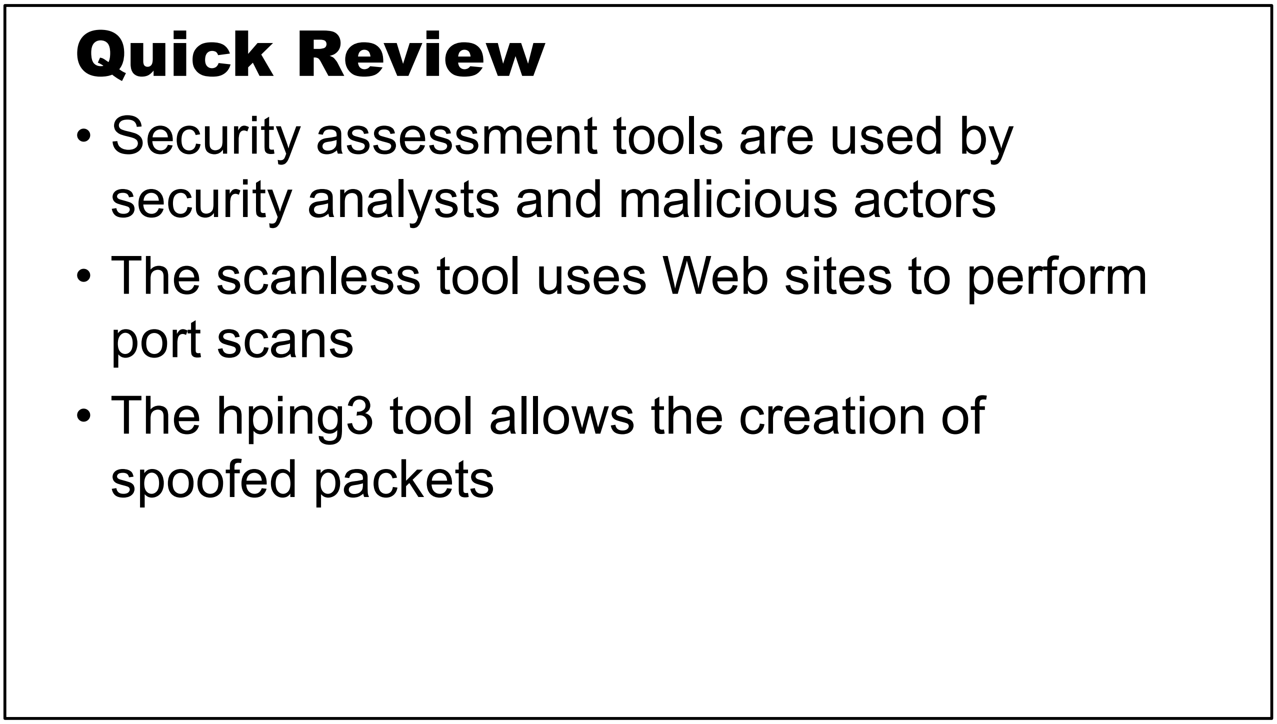
Security Testing Tools

- Reconnaissance
  - General information gathering
- Inventory
  - What is on the network?
- Vulnerability assessment
  - Are there any weaknesses?
- Penetration testing
  - Can we exploit discovered weaknesses?



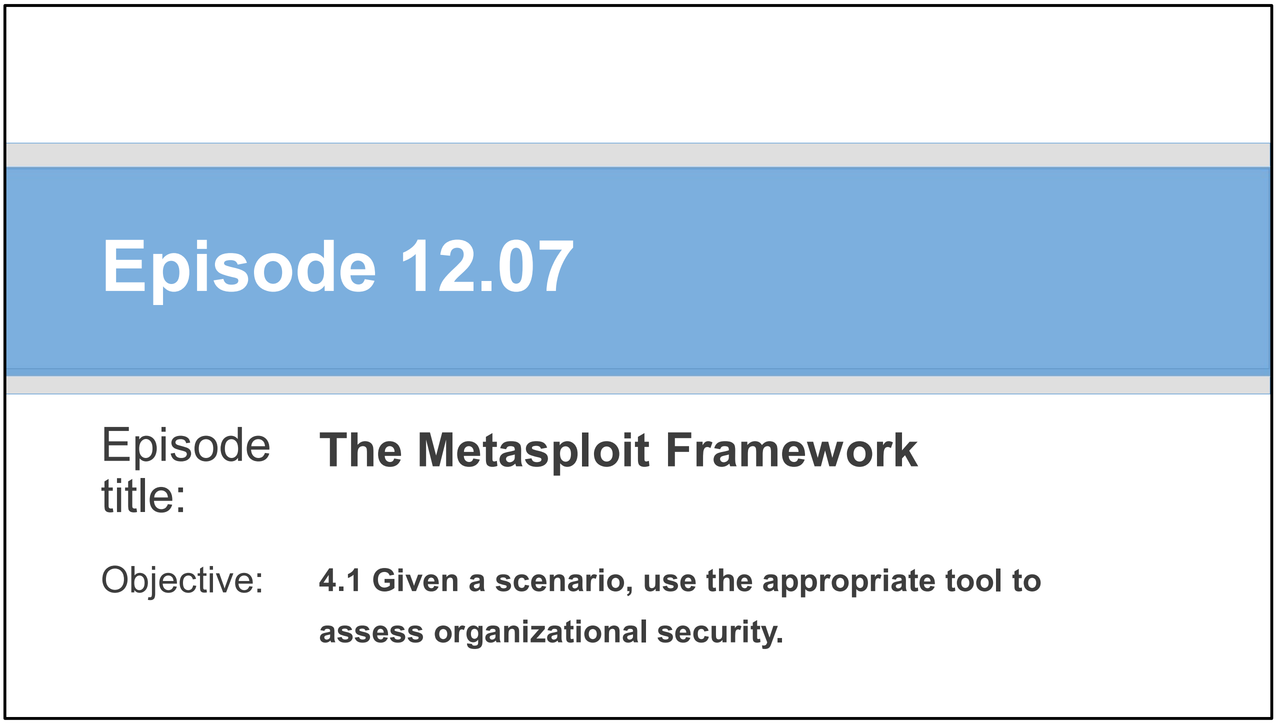
Common Security Tools

Tool	Description
curl	Used for data transfer (FTP, HTTP, Telnet, SMTP etc.)
scanless	Uses websites to perform port scans
dnsenum	Enumerates DNS records, perform zone transfers
tcpreplay	Capture, modify and replay network traffic
Cuckoo	Malware analysis tool
theHarvester	Uses public sources to harvest email addresses, open ports, employee names etc.
hping3	Packet assembly tool
Metasploit framework	Set of tools used to actively exploit many different types of vulnerabilities



Quick Review

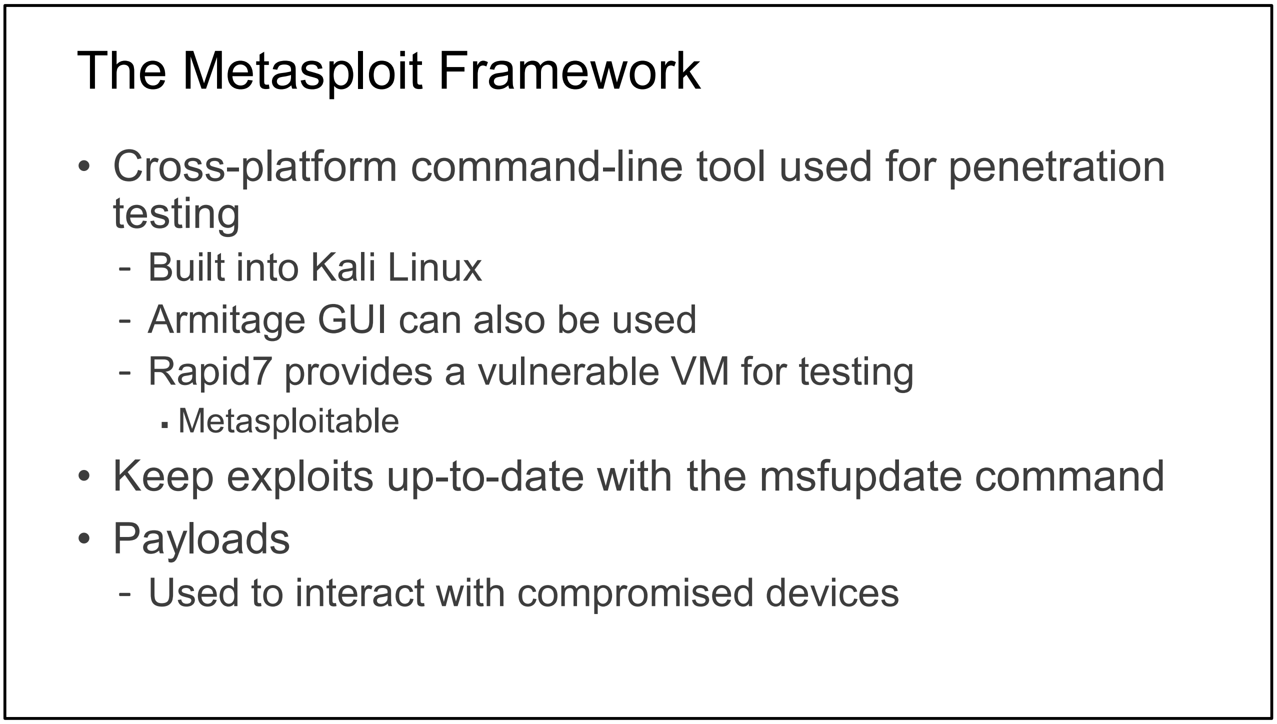
- Security assessment tools are used by security analysts and malicious actors
- The scanless tool uses Web sites to perform port scans
- The hping3 tool allows the creation of spoofed packets



Episode 12.07

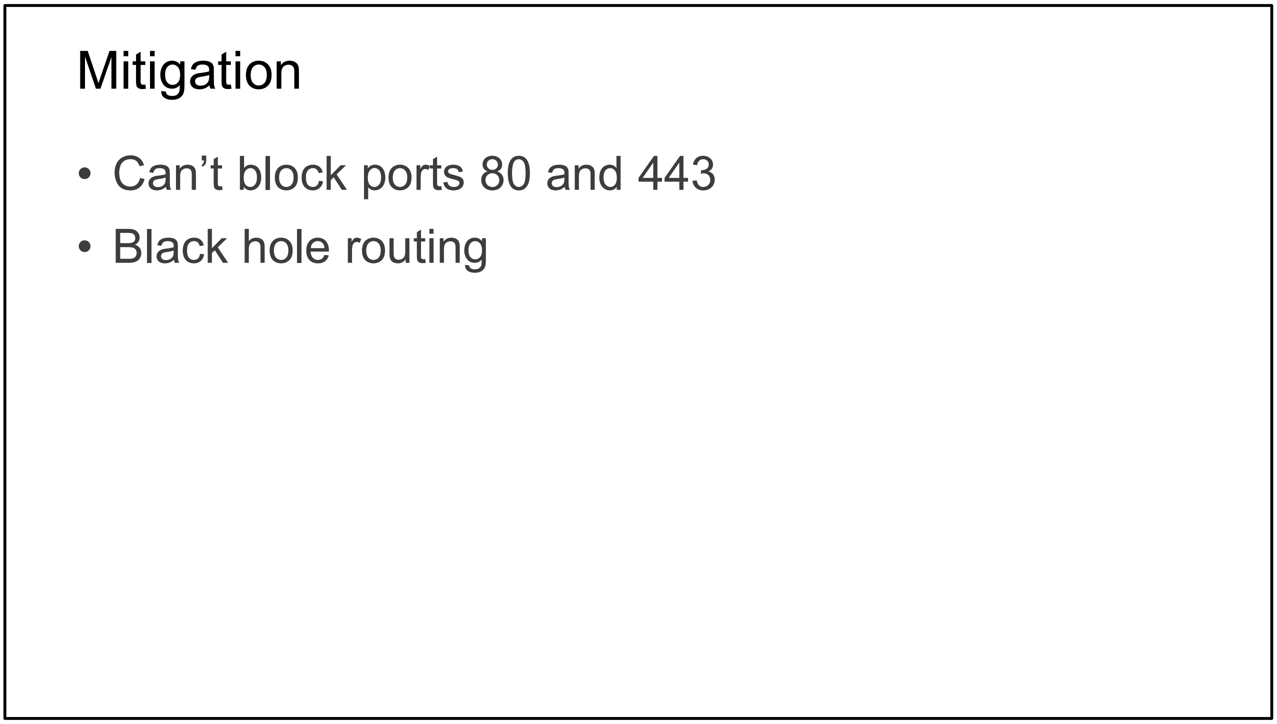
Episode title: **The Metasploit Framework**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**



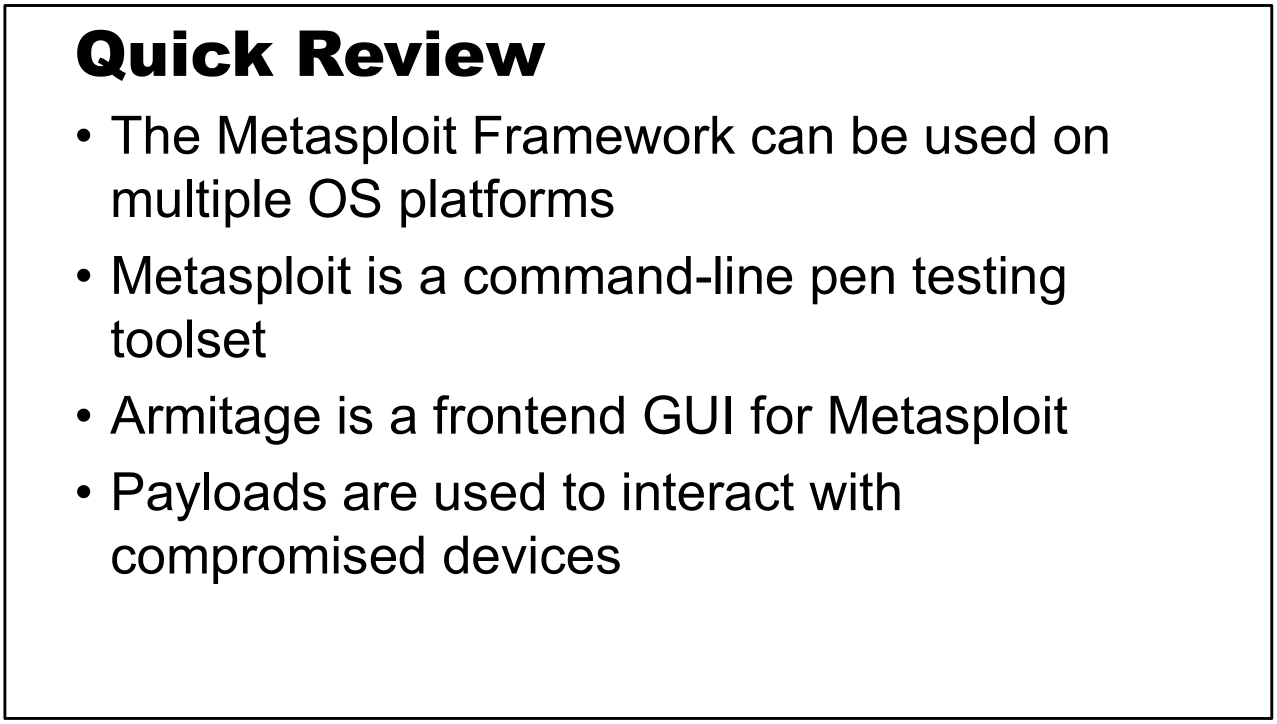
The Metasploit Framework

- Cross-platform command-line tool used for penetration testing
  - Built into Kali Linux
  - Armitage GUI can also be used
  - Rapid7 provides a vulnerable VM for testing
    - Metasploitable
- Keep exploits up-to-date with the msfupdate command
- Payloads
  - Used to interact with compromised devices



Mitigation

- Can’t block ports 80 and 443
- Black hole routing



Quick Review

- The Metasploit Framework can be used on multiple OS platforms
- Metasploit is a command-line pen testing toolset
- Armitage is a frontend GUI for Metasploit
- Payloads are used to interact with compromised devices