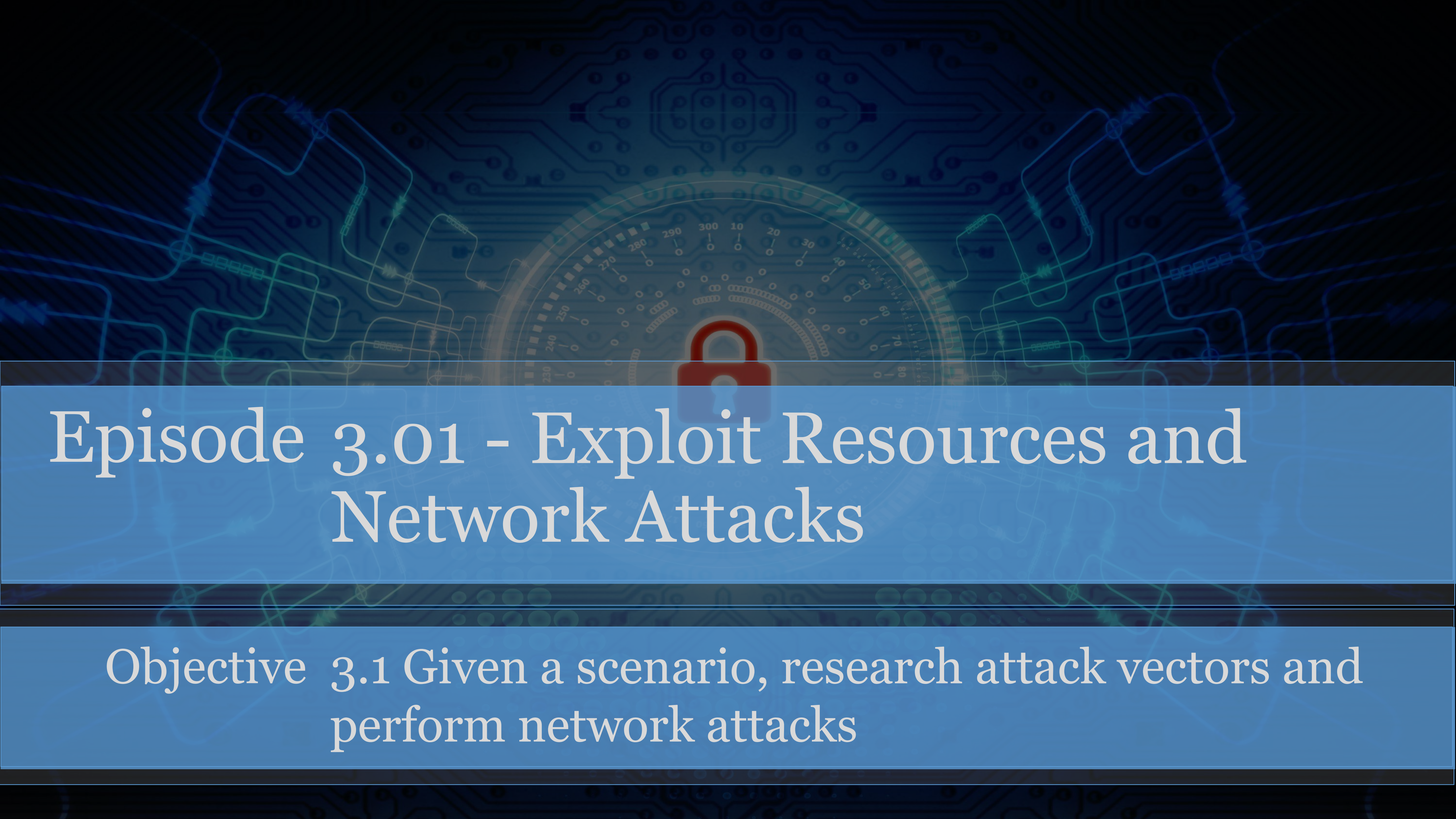
CHAPTER 3

Network-Based Attacks



Episode 3.01 - Exploit Resources and Network Attacks

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

EXPLOIT RESOURCES

- Exploit database (DB)
  - Maintained by Offensive Security
  - CVE compliant archive of public exploits
  - Useful for pentesters and security researchers
  - https://www.exploit-db.com/
- Packet storm
  - Global security resource
  - Purpose is to provide a current repository of security threat information
  - https://packetstormsecurity.com/

NETWORK ATTACKS

- Exploit chaining
  - Practice of combining exploits in a sequence that increases the probability of success
  - The idea is to incrementally compromise a system
  - For example, compromise admin passwords first, then use those passwords to access systems to carry out attacks using elevated privileges

NETWORK ATTACKS

- Password attacks
  - Password spraying
    - Attempt to use lists of insecure passwords against many accounts
  - Brute force
    - Trying all possible options to attempt to find a match
  - Dictionary
    - Attempting password alternative using a predefined list of known or weak passwords

QUICK REVIEW

- Multiple sources exist to search for exploits
- Attacks on networks focus on different ways to gain access

Episode 3.02 – Network-Based Exploits

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

NAME RESOLUTION EXPLOITS

- NETBIOS name service (NBNS)
  - Part of NetBIOS-over-TCP
  - Similar functionality to DNS
- LLMNR (Link-local Multicast Name Resolution)
  - Protocol based on DNS packet format
  - Allows IPv4 and IPv6 name resolution on the same local link
- DNS and ARP poisoning

NETWORK EXPLOITS

- SMB (Server Message Block) exploits
  - Protocol used in Windows to provide file and printer access, and remote service access
  - TCP ports 139 and 445
  - Some ransomware (EternalBlue, WannaCry) use SMB to propagate
- SNMP (Simple Network Management Protocol) exploits
  - Query and manage IP devices
  - Multiple versions - SNMPv1 is not secure

EVEN MORE NETWORK EXPLOITS

- SMTP (Simple Mail Transport Protocol) exploits
  - Standard protocol for transmitting email
  - Open relay, local relay, phishing, spam, etc.
- FTP (File Transfer Protocol) exploits
  - Overall insecure protocol for transferring files
  - No encryption for transfers and credentials
  - Easy for attackers to use for data exfiltration if FTP is available

QUICK REVIEW

- Successful redirection attacks can drive victim traffic to your chosen destination
- SMB is a popular target for propagating malware
- SNMP that is not secure can make many IP devices vulnerable
- FTP is often used to place malware and exploit tools

Episode 3.03 – FTP Exploit Demo

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

FTP EXPLOIT DEMO

- FTP demo exploit

QUICK REVIEW

- FTP can make placing malware on a victim easier
- FTP itself can be vulnerable
- In this example, FTP opened a backdoor to the victim's computer

Episode 3.04 – Man-in-the-Middle Exploits

Objective

3.1 Given a scenario, research attack vectors and perform network attacks

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

ADDITIONAL NETWORK EXPLOITS

- Man-in-the-middle
  - Family of attacks where the attacker intercepts messages between a sender and receiver
  - Attack may modify, regenerate, or forward intercepted messages

MAN-IN-THE-MIDDLE EXPLOITS

- ARP spoofing
  - Similar to DNS poisoning, but with local MAC addresses
- Pass the hash
  - Attacker intercepts an NTLM hash (user credential) and reuses it to appear as an authenticated user to Windows

MAN-IN-THE-MIDDLE EXPLOITS

- Replay
- Relay
- SSL (Secure Sockets Layer) stripping
- Downgrade

MAN-IN-THE-MIDDLE EXPLOITS

- DoS (Denial of Service)/stress test
- NAC (Network Access Control) bypass
- VLAN (Virtual Local Area Network) hopping

QUICK REVIEW

- MITM attacker intercepts all traffic between sender and receiver
- May be part of an attack chain
- Multiple MITM possibilities, including ARP spoofing, pass the hash, replay attack
- Useful to bypass normal network security controls

Episode 3.05 – Labtainers Lab (TCP/IP Attacks)

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

Lab Networking: tcpip

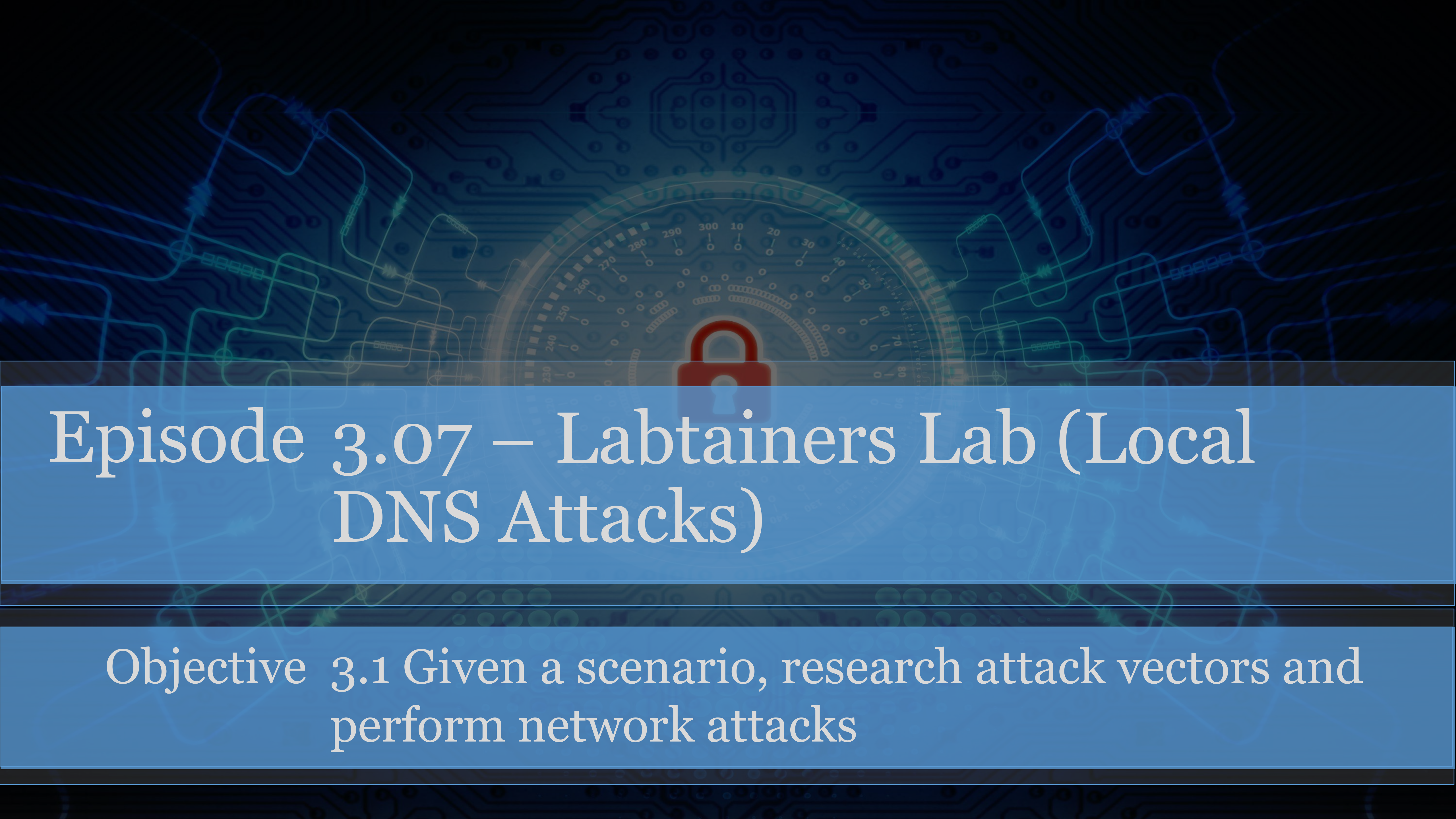
- Intro lab (TCP/IP attacks)

Episode 3.06 – Labtainers Lab (ARP Spoof Attack)

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

Lab Networking: arp-spoof

- Intro lab (arp-spoof attack)



Episode 3.07 – Labtainers Lab (Local DNS Attacks)

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

Lab Networking: local-dns

- Intro lab (Local DNS attacks)

Episode 3.08 – Labtainers Lab (MACs and Hash Functions)

Objective 3.1 Given a scenario, research attack vectors and perform network attacks

Lab Crypto Labs: macs-hash

- Intro lab (MACs and Hash functions)
- More exploration than attacks