CHAPTER 9

Post-Exploitation

Episode 9.01 - Post-Exploitation Techniques

Objective 3.7 Given a scenario, perform post-exploitation techniques

POST-EXPLOITATION TECHNIQUES

- What to do once you're in
  - Make it easier next time
- Lateral movement
  - RPC/DCOM (Remote Procedure Call / Distributed Component Object Model)
    - PsExec – Utility that supports executing processes on other systems (i.e. telnet)
    - WMI (Windows Management Instrumentation) – Managing devices and applications from remote computers
    - Scheduled tasks

LATERAL MOVEMENT

- PS remoting/WinRM
  - PowerShell remoting/Windows Remote Management
- SMB (Server Message Block)
  - Protocol for exposing shares to remote computers (Linux, etc. too)
- RDP (Remote Desktop Protocol)
  - Ability to access a desktop from a remote computer
- Apple Remote Desktop
  - Apple's RDP

LATERAL MOVEMENT

- VNC (Virtual Network Computing)
- X-server forwarding
  - X-windows access to Linux desktop
- Telnet
  - Unsecure remote access (everything in cleartext)
- SSH (Secure Shell)
  - More secure remote access to shell
- RSH/Rlogin (Remote Shell / Remote login)
  - Legacy secure remote access

QUICK REVIEW

- Don't reinvent the wheel each time - once you're in, make it easier next time
- Enable remote access if possible
- Use remote access to move laterally within a network

Episode 9.02 - Post-Exploitation Tools

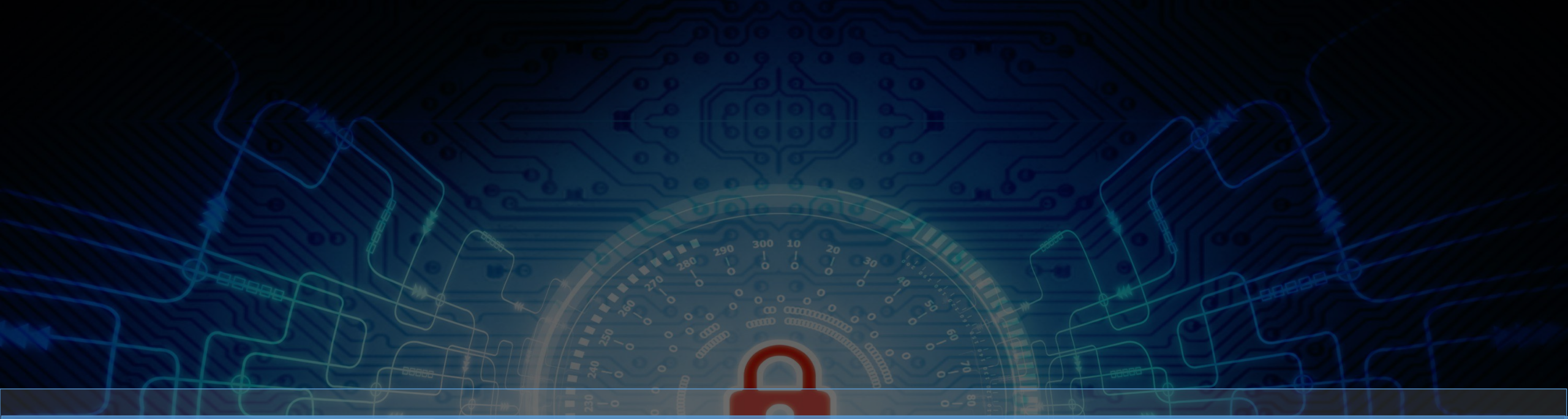
Objective 3.7 Given a scenario, perform post-exploitation techniques

POST-EXPLOITATION TOOLS

- Empire (4.2.12.5)
  - https://alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/
- Mimikatz (4.2.2.7)
  - https://github.com/ParrotSec/mimikatz
- Bloodhound
  - https://bloodhound.readthedocs.io/en/latest/

QUICK REVIEW

- Post-exploitation allows an attacker to linger and prolong an attack
- Popular post-exploitation tools include Empire, Mimikatz, and Bloodhound



Episode 9.03 - Network Segmentation Testing

Objective 3.7 Given a scenario, perform post-exploitation techniques

NETWORK SEGMENTATION TESTING

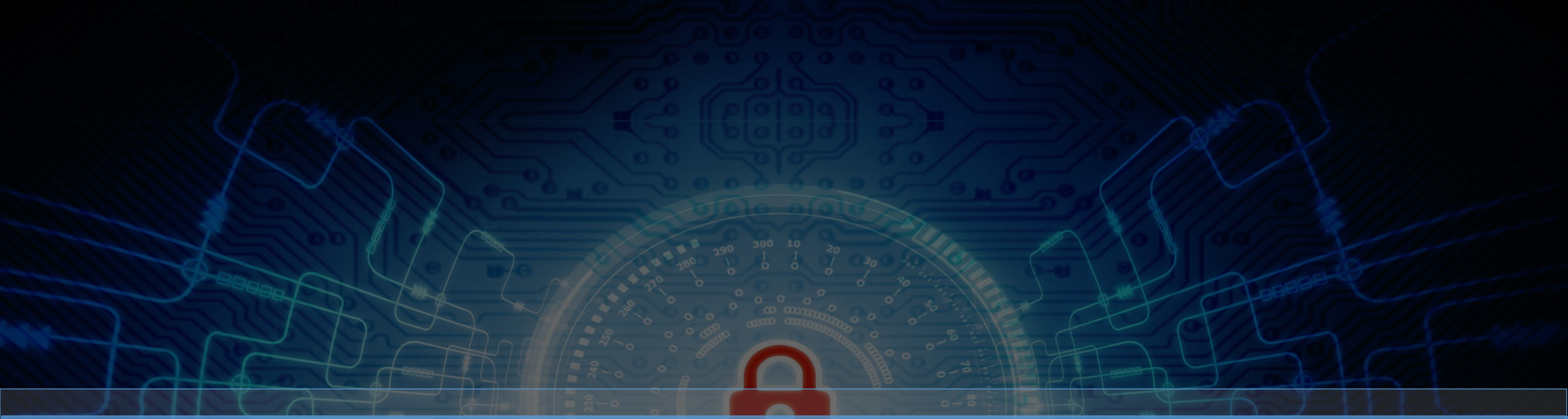
- Tests to confirm that network segments work as designed
  - Only approved traffic flows between segments
  - No gaps exist that attackers can exploit
- Involves scanning and carrying out a vulnerability assessment on each network segment

NETWORK SEGMENTATION TESTING

- Strategy
  - ICMP scan
  - TCP scan
  - UDP scan

QUICK REVIEW

- Network segmentation ensures that unauthorized traffic does not flow outside authorized segments or zones
- Scans should not be allowed to transcend segments
- Testing for proper segmentation should include ICMP, TCP, and UDP scans



Episode 9.04 - Persistence and Stealth

Objective 3.7 Given a scenario, perform post-exploitation techniques

PERSISTENCE

- Scheduled jobs
  - Cron or Task Manager
- Scheduled task
  - Same as above
- Daemons
  - Background processes or services

PERSISTENCE

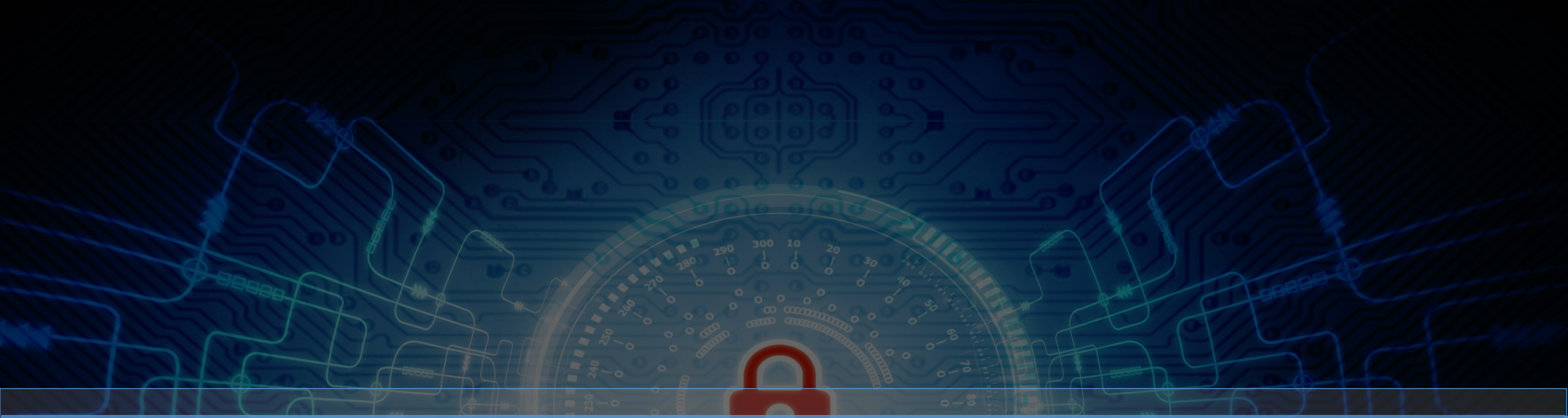
- Back doors
  - Bypass standard security controls
- Trojan
  - Malware that looks like it does something useful
- New user creation
  - Makes later logins easier

STEALTH

- Clean up files, including tools installed
- Hiding files that you need to leave
- Sanitize log files (remove entries or entire logs)
- Remove any traces of activity while accessing the environment

QUICK REVIEW

- Set up persistent processes to maintain a presence
- Install low profile tools and malware to make your job easier
- Leave artifacts that keep the attack going and make it easier to get back in
- Once the attack is over, clean up to avoid post-mortem detection



Episode 9.05 - Detection Avoidance Techniques

Objective 3.7 Given a scenario, perform post-exploitation techniques

DETECTION AVOIDANCE

- Living-off-the-land techniques/fileless malware
  - PsExec – Lightweight telnet replacement from Microsoft
    - Supports launching remote interactive command prompts
  - Windows Management Instrumentation (WMI)
    - Extensions that provide OS interface capability
  - PowerShell (PS) remoting and Windows Remote Management (WinRM)

DETECTION AVOIDANCE

- Data exfiltration
- Covering your tracks
- Steganography
- Establishing a covert channel

QUICK REVIEW

- Avoiding detection allows attackers to do more damage
- A key to detection avoidance is fooling tools and controls that detect malicious activity
- Removing activity from log files is a common tactic