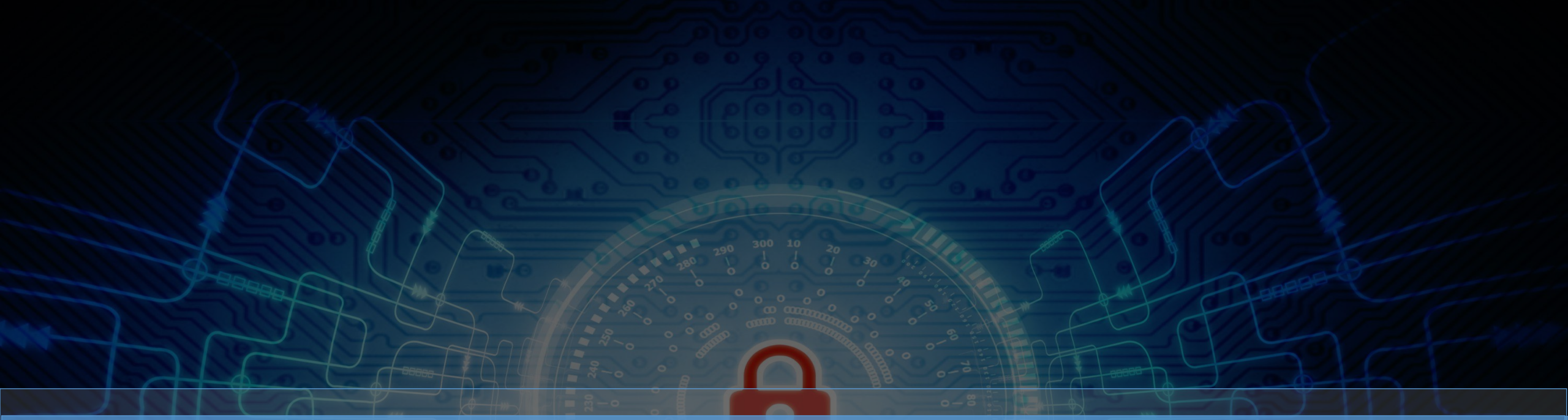
CHAPTER 12

Tools and Programming



Episode 12.01 - Pen Testing Toolbox

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

RECONNAISSANCE

- For reconnaissance, use:
  - Nmap
  - Whois
  - Nslookup
  - Theharvester
  - Shodan
  - Recon-NG
  - Censys
  - Aircrack-NG
  - Kismet
  - WiFite
  - SET
  - Wireshark
  - Hping
  - Metasploit framework

ENUMERATION

- To list targets, use:
  - Nmap
  - Nslookup
  - Wireshark
  - Hping

VULNERABILITY SCANNING

- To scan for vulnerabilities, use:
  - Nmap
  - Nikto
  - OpenVAS
  - SQLmap
  - Nessus
  - W3AF
  - OWASP ZAP
  - Metasploit framework

CREDENTIAL ATTACKS

- For offline password cracking, use:
  - Hashcat
  - John the Ripper
  - Cain and Abel
  - Mimikatz
  - Aircrack-NG

CREDENTIAL ATTACKS

- For brute-forcing services, use:
  - SQLmap
  - Medusa
  - Hydra
  - Cain and Abel
  - Mimikatz
  - Patator
  - W3AF
  - Aircrack-NG

PERSISTENCE

- Once you have exploited a target, use these to make sure you can get back in:
  - SET
  - BeEF
  - SSH
  - NCAT
  - NETCAT
  - Drozer
  - Powersploit
  - Empire
  - Metasploit framework

CONFIGURATION COMPLIANCE

- To evaluate a configuration to determine if it's compliant with a standard or regulation, use:
  - Nmap
  - Nikto
  - OpenVAS
  - SQLmap
  - Nessus

EVASION

- To evade detection, use:
  - SET
  - Proxychains
  - Metasploit framework

DECOMPILATION

- To decompile executables, use:
  - Immunity debugger
  - APKX
  - APK studio

PENETRATION TESTING USE CASES

- Forensics
  - To carry out digital forensics, use:
    - Immunity debugger
- Debugging
  - To debug code, use:
    - OLLYDBG
    - Immunity debugger
    - GDB
    - WinDBG
    - IDA

SOFTWARE ASSURANCE

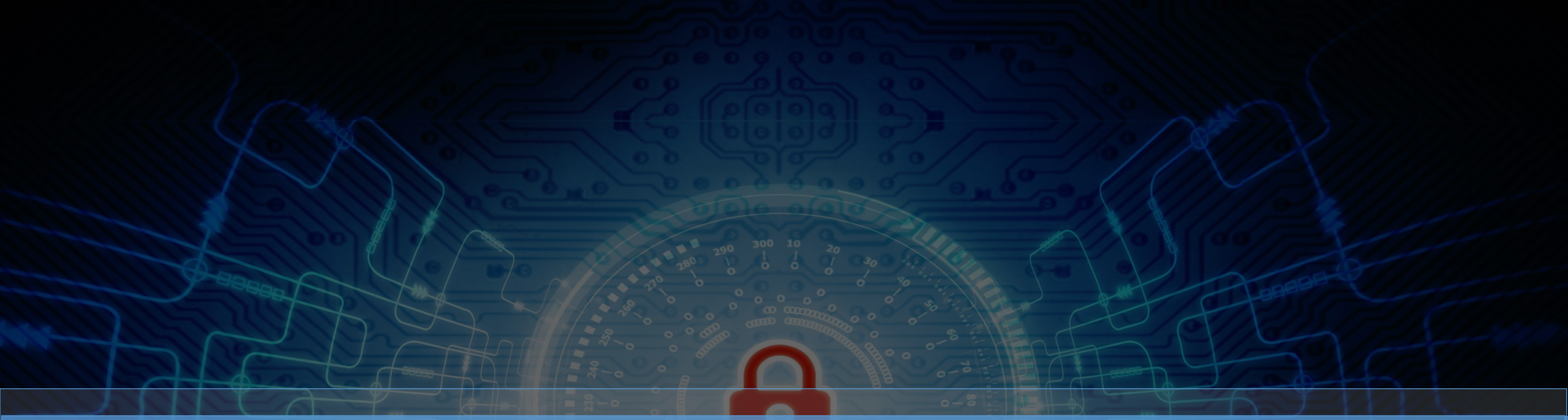
- For general software assurance, use:
  - Findsecbugs
  - SonarQube
  - YASCA
- For fuzzing, use:
  - Peach
  - AFL

PENETRATION TESTING USE CASES

- Forensics – Immunity debugger
- Debugging – OLLYDBG, Immunity debugger, GDB, WinDBG, IDA
- Software assurance – Findsecbugs, SonarQube, YASCA
  - Fuzzing – Peach, AFL
  - SAST (Static Application Security Testing)
  - DAST (Dynamic Application Security Testing)

QUICK REVIEW

- Know what each of the tools listed in the objectives are commonly used for
- Some tools, such as nmap, can fit into multiple use cases
- It’s more important to understand the purpose of a tool than to memorize categories



Episode 12.02 - Using Kali Linux

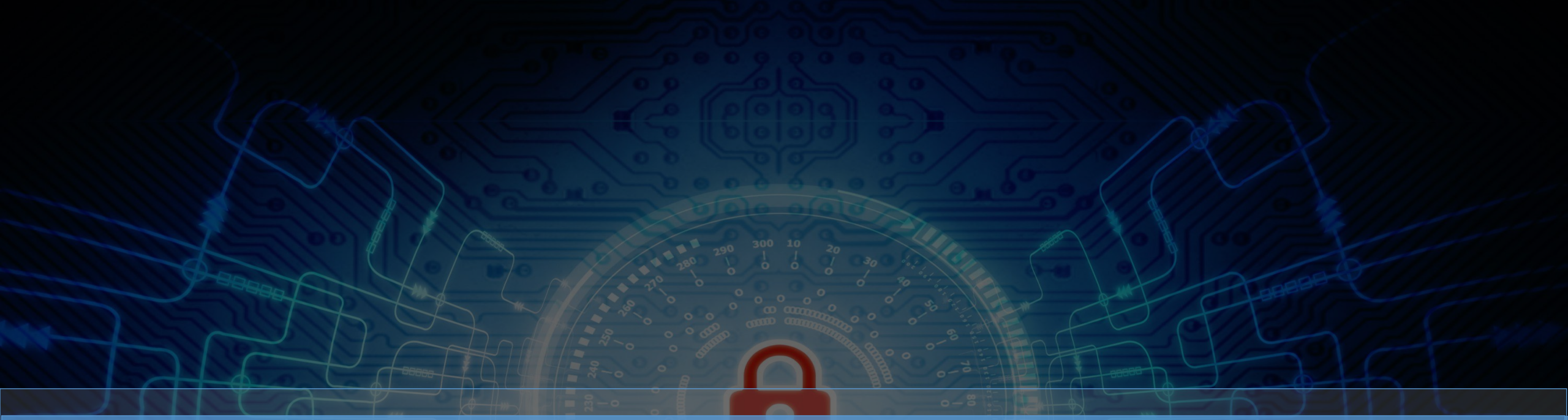
Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

KALI LINUX DEMO

- Kali Linux demo

QUICK REVIEW

- Kali Linux is only one open source Linux distribution targeted at penetration testing
- Don't limit a pen testing toolbox to just Kali Linux
- Briefly launch each tool in Kali Linux listed in the exam objectives to explore their uses
- Remember that knowing Kali Linux is not a PenTest+ objective



Episode 12.03 - Scanners and Credential Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

SCANNERS

Tool	Notes	URL
Nikto	Web server vulnerability scanner	https://github.com/sullo/nikto
OpenVAS (Open Vulnerability Assessment System)	Open Source vulnerability scanner and manager	https://www.openvas.org/
SQLmap (Structured Query Language)	Automatic SQL injection and database takeover tool	https://sqlmap.org/
Nessus	Commercial vulnerability scanner (free for non-professional use)	https://www.tenable.com/products/nessus/nessus-professional

CREDENTIAL TESTING TOOLS

Tool	Category	Notes	URL
Hashcat	Offline	Advanced password recovery (world's fastest)	https://hashcat.net/hashcat/
Medusa	Online	Parallel network login auditor	https://foofus.net/goons/jmk/medusa/medusa.html
Hydra	Online	Parallelized login cracker	https://sectools.org/tool/hydra/
Cewl		Custom wordlist generator	https://digi.ninja/projects/cewl.php
John the Ripper	Offline	Password cracker	https://www.openwall.com/john/

CREDENTIAL TESTING TOOLS

Tool	Category	Notes	URL
Cain and Abel	Online/offline	Windows password recovery tool	https://www.oxid.it/cain.html
Mimikatz	Online/offline	A little tool to play with Windows security	https://github.com/gentilkiwi/mimikatz
Patator	Online	Multi-purpose brute-forcer	https://github.com/lanjelot/patator
Dirbuster		Multi-threaded app to brute force directories and file names on web servers	https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
W3AF	Online	Web Application Attack and Audit framework	https://w3af.org/

Analyze tool output

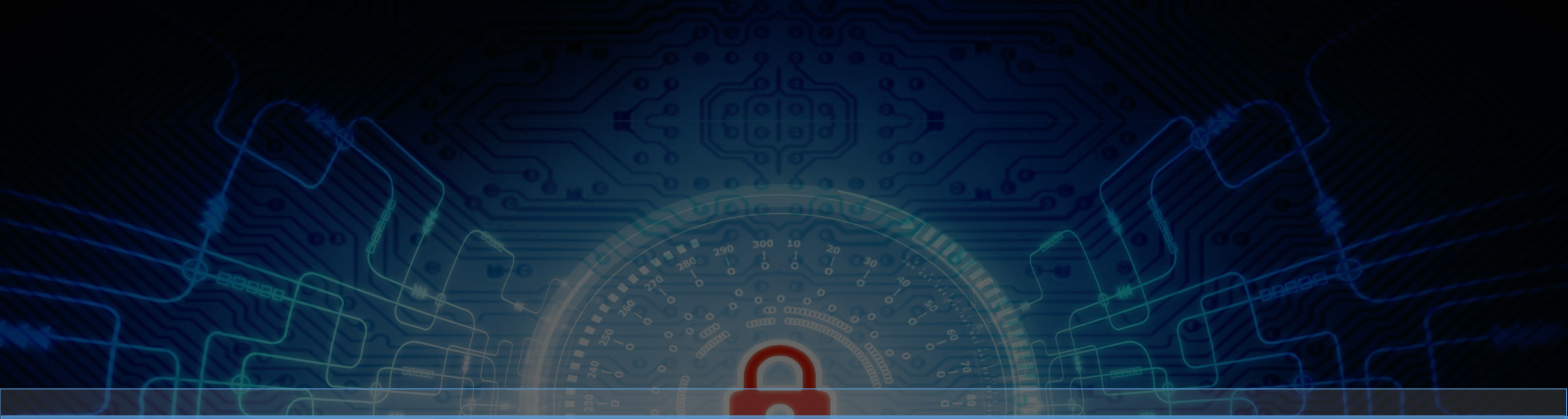
- Password cracking – demo John the Ripper

Analyze tool output

- Pass the hash – demo Mimikatz

QUICK REVIEW

- Scanners are "meta" tools that provide several levels of output
- Scanners are powerful, but very noisy and using them risks being detected
- Credential cracking tools run either in online or offline modes
- Effective dictionary attacks depend on good user/password lists



Episode 12.04 - Code Cracking Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

DEBUGGERS

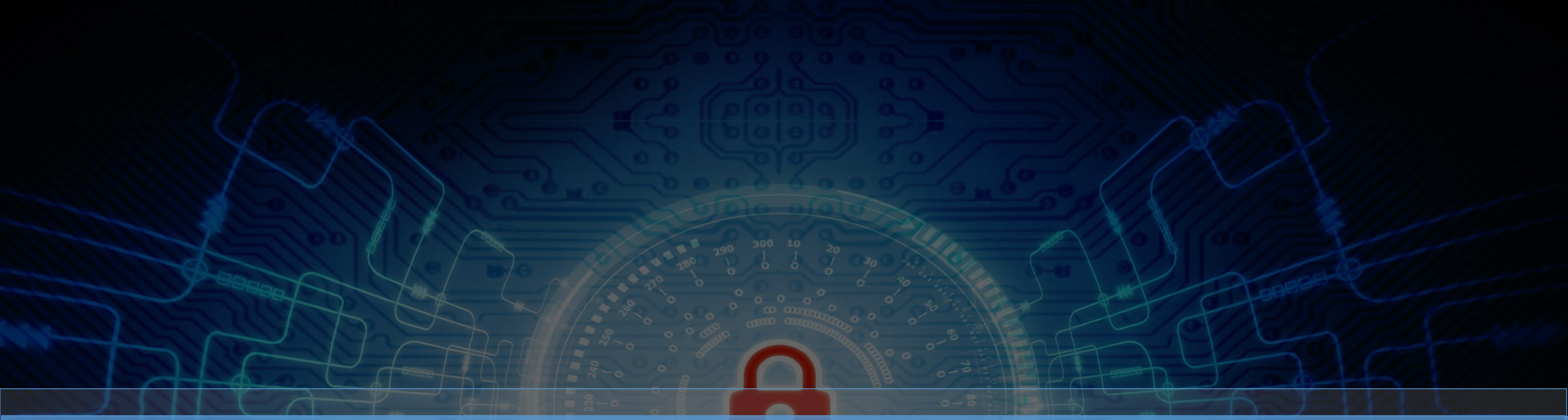
Tool	Notes	URL
OLLYDBG	Windows 32-bit	https://www.ollydbg.de/
Immunity debugger	Write exploits, analyze malware, and reverse engineer binary files	https://www.immunityinc.com/products/debugger/
GDB	GNU project debugger	https://www.gnu.org/software/gdb/
WinDBG	Windows debugger	https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
IDA	Cross platform debugger	https://www.hex-rays.com/products/ida/debugger/index.shtml

SOFTWARE ASSURANCE TOOLS

Tool	Notes	URL
Findbugs/findsecbugs	Auditor of Java web applications	https://find-sec-bugs.github.io/
Peach	Fuzzer – automated testing	https://www.peach.tech/products/peach-fuzzer/
AFL	American Fuzzy Lop - fuzzer	https://lcamtuf.coredump.cx/afl/
SonarQube	Continuous inspection – automated testing	https://www.sonarqube.org/
YASCA	Yet Another Source Code Analyzer	https://github.com/scovetta/yasca

QUICK REVIEW

- Debuggers are advanced tools and can reveal how a program works
- Debuggers can also allow testers to modify data as the program is running
- Software assurance tools can help to identify vulnerabilities in applications



Episode 12.05 – Open-Source Research Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

OPEN SOURCE INTELLIGENCE (OSINT) TOOLS

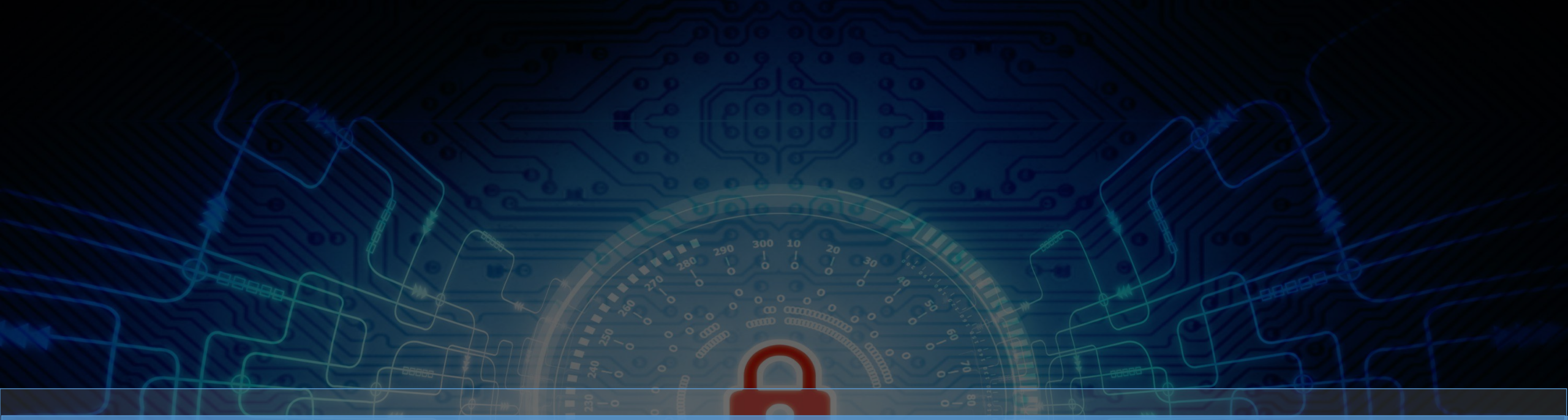
Tool	Notes	URL
Whois	Domain details (contacts, name servers, etc.)	https://whois.icann.org/en (and many more)
Nslookup	DNS information	Installed or available on most OSs
Foca	Fingerprint Organizations with Collected Archives – finds document metadata	https://github.com/ElevenPaths/FOCA
Theharvester	Gathers info from many sources (email, hosts, open ports, etc.)	https://github.com/laramies/theHarvester
Shodan	Finds Internet connected devices	https://www.shodan.io/
Maltego	Data mining for investigations	https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php
Recon-NG	Web reconnaissance	https://bitbucket.org/LaNMaSteR53/recon-ng
Censys	Finds Internet connected devices	https://censys.io/

ANALYZE TOOL OUTPUT

- Whois demo
- Nslookup demo

QUICK REVIEW

- OSINT data can help fill in information gaps
- Some information is not based on IP addresses or domain names
- Be creative when exploring attack vectors for targets
- Targets can be devices, people, user accounts, and even facilities



Episode 12.06 – Wireless and Web Pen Testing Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

WIRELESS TOOLS

Tool	Notes	URL
Aircrack-NG	Monitoring, attacking, testing, cracking	https://www.aircrack-ng.org/
Kismet	Wireless detector, sniffer and intrusion detection system	https://www.kismetwireless.net/
WiFite	Wrapper for other wireless tools (current version is WiFite2)	https://github.com/derv82/wifite2

WEB PROXIES AND SOCIAL ENGINEERING TOOLS

Web proxies

Tool	Notes	URL
OWASP ZAP	Zed Attack Proxy – Web application security scanner	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
Burp Suite	Graphical tool for testing web application security	https://portswigger.net/burp

Social engineering tools

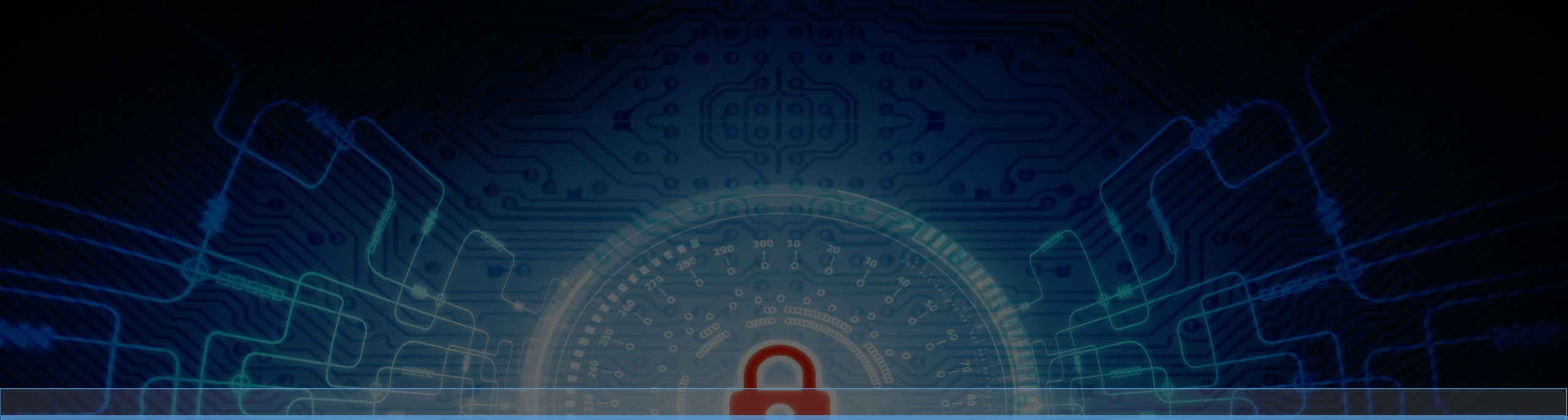
Tool	Notes	URL
SET	Social Engineering Toolkit – penetration testing using social engineering	https://www.trustedsec.com/social-engineer-toolkit-set/
BeEF	Browser Exploitation Framework – focus is on web browser	http://beefproject.com/

ANALYZE TOOL OUTPUT

- Proxying a connection - demo

QUICK REVIEW

- Wireless attackers can intercept traffic easier than wired network traffic
- The rapid IoT (Internet of Things) growth has resulted in lots of unsecure wireless devices
- Web applications are often fertile grounds for finding vulnerabilities



Episode 12.07 – Remote Access Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

REMOTE ACCESS TOOLS

Tool	Notes	URL
SSH	Secure shell	Included or available in most OSs
NCAT	Similar to nc, but from Nmap developers	https://nmap.org/ncat/
NETCAT	Same as nc	Included or available in most OSs
Proxychains	Forces TCP connections through a proxy	https://github.com/haad/proxychains

ANALYZE TOOL OUTPUT

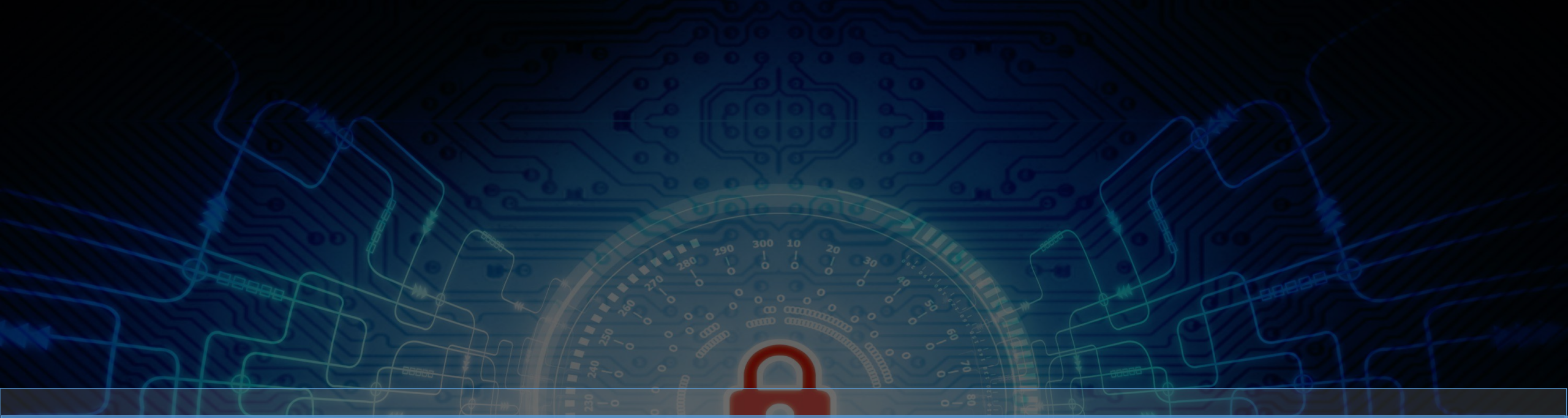
- Setting up a bind shell - demo

ANALYZE TOOL OUTPUT

- Getting a reverse shell - demo

QUICK REVIEW

- There are multiple ways to leverage remote connections
- The PenTest+ exam focuses on command-line tools for remote access
- Remote access is often followed by privilege escalation attacks and/or preceded by credential attacks



Episode 12.08 – Analyzers and Mobile Pen Testing Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

NETWORKING AND MOBILE TOOLS

Networking Tools

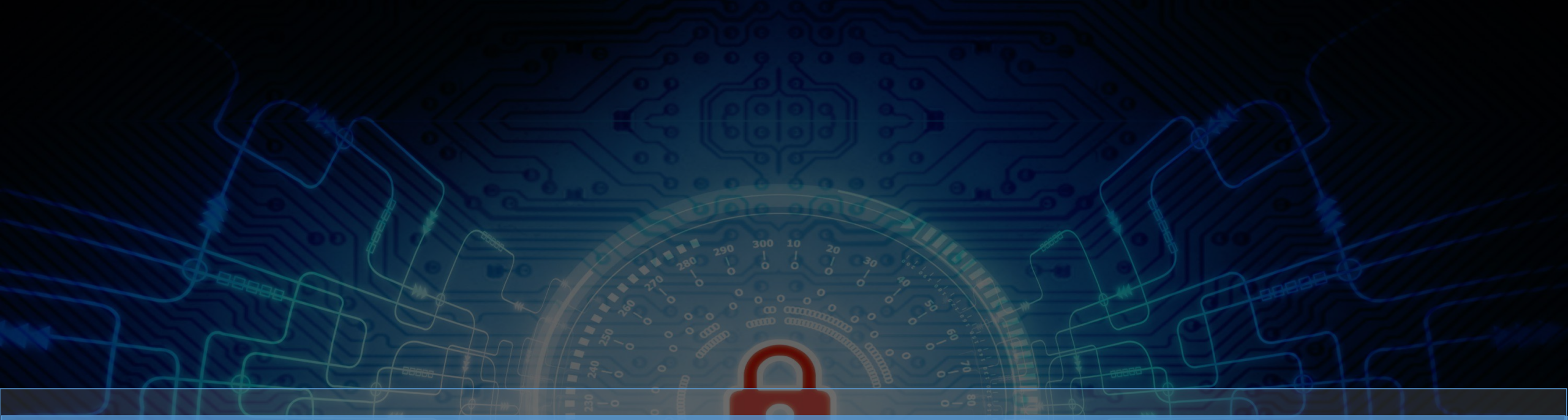
Tool	Notes	URL
Wireshark	Packet sniffer/protocol analyzer	https://www.wireshark.org/
Hping	Packet assembler/analyzer	https://www.hping.org/

Mobile Tools

Tool	Notes	URL
Drozer	Android security and attack framework	https://labs.mwrinfosecurity.com/tools/drozer/
APKX	Android APK decompiler	https://github.com/b-mueller/apkx
APK Studio	Android app decompiler	https://vaibhavpandey.com/apkstudio/

QUICK REVIEW

- Sniffers show the contents of network packets (may be encrypted)
- Some tools allow packets to be changed before sending them to the recipient
- A proxy allows testers to launch man-in-the-middle exploits



Episode 12.09 – Other Pen Testing Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

MISCELLANEOUS TOOLS

Tool	Notes	URL
Searchsploit	Search tool for exploit database	https://www.exploit-db.com/searchsploit/
Powersploit	Post-exploitation framework (MS PowerShell)	https://github.com/PowerShellMafia/PowerSploit
Responder	Microsoft network poisoner	https://github.com/SpiderLabs/Responder
Impacket	Python classes for working with network protocols	https://github.com/CoreSecurity/impacket
Empire	PowerShell/Python post-exploitation agent	https://github.com/EmpireProject/Empire
Metasploit framework	Comprehensive penetration testing framework	https://www.metasploit.com/

QUICK REVIEW

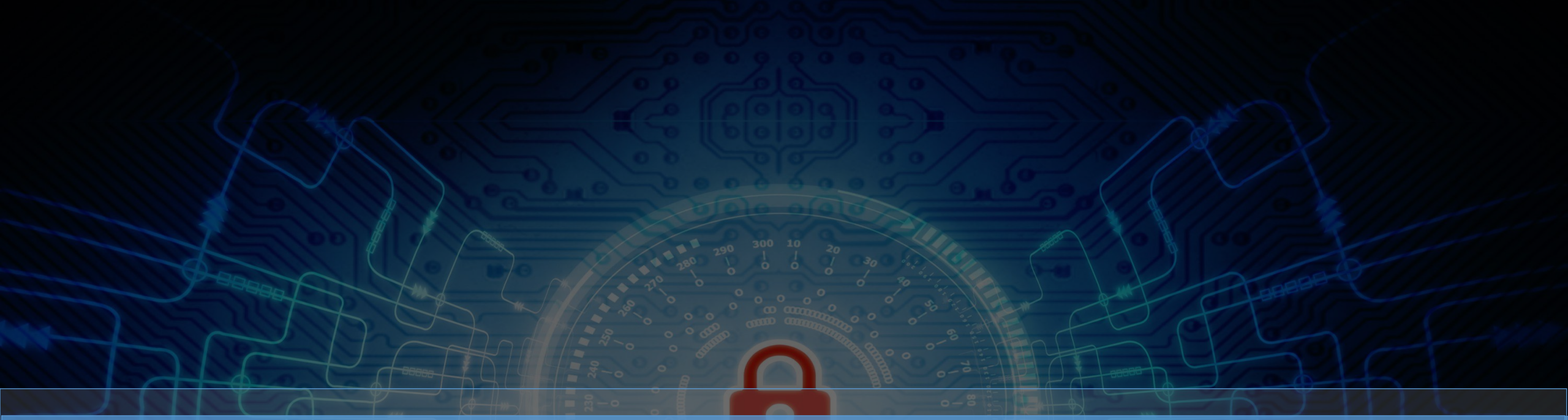
- Searchsploit easily searches out exploits using keywords
- Powersploit and Empire are tools that can be used for post-exploitation activities
- Responder is a network poisoner that can compromise Microsoft networks
- Metasploit is comprehensive pen testing framework with a number of useful tools within it

12.10 – Labtainers Lab (Metasploit Framework)

- 5.3 Explain use cases of the following tools during the phases of a penetration test

LAB SOFTWARE VULNERABILITIES: METASPLOIT

- Intro lab (Metasploit framework)
- Lab requires download and setup time
  - All automatic

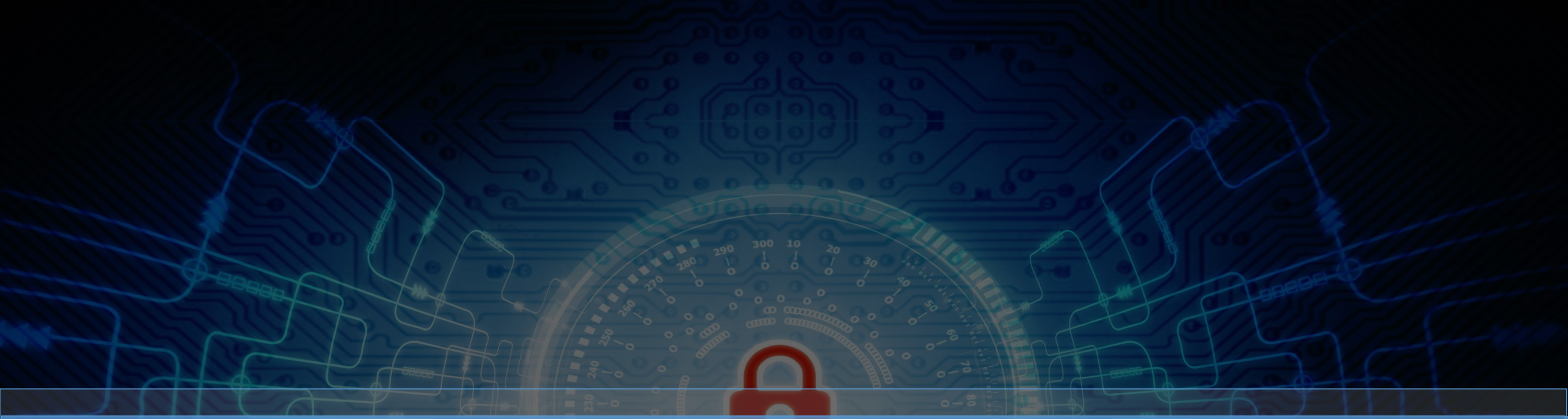


Episode 12.11 – Labtainers Lab (Wireshark Packet Inspection)

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

LAB NETWORK TRAFFIC ANALYSIS: PACKET-INTROSPECTION

- Intro lab (Using Wireshark for more advanced packet analysis)

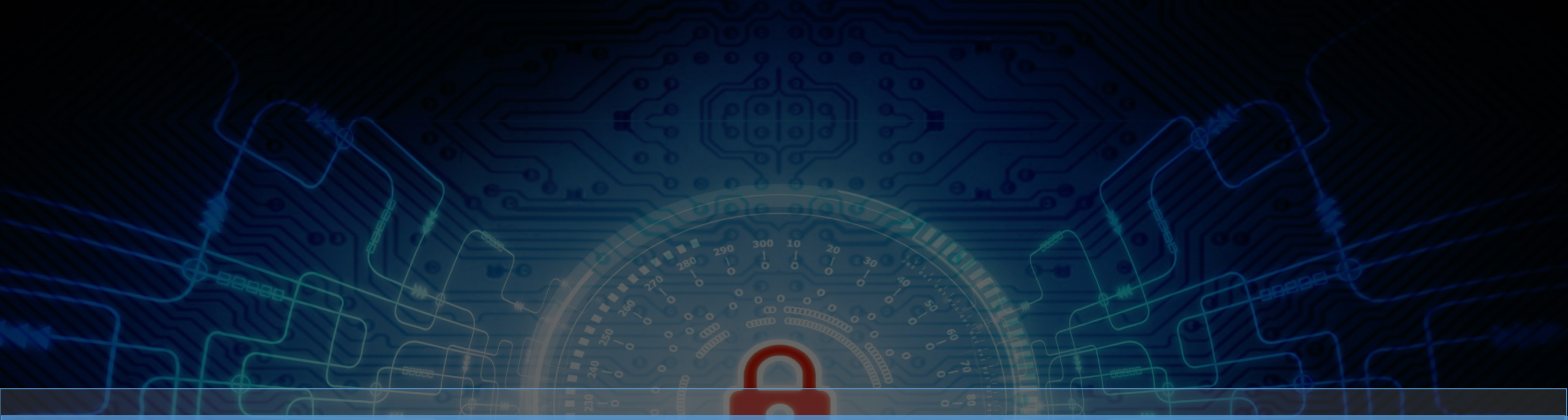


Episode 12.12 - Labtainers Lab (SSH)

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

LAB CRYPTO LABS: SSHLAB

- Intro lab (Secure remote access with SSH)



Episode 12.13 – Scanners, Debuggers, and Wireless Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

SCANNERS

- Tools that carry out active reconnaissance
- Wapiti
  - https://wapiti-scanner.github.io/
- WPScan
  - https://github.com/wpscanteam/wpscan
- Brakeman
  - https://brakemanscanner.org/
- Scout Suite
  - https://github.com/nccgroup/ScoutSuite

DEBUGGERS

- Covenant
  - https://github.com/cobbr/Covenant

WIRELESS

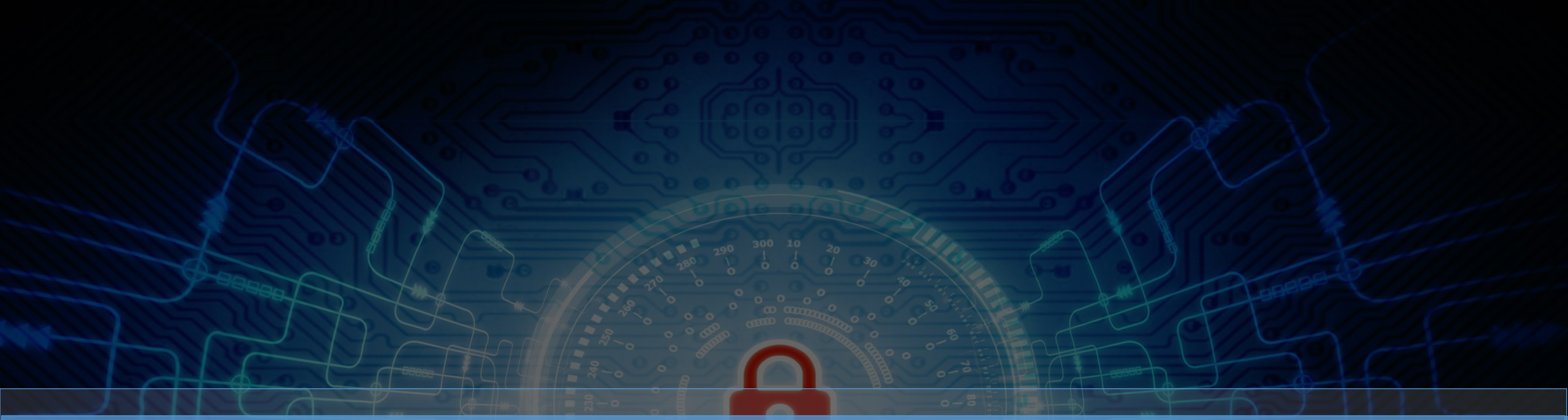
- EAPHammer
  - https://github.com/s0lst1c3/eaphammer
- mdk4
  - https://github.com/aircrack-ng/mdk4
- Spooftooph
  - https://www.kali.org/tools/spooftooph/

WIRELESS

- Reaver
  - https://www.kali.org/tools/reaver/
- Wireless Geographic Logging Engine (WiGLE)
  - https://www.wigle.net/
- Fern
  - https://www.kali.org/tools/fern-wifi-cracker/

QUICK REVIEW

- Many tools are available for pen testers
- A good toolbox should include a variety of tools
- Don’t reinvent the wheel
  - Be familiar with what is already out there



Episode 12.14 – Web, Steganography, and Cloud Tools

Objective 5.3 Explain use cases of the following tools during the phases of a penetration test

WEB APPLICATION TOOLS

- No pen testing toolbox would be complete without web application and other miscellaneous tools
- Gobuster
  - https://www.kali.org/tools/gobuster/

MISC. TOOLS

- mitm6
  - https://github.com/dirkjanm/mitm6
- CrackMapExec
  - https://github.com/byt3bl33d3r/CrackMapExec
- TruffleHog
  - https://github.com/trufflesecurity/trufflehog

STEGANOGRAPHY TOOLS

- Open stego
  - https://www.openstego.com/
- Steghide
  - https://www.kali.org/tools/steghide/
- Snow
  - https://github.com/mattkwan-zz/snow
- Coagula
  - https://www.abc.se/~re/Coagula/Coagula.html

STEGANOGRAPHY TOOLS

- Sonic Visualizer
  - https://www.sonicvisualiser.org/
- TinEye
  - https://tineye.com/
- Metagoofil
  - https://www.kali.org/tools/metagoofil/
- Online SSL checkers
  - https://www.sslshopper.com/ssl-checker.html
  - https://www.sslchecker.com/sslchecker

CLOUD TOOLS

- CloudBrute
  - https://www.kali.org/tools/cloudbrute/
- Pacu
  - https://github.com/RhinoSecurityLabs/pacu
- Cloud Custodian
  - https://github.com/cloud-custodian/cloud-custodian

DEPRECATED TOOLS

- Tools come and go as technology changes
- There are currently at least 3 deprecated tools on the exam
  - Cain (Cain and Abel)
  - DirBuster
  - OllyDbg
- Why are they still on the exam?
  - Part of the historical landscape
  - Lots of tutorials, books, and articles include them