

Hacker Tools & Exploits: Metasploit & Password Cracking

5 Days

DURATION

5

MODULES

125

TOPICS

21

HANDS-ON ACTIVITIES

LEARNING OBJECTIVES

- Conduct live forensics on Windows systems, memory and network artefacts
- Apply the MITRE ATT&CK framework to assess adversary techniques
- Perform reconnaissance and scanning using SHODAN and SpiderFoot
- Enumerate Windows Active Directory targets with BloodHound
- Crack passwords using John the Ripper and Hashcat
- Analyse password and web server logs with Elastic Stack
- Exploit systems and web applications using Metasploit
- Evade endpoint defences and cover tracks after compromise

5 Modules, 125 Topics

01

Live Forensics and Incident Response

OVERVIEW

- Live Windows examination
- Network investigation
- Memory investigation
- Malware investigation

INCIDENT RESPONSE

- Common incident response mistakes
- Incident goals and milestones
- Post-incident activities

DIGITAL INVESTIGATIONS

- Asking and answering the right questions
- Pivoting during an investigation
- Taking notes and writing reports
- Artifact and event-based timelines

LIVE EXAMINATION

- How to start, even with minimal information
- Examining a live environment
- Identifying abnormal activity

DIGITAL EVIDENCE

- Understanding what digital evidence is and how to collect it
- The role and elements of a chain of custody
- How to collect digital evidence

NETWORK INVESTIGATIONS

- Analyzing packet captures using tcpdump
- Web proxy logs

MEMORY INVESTIGATIONS

- How to investigate memory images using the Volatility framework

MALWARE INVESTIGATIONS

- Basic approaches for investigating malware
- Best practices for working with malware
- Environment using snapshot and continuous recording tools

Introducing the MITRE ATT&CK Framework and Reconnaissance

INTRODUCING THE MITRE ATT&CK FRAMEWORK

- Attacker evolution and the network for tool, technique, and practice (TTP) mapping
- Using the MITRE ATT&CK Framework for smarter adversary assessment
- How we integrate SEC504 with the MITRE ATT&CK Framework

RECONNAISSANCE

- What does your network reveal?
- Are you leaking too much information?
- Using certificate transparency for pre-production server identification
- Domain Name System harvesting
- Data gathering from job postings, websites, and government databases
- Identifying publicly compromised accounts
- FOCA for metadata analysis
- Aggregate OSINT data collection with SpiderFoot
- Mastering SHODAN searches for target discovery

SCANNING

- Learn the techniques attackers use to enumerate your networks
- Locating and attacking personal and enterprise Wi-Fi
- Identifying and exploiting proprietary wireless systems
- **Port scanning:** small and large-scale enumeration tasks
- Quick and effective intel collection from web servers
- Characterizing network targets by OS, service, patch level
- Vulnerability scanning and finding prioritization

ENUMERATING WINDOWS ACTIVE DIRECTORY TARGETS

- Windows Active Directory domain enumeration with BloodHound, SharpView
- Windows Command and Control with PowerShell Empire
- Operating system bridging from Linux to Windows targets
- Defending against SMB attacks with sophisticated Windows networking features
- Understanding SMB security features through Windows Server 2019

DEFENSE SPOTLIGHT: DEEPBLUECLI

- Using PowerShell to enumerate Windows systems
- Fast and effective Windows event log analysis
- Leveraging PowerShell output modifiers for reporting, analysis
- Characterizing common Windows scans and attacks against Windows servers

Password Attacks and Cracking

PASSWORD ATTACKS

- How attackers bypass account lockout policies
- Choosing a target protocol for password guessing attacks
- Techniques for choosing password lists
- How attackers reuse compromise password lists against your organization
- Techniques for password cracking
- Recommendations for password cracking in your organization

DEFENSE SPOTLIGHT: LOG ANALYSIS WITH ELASTIC STACK (FORMERLY ELK)

- Establishing a lightweight log analysis system with Elasticsearch, Logstack, Beats, and Kibana
- Understanding Linux and UNIX authentication logging data
- Configuring Filebeat for simple log ingestion
- Using Kibana to identify password attack events
- Customizing Kibana visualization for effective threat hunting

UNDERSTANDING PASSWORD HASHES

- Hashing algorithms, processes, and problems
- Understanding Windows hashing function through Windows Server 2019
- Password hash function strength and quality metrics
- Extracting Windows domain password hashes using built-in tools
- Getting password hashes from Windows 10 systems
- Decoding UNIX and Linux password hashes
- **Mitigating GPU-based cracking:** PBKDF2, bcrypt, and scrypt

PASSWORD CRACKING ATTACKS

- **John the Ripper:** single, wordlist, incremental, and external cracking modes
- **Cracking hashes with Hashcat:** straight and combinator attacks
- Effective hash computation using mask attacks
- Breaking user password selection weaknesses with Hashcat rules
- Three simple strategies for defeating password cracking

DEFENSE SPOTLIGHT: DOMAIN PASSWORD AUDITING

- Enumerating Windows domain settings with simple PowerShell one-line scripts
- Characterizing systemic behavior in user password selection
- Identifying bad password offenders in your organization
- Mitigating password sharing in Windows domains

Exploitation and Web Application Attacks

USING METASPLOIT FOR SYSTEM COMPROMISE

- Using the Metasploit framework for specific attack goals
- Matching exploits with reconnaissance data
- Deploying Metasploit Meterpreter Command & Control
- Identifying Metasploit exploit artifacts on the system and network

DRIVE-BY AND WATERING HOLE ATTACKS

- Examining the browser attack surface
- Identifying browser vulnerabilities with JavaScript
- Code-executing Microsoft Office attacks
- Backdooring legitimate code with attacker payloads

DEFENSE SPOTLIGHT: SYSTEM RESOURCE USAGE MONITOR (SRUM)

- Assessing attacker activity with Windows 10 app history
- Extracting useful data from the protected SRUM database
- Converting raw SRUM data to useful post-exploit analysis

WEB APPLICATION ATTACKS

- Account harvesting for user enumeration
- Command injection attacks for web server remote command injection
- **SQL Injection:** Manipulating back-end databases
- **Session Cloning:** Grabbing other users' web sessions
- **Cross-Site Scripting:** Manipulating victim browser sessions

DEFENSE SPOTLIGHT: EFFECTIVE WEB SERVER LOG ANALYSIS

- Using Elastic Stack (ELK) tools for post-attack log analysis
- Configuring Filebeat for web server log consumption
- Using the Kibana Query Language (KQL) to identify custom web attacks
- Hunting for common SQL Injection attack signatures
- Decoding obfuscated attack signatures with CyberChef

Post-Exploitation, Pivoting, and Covering Tracks

ENDPOINT SECURITY BYPASS

- Evading EDR analysis with executable manipulation: ghostwriting
- Manipulating Windows Defender for attack signature disclosure
- Using LOLBAS to evade application whitelisting
- Adapting Metasploit payloads on protected platforms

PIVOTING AND LATERAL MOVEMENT

- Pivoting from initial compromise to internal networks
- Effective port forwarding with Meterpreter payloads
- Leveraging compromised hosts for internal network scanning, exploitation
- Windows netsh and attacker internal network access

Post-Exploitation, Pivoting, and Covering Tracks (continued)

PRIVILEGED INSIDER NETWORK ATTACKS

- Leveraging initial access for network attacks
- Deploying packet sniffers, MITM attack tools
- Native packet capture on compromised Windows hosts
- **Abusing weak protocols:** DNS, HTTP
- Network service impersonation attacks with Flamingo
- Abusing Windows name resolution for password disclosure

COVERING TRACKS

- Maintaining access by manipulating compromised hosts
- Editing log files on Linux and Windows systems
- Hiding data in Windows ADS
- Network persistence through hidden Command & Control

DEFENSE SPOTLIGHT: REAL INTELLIGENCE THREAT ANALYTICS (RITA)

- Characterizing advanced Command & Control activity over the network
- Capturing and processing network data with Zeek
- **Network threat hunting:** beacons, long connections, strobes, and DNS analysis

POST-EXPLOITATION DATA COLLECTION

- Harvesting passwords from compromised Linux hosts
- Password dumping with Mimikatz and EDR bypass
- Defeating Windows and macOS password managers
- Windows keystroke logging attacks
- Data exfiltration over blended network protocols

NOTES

- Where To Go From Here: techniques for solving the problem of needing time for study, understanding the Forgetting Curve dilemma, techniques for developing long-term retention from what you have learned, and building study strategies for certification, applying your knowledge.

Practise What You Learn

#	MODULE	ACTIVITY
03	Password Attacks and Cracking	EXERCISES
		■ Online password guessing attacks with Hydra
		■ Defense Spotlight: Password guessing attack analysis with Elastic Stack
		■ Effective password cracking using Hashcat and John the Ripper
		■ Defense Spotlight: Domain Password Exposure Analysis with DPAT
04	Exploitation and Web Application Attacks	■ Data exfiltration, scanning, and pivoting with Netcat
		OVERVIEW
		■ Metasploit Attack and Analysis
		■ Software Update Browser Exploitation
		■ System Resource Utilization Database Analysis
		■ Command Injection Attack
		■ Cross Site Scripting Attack
		■ SQL Injection Attack
05	Post-Exploitation, Pivoting, and Covering Tracks	■ SQL Injection Log Analysis
		HANDS-ON ANALYSIS
		■ Exploiting user password misuse
		■ Completing scanning, reconnaissance analysis
		■ Using OSINT resources to collect information about a target network
		■ Matching reconnaissance data with public exploits
		■ Privilege escalation on Linux and Windows systems
		■ Exploiting common Windows Domain vulnerabilities
		■ Pillaging data on compromised systems
		■ Pivoting from initial compromise to internal network access
		■ Identifying attacker artifacts following a network compromise

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com