simspace

TRAINING CATALOG

2Q 2024

Disclaimer

While this catalog is designed to provide the audience with as accurate and up-to-date information as possible on tradecraft, methodologies, technologies, vulnerabilities, and exploits, the information provided is based upon the information available at time of publishing. Should new and updated information become available, SimSpace will update its Content Catalog appropriately.

All content available in this catalog is approved for worldwide distribution and usage.

Table of Contents

Index

Title	Difficulty	Duration (Hr)	Type	Audience
Advanced Forensic Analysis Challenge: Dead Drop	Intermediate	0.5	Challenge	Blue
Application Security Overview	Foundational	1	Training	Blue
ASCII and JSON Logs: Interpreting and Processing	Intermediate	1	Training	Blue
Attacking with XSS	Intermediate	1.5	Training	Purple
Baselining on Windows: Introduction	Intermediate	1	Training	Blue
Basic Malware Analysis Challenge: Alien Autopsy	Intermediate	4	Challenge	Blue
Basic Malware Analysis Exercise	Intermediate	2	Training	Blue
Basic Malware Analysis Workshop	Intermediate	2	Training	Blue
Basic Regular Expressions	Foundational	1	Training	Purple
Binary and Hex: Introduction	Foundational	1	Training	Purple
Boot2Root Workshop 1	Foundational	1	Training	Red
Boot2Root Workshop 2	Intermediate	1	Training	Red
Boot2Root Workshop 3	Intermediate	4	Training	Red
Boot2Root Workshop 4	Advanced	2	Training	Red
Continuous Integration (CI) Overview	Foundational	0.5	Training	Purple
Continuous Integration Challenge: Blame Thrower	Foundational	1	Challenge	Purple
Create or Modify System Process: MITRE ATT&CK® Purple	Intermediate	1	Training	Purple
Credential Management and Harvesting	Foundational	2	Training	Red
Cross-Site Request Forgery (CSRF): Introduction	Foundational	0.75	Training	Purple
Cross-Site Scripting (XSS): Introduction	Foundational	0.75	Training	Purple
CurveBall: Legacy Threat	Intermediate	2	Training	Purple
Cyber Attack Challenge: Cedar Bunny	Intermediate	2	Challenge	Red
Cyber Attack Challenge: Oak Rabbit	Expert	24	Challenge	Red
Cyber Defense Challenge: Blind Burglar	Advanced	4	Challenge	Blue
Cyber Defense Challenge: Business Aquarium	Advanced	4	Challenge	Blue
Cyber Defense Challenge: Stagecoach Holdup	Advanced	2	Challenge	Blue
■ Cyber Defense Walkthrough: Blue Lightfoil	Foundational	8	Challenge	Red
Cyber Kill Chain®	Foundational	1	Training	Purple
■ Cyber Offense Walkthrough: Red Lightfoil	Foundational	8	Training	Red
Defeating CSRF Protections with XSS	Foundational	0.75	Training	Red
Dirty COW	Intermediate	1	Training	Purple
Dirty Pipe: Legacy Threat	Intermediate	2	Training	Purple
Docker Fundamentals	Foundational	0.75	Training	Blue
Elastic Configuration and Data Ingestion	Intermediate	1	Training	Blue
Elastic Endpoint Forwarders	Intermediate	1	Training	Blue
Elastic Incident Investigation	Foundational	1.5	Training	Blue
Elastic Manual Uploads	Foundational	1.5	Training	Blue
Elastic Overview	Foundational	1.5	Training	Blue

■ New 2Q 2024

Index

Title	Difficulty	Duration (Hr)	Type	Audience
■ Empire Installation, Configuration and Basic Use	Foundational	2	Training	Red
Encrypted Traffic Forensics: CA and Issuance	Intermediate	0.5	Training	Blue
Encrypted Traffic Forensics: Introduction	Intermediate	1	Training	Blue
Encrypted Traffic Forensics: JA3, JA3S, and Other Tools	Intermediate	1	Training	Blue
Endpoint Security with HBSS/ESS	Intermediate	1	Training	Blue
Enumeration: Introduction	Foundational	1.5	Training	Red
Exploit Public-Facing Application: MITRE ATT&CK® Red	Intermediate	1	Training	Red
Files on Windows: Introduction	Foundational	0.5	Training	Purple
Flow Control in PowerShell	Foundational	1	Training	Blue
Follina Defense: Legacy Threat	Intermediate	1.5	Training	Blue
Follina Offense: Legacy Threat	Intermediate	1.5	Training	Red
Fuzzing: Memory Corruption Vulnerabilities	Advanced	1	Training	Purple
GDB: Introduction	Intermediate	1	Training	Purple
Git: Introduction	Foundational	1	Training	Blue
Heap Overflows: Memory Corruption Vulnerabilities	Advanced	1	Training	Purple
Host Analyst Assessment: Digital Scorpion	Intermediate	4	Challenge	Blue
Host Analyst Exercise: Threat Hunting and Incident Response	Intermediate	1	Training	Blue
■ Host Analyst: APT28 Exercise	Advanced	1	Training	Blue
■ Host Analyst: APT28 Workshop 1	Foundational	1	Training	Blue
■ Host Analyst: APT28 Workshop 2	Intermediate	1	Training	Blue
■ Host Analyst: APT34 Exercise	Advanced	2.5	Training	Blue
■ Host Analyst: APT34 Workshop 1	Foundational	2.5	Training	Blue
■ Host Analyst: APT34 Workshop 2	Intermediate	1.5	Training	Blue
■ Host Analyst: APT38 Exercise	Advanced	1	Training	Blue
■ Host Analyst: APT38 Workshop 1	Foundational	1	Training	Blue
■ Host Analyst: APT38 Workshop 2	Intermediate	1	Training	Blue
■ Host Analyst: APT40 Exercise	Advanced	1	Training	Blue
■ Host Analyst: APT40 Workshop 1	Foundational	1.5	Training	Blue
■ Host Analyst: APT40 Workshop 2	Intermediate	1	Training	Blue
Host Forensics Challenge: Wise Skunk	Intermediate	0.5	Challenge	Blue
Identifying Indicators of Compromise	Foundational	1	Training	Blue
■ ICS Foundations: Attacks	Foundational	1	Training	Blue
■ ICS Foundations: Introduction	Foundational	3.25	Training	Blue
■ ICS Foundations: Modbus-CLI and PLC Interaction	Foundational	2	Training	Blue
■ ICS Foundations: Network Defense	Foundational	3	Training	Blue
■ ICS Foundations: PLCs and Ladder Logic	Foundational	2	Training	Blue
■ ICS Foundations: Protocols	Foundational	9	Training	Blue
■ ICS Foundations: Ransomware	Foundational	2	Training	Blue

■ **New 2Q 2024**

Index

Title	Difficulty	Duration (Hr)	Type	Audience
Incident Identification and Prioritization Challenge: Plug and Play	Intermediate	1.5	Challenge	Blue
Indicator Removal on Host: MITRE ATT&CK® Purple	Intermediate	1	Training	Purple
Initial Access	Intermediate	2	Training	Red
Insecure Deserialization and SSTI	Intermediate	1	Training	Purple
Integration Testing in CI	Foundational	0.5	Training	Blue
Introduction to Application Security Challenge: Flabbergasted Florist	Foundational	1	Challenge	Blue
Introduction to SOC Challenge: SOC Monkey	Foundational	1	Challenge	Blue
Invoke-PSImage: Steganography	Intermediate	1	Training	Red
Kerberoasting: MITRE ATT&CK® Red	Foundational	1	Training	Red
Kibana Data Visualization	Intermediate	1	Training	Blue
Kibana: Introduction	Foundational	1	Training	Blue
Kibana SIEM Application	Intermediate	1	Training	Blue
Lateral Movement	Intermediate	4	Training	Red
Linux Configuration and Logging: Introduction	Foundational	1	Training	Purple
Linux Firewall	Foundational	3	Training	Blue
Linux Internals	Foundational	1	Training	Purple
Local File Inclusion (LFI): Introduction	Foundational	1	Training	Red
Local Permissions on Windows	Foundational	1	Training	Purple
Log4Shell Defense: Legacy Threat	Intermediate	1	Training	Blue
Log4Shell Offense: Legacy Threat	Intermediate	1	Training	Red
Logic and Implementation Vulnerabilities	Intermediate	1	Training	Red
Memory Corruption Vulnerabilities Challenge: iBreach	Advanced	1	Challenge	Red
Memory Corruption Vulnerabilities: Introduction	Advanced	1	Training	Purple
Metasploit Framework: Introduction	Foundational	1.5	Training	Red
Mind Maps	Foundational	2	Training	Blue
MITRE ATT&CK Framework	Foundational	1.5	Training	Blue
MITRE ATT&CK Practical Use	Foundational	1	Training	Blue
MITRE ATT&CK Threat Mapping	Intermediate	1.5	Training	Blue
Modifying Zeek Scripts	Intermediate	1	Training	Blue
MSFvenom: Introduction	Foundational	1	Training	Red
Network Analyst Challenge: Broken Halo	Advanced	4	Challenge	Blue
Network Analyst Challenge: Hidden Lotus	Advanced	4	Challenge	Blue
Network Analyst Exercise: Network Threat Hunting	Intermediate	3.5	Training	Blue
Network Analyst Walkthrough: ASCII and JSON Logging	Intermediate	0.5	Training	Blue
Network Analyst Walkthrough: Modifying Zeek Scripts	Intermediate	0.5	Training	Blue
Network Analyst Walkthrough: Packet Capture and Analysis	Intermediate	1	Training	Blue
Network Configuration in Windows	Foundational	2	Training	Red
Network Device Configuration	Foundational	1	Training	Blue

Index

Title	Difficulty	Duration (Hr)	Type	Audience
Network Firewalls	Foundational	1	Training	Blue
Network Forensics Challenge: Zeeking the Predator	Intermediate	1	Challenge	Blue
Network Remediation: Introduction	Intermediate	2	Training	Blue
NetworkMiner: Introduction	Foundational	1	Training	Blue
Nmap: Introduction	Foundational	0.75	Training	Purple
Open-Source Intelligence (OSINT): Introduction	Foundational	1	Training	Purple
Open-Source Intelligence (OSINT) Techniques	Foundational	1	Training	Blue
Operational Security 101	Foundational	1.5	Training	Blue
OSI Model	Foundational	0.5	Training	Purple
Packet Capture and Analysis	Foundational	1	Training	Purple
Parsing Network Traffic with Zeek	Intermediate	1	Training	Blue
Perl Compatible Regular Expressions (PCRE)	Foundational	1	Training	Purple
Persistence	Foundational	4	Training	Red
PowerShell Objects, Properties, and Methods	Foundational	1.5	Training	Red
PowerShell Script Creation Mechanics	Foundational	1	Training	Red
PowerShell: Introduction	Foundational	1	Training	Blue
PrintNightmare Defense: Legacy Threat	Advanced	1.5	Training	Blue
PrintNightmare Offense: Legacy Threat	Advanced	1	Training	Red
Privilege Escalation	Intermediate	2.5	Training	Red
Protocol Basics	Foundational	0.5	Training	Red
Protocol Traffic Analysis Walkthrough	Foundational	1	Training	Red
ProxyLogon Defense: Legacy Threat	Advanced	1	Training	Blue
ProxyLogon Offense: Legacy Threat	Advanced	1	Training	Red
PwnKit Defense: Legacy Threat	Intermediate	2.5	Training	Blue
PwnKit Offense: Legacy Threat	Intermediate	2	Training	Red
■ Ransomware Challenge: Scarlet Sunrise	Foundational	48	Challenge	Red
■ Ransomware Walkthrough: Scarlet Sunrise	Foundational	8	Training	Red
Reconnaissance Challenge: Stakeout	Foundational	1	Challenge	Red
Reducing Vulnerabilities in Code Challenge: Shellshocked Sally	Intermediate	0.75	Challenge	Blue
Removing Artifacts	Foundational	2	Training	Red
Reverse Shells	Foundational	1	Training	Purple
Secure Coding	Intermediate	0.75	Training	Blue
Secure SDLC: Deployment and Maintenance	Foundational	1	Training	Blue
Secure SDLC: Development	Foundational	1	Training	Blue
Secure SDLC: Requirements and Design	Foundational	1	Training	Blue
Secure SDLC: Testing	Foundational	1	Training	Blue
Security Operations Center (SOC) Overview	Foundational	0.5	Training	Blue
Security Testing	Intermediate	1	Training	Blue

■ **New 2Q 2024**

Index

Title	Difficulty	Duration (Hr)	Type	Audience
SIEM Challenge: Lone Shark	Foundational	2	Challenge	Blue
SIEM: Conceptual Introduction	Foundational	1	Training	Blue
SIEM Fundamentals Challenge: Little Lone Shark	Foundational	1	Challenge	Blue
SIEM: Practical Introduction	Intermediate	1.5	Training	Blue
SIEM Walkthrough: Incident Response	Advanced	1	Training	Blue
Sigma: Introduction	Intermediate	0.5	Training	Blue
SIP Telephony	Intermediate	0.75	Training	Blue
SOC: Incident Response	Foundational	0.75	Training	Blue
SOC: Security Monitoring	Foundational	0.5	Training	Blue
SOC: Threat Hunting	Foundational	0.75	Training	Blue
Splunk Boss of the SOC V1	Intermediate	6	Challenge	Blue
Splunk Boss of the SOC V2	Intermediate	6	Challenge	Blue
Splunk Boss of the SOC V3	Intermediate	6	Challenge	Blue
Splunk Configuration and Data Ingestion	Intermediate	1	Training	Blue
Splunk Enterprise Security	Advanced	1.5	Training	Blue
Splunk Forwarders and Normalization	Foundational	1	Training	Blue
Splunk Incident Investigation	Foundational	2	Training	Blue
Splunk Overview	Foundational	1.5	Training	Blue
Splunk Post Incident Investigation Actions	Foundational	1	Training	Blue
Splunk Searching	Foundational	1.5	Training	Blue
SQL and OS Injection: Introduction	Intermediate	1	Training	Red
SQLi Attack Types	Intermediate	1	Training	Red
sqlmap: Introduction	Foundational	1	Training	Red
Stack Overflows: Memory Corruption Vulnerabilities	Advanced	1	Training	Purple
Steal or Forge Kerberos Tickets: MITRE ATT&CK® Purple	Advanced	2	Training	Purple
Supply Chain Compromise: MITRE ATT&CK® Red	Advanced	4	Training	Red
Suricata: Introduction	Foundational	0.75	Training	Blue
Suricata Rule Writing	Intermediate	1.5	Training	Blue
System Monitor (Sysmon)	Foundational	1	Training	Blue
Telemetry Challenge: Faulty Firewall	Foundational	1	Challenge	Blue
Threat Hunting in Windows Files	Foundational	1	Training	Blue
Threat Hunting Physical Devices	Intermediate	1	Training	Blue
Threat Hunting with IOCs Challenge: Dragnet Diaries	Intermediate	1	Challenge	Blue
Threat Hunting with IOCs Exercise	Intermediate	2	Training	Blue
Threat Hunting with IOCs Workshop	Foundational	1	Training	Blue
Threat Hunting with MITRE ATT&CK®	Foundational	2.5	Training	Blue
Threat Hunting with Splunk	Foundational	2	Training	Red
Threat Modeling	Foundational	0.75	Training	Blue

Index

Title	Difficulty	Duration (Hr)	Type	Audience
Unit Testing in CI	Foundational	1	Training	Blue
Unsecured Credentials: MITRE ATT&CK® Purple	Intermediate	1.5	Training	Purple
Volatility: Introduction	Foundational	0.5	Training	Blue
Vulnerability Enumeration	Foundational	1	Training	Red
Vulnerability Remediation	Intermediate	1	Training	Blue
Web Application Exploitation	Foundational	1	Training	Purple
Web Application Fuzzing	Foundational	1	Training	Red
Web Vulnerabilities Challenge: Fools Errant	Intermediate	1	Challenge	Purple
Web Vulnerabilities: Introduction	Intermediate	1	Training	Red
Windows Command Line and Administration	Foundational	1	Training	Purple
■ Windows Droppers	Foundational	4	Training	Red
Windows Event Forwarding	Intermediate	1	Training	Blue
Windows Internals: Introduction	Foundational	0.5	Training	Purple
Windows Libraries: Introduction	Foundational	2	Training	Blue
Windows Logging and Monitoring	Foundational	1	Training	Purple
Windows Logging: Introduction	Foundational	2	Training	Purple
Windows Memory Analysis: Introduction	Foundational	0.75	Training	Blue
Windows Processes: Introduction	Foundational	2	Training	Blue
Windows Registry: Introduction	Foundational	0.5	Training	Purple
Wireshark: Introduction	Foundational	1.5	Training	Red
XML External Entities (XXE) Attacks	Intermediate	1	Training	Red
XXE Attacks and SSRF Vulnerabilities	Intermediate	1	Training	Purple
YARA and Signature-Based Writing	Foundational	2	Training	Blue
Zerologon: Legacy Threat	Foundational	2	Training	Purple

Challenges

Advanced Forensic Analysis Challenge: Dead Drop

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

This challenge tests encrypted traffic forensics and Windows baselining skills. It also requires skills with using Suricata, Wireshark, and JA3 signatures to locate infected devices.

Goals

- Identify network indicators of compromise (IOC) on infected devices.
- Use network IOC to find further infected devices.
- Identify host IOC on infected devices.
- Use host IOC to find infected devices.

Basic Malware Analysis Challenge: Alien Autopsy

Intermediate

Publisher: SimSpace

Individual

4 hours

Description

Assume a junior malware analyst's role on the morning of a malware outbreak. Use your skills to identify key indicators that can be used to track the outbreak and prevent it from spreading.

Goals

- Report facts about an unknown binary from initial detonation.
- Create an MD5 hash from an unknown executable.
- Perform basic static analysis to gather facts.
- Perform basic dynamic analysis to gather facts.
- Review findings for inclusion in a post-compromise report.

Continuous Integration Challenge: Blame Thrower

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Investigate the trials and tribulations in a development team's attempt to implement continuous integration and modern, secure coding practices.

Goals

- Navigate a Git repository.
- Recognize the best practices a development team implemented in their continuous integration workflow.
- Identify the security vulnerability in the team's implementation.
- Investigate an attack's cause and its mitigation.

Cyber Attack Challenge: Cedar Bunny

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Test your red team skills in a simple, simulated environment. With multiple threads to pull on, this red-team challenge will draw you to demonstrate your favorite tactics and techniques to gather shells and flags across the challenge field.

Goals

- Use external reconnaissance to enumerate the interior of a network.
- Identify entry points and elevation points that can bring a challenger to superuser status.
- Decide from a platform of tools and maneuvers which will be optimal in achieving and maintaining network supremacy.

Cyber Attack Challenge: Oak Rabbit

Expert

Publisher: SimSpace

Individual

24 hours

Description

Test your red team skills in a realistic enterprise environment. With multiple threads to pull on, you'll find your favorite TTPs will get you your shells and flags.

Goals

- Use external reconnaissance to enumerate the interior of a network.
- Identify entry points and elevation points that can bring a challenger to superuser status.
- Select from a platform of tools to decide the optimal maneuvers to achieve and maintain network supremacy.

Cyber Defense Challenge: Blind Burglar

Advanced

Publisher: SimSpace

Individual

4 hours

Description

A capture-the-flag challenge in which network defenders uncover crypto-mining software installed across their networks, and trace their invasions to the security shortcomings that allowed them in.

Goals

- Identify the initial compromise point of the network and its matching CVE.
- Evaluate Sigma rules to identify a specific attack.
- Use multiple SIEM tools to trace a complete attack path.
- Identify all network components compromised in an attack chain.
- Identify suspicious files or activities on a machine or target network.

Cyber Defense Challenge: Business Aquarium

Advanced

Publisher: SimSpace

Individual

4 hours

Description

In this capture-the-flag challenge, trace the path of an attacker traversing a network through social mistrust, discover their malware, identify their command-and-control infrastructure, and find out what they were after.

Goals

- Identify the sensitive document(s) and how they were exfiltrated.
- Identify where the attacker gained initial access to a network.
- Identify how the attacker gained initial access to a network.
- Identify the security misconfigurations that allowed the attack to work.

Cyber Defense Challenge: Stagecoach Holdup

Advanced

Publisher: SimSpace

Individual

2 hours

Description

This capture-the-flag challenge employs Kibana, Hybrid Hunter, and other tools to find an infestation of ransomware in the company network and trace events back to initial compromise.

Goals

- Identify the ransomware malware and its locations on a network.
- Identify where the attacker gained initial access to a network.
- Identify how the attacker gained initial access to a network.
- Identify the security misconfigurations that allowed the attack to work.

Cyber Defense Walkthrough: Blue Lightfoil

Foundational

Publisher: SimSpace

Individual

8 hours

Description

This walkthrough employs Splunk to investigate a compromised enterprise network.

Goal

- Identify compromised hosts.
- Identify techniques used by the attacker.

Host Analyst Assessment: Digital Scorpion

Intermediate

Publisher: SimSpace

Individual

4 hours

Description

You are tasked with investigating a malware infection on a small network. Use blue team tools and techniques, including Windows logs, Powershell, YARA, and Volatility, to analyze the hosts and uncover the extent of the infection.

Goals

- Identify the presence of a malware infection.
- Discover the changes to the system made by the malware.
- Determine the original point of infection.
- Analyze a memory capture to find the presence of active C2.
- Find the location of a second infection using malware signatures.

Host Forensics Challenge: Wise Skunk

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

In this challenge, you assume the role of the primary blue team operator during a host-based investigation of a red team audit.

Goals

- Conduct basic forensic investigations using Windows logs.
- Using the method of your choice, view and interpret Linux log files.

Incident Identification and Prioritization Challenge: Plug and Play

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

Your network is under attack! Whether by a knowing compromise or means of subterfuge, a malicious actor has found their way in. Using your knowledge of SIEM fundamentals and network monitoring software, dig out the source of this attacker's intrusion and expel them!

Goals

- Use log aggregation software to unearth a network intrusion.
- Identify Indicators of Compromise (IOC) using domain name lookups.
- Identify IOC from Windows and Linux logging.

Introduction to Application Security Challenge: Flabbergasted Florist

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Showcase your application security mettle by helping Flora McMahon secure her application as she plans to release a new feature in this exciting challenge.

Goals

- Recommend misuse cases and security requirements for a new application feature.
- Identify new threats against an application.
- Run a SAST tool against an application and analyze the results.
- Run security unit tests on an application and analyze the results.
- Identify the capabilities of application testing tools.
- Analyze ModSecurity logs to identify an attack.
- Recommend techniques to secure the deployment and maintenance of an application.

Introduction to SOC Challenge: SOC Monkey

Foundational

Publisher: SimSpace

Individual

1 hour

Description

DroneRaptor is building a SOC and has called you in to consult on the process. As they progress through the steps of planning, building, and implementing a SOC, you will be presented with options for them to take. Once they get to the implementation phase, you will have to perform some incident investigation activities.

Goals

- Select an appropriate SOC architecture, given constraints and goals.
- Identify the roles of members of the SOC.
- Identify relevant tools that will be used in the SOC.
- Implement the correct alert triage procedure.
- Implement the correct incident response procedure.
- Perform threat hunting to identify a current threat.

Memory Corruption Vulnerabilities Challenge: iBreach

Advanced

Publisher: SimSpace

Individual

1 hour

Description

In this challenge, you perform fuzz testing on an application containing a memory corruption vulnerability. To demonstrate the impact of the vulnerability, you exploit the remote application to achieve remote code execution.

Goals

- Identify a vulnerability using the boofuzz framework.
- Locate a memory corruption vulnerability using GNU Debugger.
- Exploit the memory corruption vulnerability with Python.
- Identify possible solutions to mitigate the vulnerability.

Network Analyst Challenge: Broken Halo

Advanced

Publisher: SimSpace

Individual

4 hours

Description

Your network is under attack! Examine the artifacts of an intrusion and recreate the steps of the attack chain. Use incident response skills, such as packet capture analysis and Linux command-line utilities, to gather the basic facts about your company's compromise.

Goals

- Identify the hostname of the initial point of compromise.
- Identify the IP address that launched the initial attack.
- Identify the exploited service and resource of the initial point of compromise.
- Identify the IP address of the host used for lateral movement.
- Identify the Fully Qualified Domain Name of the server used for stage 2 malware download.
- Identify the beaconing interval of the malware C2 agent.
- Recover the file used to download the malware C2 agent.
- Write a Zeek script to identify C2 traffic.

Network Analyst Challenge: Hidden Lotus

Advanced

Publisher: SimSpace

Individual

4 hours

Description

In this blue team assessment, use network threat hunting and forensics skills to uncover a sophisticated breach of a realistic corporate network.

Goals

- Fully scope a network breach and identify all compromised devices.

Network Forensics Challenge: Zeeking the Predator

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

A challenge to test skills with network forensics using Suricata, Wireshark, and Zeek.

Goals

- Confirm a potential attack via Suricata alerts.
- Identify a network indicator from which to pivot.
- Identify one or more attacked hosts.
- Confirm fully infected host(s) that require remediation.
- Extract the attacker's tool.

Ransomware Challenge: Scarlet Sunrise

Foundational

Publisher: SimSpace

Individual

48 hour

Description

Examines host and network artifacts to investigate a cyber intrusion and ransomware attack. Includes brief post-question explanations.

Goals

- Gather evidence associated with the attack.
- Identify IOCs to inform intelligence feeds.
- Identify attacker infrastructure, such as domain names and Internet Protocol (IP) addresses.
- Collect evidence to support subpoena and search warrant requests.
- Log evidence in an IR timeline.

Reconnaissance Challenge: Stakeout

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Use discovery, enumeration, and open-source intelligence (OSINT) to identify potential cyber attack vectors for the fictional company SomeCorp.

Goals

- Perform reconnaissance on SomeCorp to identify information to leverage in an attack.
- Use OSINT sources to obtain data for social engineering.
- Discover and enumerate hosts, services, and web applications.

Reducing Vulnerabilities in Code Challenge: Shellshocked Sally

Intermediate

Publisher: SimSpace

Individual

0.75 hours

Description

Sally's website is riddled with vulnerabilities. Help her team to make their site's code more secure by going over secure coding, security testing, threat modeling, and vulnerability remediation.

Goals

- Review the specifications of the Common Vulnerability Scoring System (CVSS).
- Analyze a CVSS score.
- Differentiate between vulnerability remediation and mitigation.
- Identify code that uses secure coding best practices.
- Verify secure code review processes.
- Identify and demonstrate a common security flaw in code.
- Differentiate between security testing tool types.
- Use a Dynamic Application Security Testing (DAST) tool against an application and analyze the results.
- Recommend a vulnerability remediation plan and determine the best courses of action.

SIEM Challenge: Lone Shark

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Your network is under attack! Examine the artifacts of an intrusion and recreate the steps of the attack chain. Use threat hunting skills, such as Kibana or Splunk searching and visualization, to gather the basic facts about your company's compromise. After gathering these facts, answer a series of questions about the intrusion from compromised hosts to malware artifacts.

Goals

- Identify the binary names of the supply chain compromised software.
- Identify the hostnames of infected clients.
- Identify the IP address of the malicious server that is exfiltrating data.
- Identify the hostname of the infected server.
- Identify the first timestamp of exfiltrated data.
- Identify the last timestamp of exfiltrated data.
- Identify the number of times that data was exfiltrated from the network.
- Identify the filename of the output written to disk by the malware.

SIEM Fundamentals Challenge: Little Lone Shark

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Your network is under attack! Examine the artifacts of an intrusion and recreate the steps of the attack chain. Use threat hunting skills, such as Kibana or Splunk searching and visualization, to gather the basic facts about your company's compromise. After gathering these facts, answer a series of questions about the intrusion from compromised hosts to malware artifacts.

Goals

- Identify the binary names of the supply chain compromised software.
- Identify the hostnames of infected clients.
- Identify the IP address of the malicious server that is exfiltrating data.
- Identify the hostname of the infected server.
- Identify the first timestamp of exfiltrated data.
- Identify the last timestamp of exfiltrated data.
- Identify the number of times that data was exfiltrated from the network.
- Identify the filename of the output written to disk by the malware.

Splunk Boss of the SOC V1

Intermediate

Publisher: SimSpace

Individual

6 hours

Description

The focus of this hands-on lab will be an APT scenario and a ransomware scenario. You assume the persona of Alice Bluebird, the analyst who has recently been hired to protect and defend Wayne Enterprises against various forms of cyberattack.

Splunk Boss of the SOC V2

Intermediate

Publisher: SimSpace

Individual

6 hours

Description

In this hands-on exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly to assist them with their recent issues.

Splunk Boss of the SOC V3

Intermediate

Publisher: SimSpace

Individual

6 hours

Description

Boss of the SOC is a blue-team CTF that helps you enhance your hunting and analysis skills. You will use Splunk and other tools to answer a variety of questions about security incidents that have occurred in a realistic but fictitious enterprise environment.

Telemetry Challenge: Faulty Firewall

Foundational

Publisher: SimSpace

Individual

1 hour

Description

This challenge tests the ability to tie together multiple sources of network telemetry to identify and mitigate threats and misconfigurations.
It requires skill with network firewalls, Elastic endpoint forwarders, Windows Event Forwarding, and Sysmon.

Goals

- Use Kibana/Elastic to identify a threat within the network.
- Identify and correct misconfigurations hampering investigations into the threat.
- Triage the threat and collect information about it.
- Identify and correct the misconfiguration that is allowing the threat to connect into and out of the network.

Threat Hunting with IOCs Challenge: Dragnet Diaries

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

In this challenge, your threat hunting abilities are put to the test.

Goals

- Identify network indicators of compromise on infected devices.
- Use network indicators of compromise to find further infected devices.
- Identify host indicators of compromise on infected devices.
- Use host indicators of compromise to find infected devices.

Web Vulnerabilities Challenge: Fools Errant

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

This web vulnerabilities challenge presents a set of websites intentionally vulnerable to attacks listed in the OWASP Top 10 2017.

Goals

- Obtain the highest-level access to the website: www.challenge.local.
- Obtain the highest-level access to the website: blog.challenge.local.
- Use features made available to users of www.challenge.local and blog.challenge.local with the level of access obtained to compromise the underlying server.

Blue Team Training

Blue Team Training

Blue Team Training

Application Security Overview

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An overview of how to incorporate security into each phase of the software development life cycle (SDLC). This module also reviews the common weaknesses of different application architectures and briefly discusses popular application vulnerabilities.

Outcomes

- Describe the purpose and benefits of application security.
- Identify methods of incorporating security into the SDLC.
- Recognize the risks inherent in CI/CD pipelines.
- Compare the common weaknesses of different application architectures.
- Identify the most common application vulnerabilities.

ASCII and JSON Logs: Interpreting and Processing

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Become more efficient at analyzing Linux logs by using various Linux built-in commands such as grep, cut, and awk, as well as the jq tool to view and filter JSON logs.

Outcomes

- Use grep to find a log line of interest.
- Use a Perl regular expression with grep to find matching log lines.
- Use tail or head to find the end or beginning of a log respectively.
- Use cut to show a particular column of interest from an identified log.
- Use awk to find specific information in an identified log.
- Use jq to view and filter JSON logs.

Baselining on Windows: Introduction

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

This module explores Windows Golden Images, baselining of files, processes, services, patches, and network connections. It includes hands-on labs to exercise baselining skills on a known good system as well as a compromised host.

Outcomes

- Export a Windows object's current state using Powershell.
- Compare XML objects using Powershell.
- Compute a file's MD5 hash using Powershell.
- Compare CSV objects using Powershell.
- Identify malicious deviations from a calculated baseline.

Basic Malware Analysis Exercise

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Take a guided tour of one of the most infamous pieces of malware in history: WannaCry.

Outcomes

- Create an MD5 hash from an unknown executable.
- Use FLOSS or Strings to identify text strings in an unknown executable and make inferences based on the string's content.
- Use PE-Bear to view imports, headers, and data sections of an unknown executable and make inferences about its content.
- Use network analysis tools to identify malicious network signatures for a malicious binary.
- Use host-based analysis tools to identify malware behavior.

Basic Malware Analysis Workshop

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Foundational skills of malware analysis, covering basic static and dynamic analysis, in which the analyst identifies key malware behaviors and artifacts.

Outcomes

- Identify the difference between static and dynamic analysis.
- Create an MD5 hash from an unknown executable.
- Use FLOSS64 to identify text strings in an unknown executable and make inferences based on the string's content.
- Use PE-Bear to view imports, headers, and data sections of an unknown executable and make inferences about its content.
- Use network analysis tools to identify malicious network signatures for a malicious binary.
- Use host-based analysis tools to identify malware registry key manipulation.

Docker Fundamentals

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Benefits of Docker, creating a Docker application, and Docker security best practices.

Outcomes

- Identify the advantages of using Docker instead of Linux containers (LXC).
- Interact with and examine Docker containers using Linux command line interface (CLI):
  - Add a Docker container.
  - Access an error log.
  - Mount a volume in a container.
  - Connect containers to a network.
- Design a Docker application.
- Recognize and implement Docker security best practices.

Elastic Configuration and Data Ingestion

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Covers Elasticsearch installation and configuration, importing data, and querying data from the command line and Kibana. Gain a basic understanding of how Elastic functions “under the hood” through JSON requests and formatted data. Leverage pre-formatted data as well as use a script to parse non-JSON data so it can be efficiently indexed into Elastic.

Outcomes

- Configure Elasticsearch to use a single node.
- Configure Elasticsearch to run at boot in Linux.
- Start Elasticsearch from the command line using systemctl.
- Verify Elasticsearch is running by querying the database.
- Create a custom map for importing data into an index.
- Import data using the command line.
- Query an Elasticsearch database using Kibana.

Elastic Endpoint Forwarders

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An introduction to the Beats framework of the Elastic Stack. Beats are lightweight applications that ship data to the Elastic Stack from network hosts and devices. Install and configure Auditbeat, Filebeat, Packetbeat, and Winlogbeat. Use Kibana to aggregate data and search for log artifacts.

Outcomes

- Identify the correct shipper for a provided data source.
- Install and configure a selection of Beats.
- Use the Elastic Stack to identify artifacts of interest.

Elastic Incident Investigation

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Provides an intermediate understanding of the Elastic Stack platform by operationalizing the Elastic Stack software tool to assist in a cyber investigation and to detect malicious cyber activity.

Outcomes

- Perform the steps necessary to leverage Elastic Stack as an investigation tool.

Elastic Manual Uploads

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

A detailed look at how to operationalize the Elastic Stack to enable defensive cyberspace operations.

Outcomes

- Discuss the process of manually uploading logs to the Elastic Stack.
- Identify various ways to use Elastic Stack in an operational environment.
- Identify methods used to troubleshoot the Elastic Stack.

Elastic Overview

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Explore the Elastic Stack and its use in Security Information and Event Management (SIEM) within operational environments.

Outcomes

- Discuss how the Elastic Stack is architected.
- Identify various methods and ways to ingest data into the stack.

Encrypted Traffic Forensics: CA and Issuance

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

This module covers investigating certificates and verifying if the certificate is valid.

Outcomes

- Use Suricata and Zeek for forensic analysis of encrypted traffic.

Encrypted Traffic Forensics: Introduction

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

The basics of how to conduct forensic analysis on encrypted network traffic.

Outcomes

- Describe the two primary types of encryption.
- Summarize the basics of public-key cryptography.
- Summarize the relationship of Transport Layer Security with encryption.
- Use Suricata for forensic analysis of encrypted traffic.

Encrypted Traffic Forensics: JA3, JA3S, and Other Tools

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

This module covers using fingerprinting methods and other forensic tools to identify programs sending encrypted traffic.

Outcomes

- Use JA3 and JA3S fingerprinting for encrypted traffic analysis.

Endpoint Security with HBSS/ESS

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An introduction to concepts related to basic usage of HBSS/ESS, a McAfee product that includes the ePolicy Orchestrator and Endpoint Security. It includes creation of expert rules to detect malicious behavior.

Outcomes

- Locate core functionality of HBSS as it relates to defensive host analysis.
- Identify malware using basic antivirus detection.
- Recognize the tradeoffs when enabling antivirus signature rules.
- Describe the limitations of basic antivirus detection.
- Implement expert rules to detect and limit the impact of novel malware.

Flow Control in PowerShell

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Fundamental PowerShell flow control elements for creating complex scripts. Covers comparison and logical operators, if statements, loops, and error handling.

Outcomes

- Interpret PowerShell's comparison operators, logical operators, and if statements.
- Differentiate between types of PowerShell loops and their functions.
- Recognize and implement PowerShell loop logic.
- Decipher error handling in PowerShell.
- Automate Windows system administrative tasks using PowerShell scripts.

Git: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to version control with an overview of Git fundamentals that includes adding, removing and committing files and changes; creating and interfacing with repositories locally or centralized; and several advanced Git commands.

Outcomes

- State the benefits of version control.
- Explain the difference between local and remote repositories.
- Explain the difference between GitHub and GitLab.
- Implement Git.
- Identify version control actions and the Git commands used to perform them.
- Perform an initial commit to a repository.
- Save changes made locally to a repository.
- Pull code from a repository.
- Observe a repository and locate important information about changes.

Host Analyst Exercise: Threat Hunting and Incident Response

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Engage in a hands-on exercise as a contractor hired by a small company to augment its security staff. Use blue team techniques and tools, such as YARA and Volatility, to perform incident response procedures in their network.

Outcomes

- Use blue team tools for threat hunting and incident response to accomplish the following:
  - Identify process anomalies using a known good baseline.
  - Conduct forensic investigations using Windows logs.
  - Identify active processes in acquired memory image.
  - Use YARA for threat hunting.

Host Analyst: APT28 Workshop 1

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine APT28 TTPs through a defensive lens using the MITRE ATT&CK framework and known indicators of compromise.

Outcomes

- Identify host indicators of compromise attributed to APT28.
- Detect APT28 malicious activity.
- Given an APT28 intrusion, determine which host IOCs are present.

Host Analyst: APT28 Workshop 2

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Examine a potential attack chain that uses APT28 TTPs, and conduct threat hunting to identify indicators of compromise.

Outcomes

- Identify host indicators of compromise attributed to APT28.
- Detect APT28 malicious activity.
- Determine which host IOCs are present.

Host Analyst: APT28 Exercise

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Apply knowledge gained in APT28 workshops, with less guidance, to identify all indicators, including possible changes in TTPs.

Outcomes

- Identify networking indicators of compromise attributed to APT28.
- Detect APT28 malicious activity.
- Given an APT28 intrusion, determine which host IOCs are present.

Host Analyst: APT34 Workshop 1

Foundational

Publisher: SimSpace

Individual

2.5 hours

Description

Examine APT34 TTPs through a defensive lens using the MITRE ATT&CK framework and known indicators of compromise.

Outcomes

- APT34 analysis
- Data source review

Host Analyst: APT34 Workshop 2

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

Examine APT34 TTPs through a defensive lens using the MITRE ATT&CK framework and known indicators of compromise.

Outcomes

- Workshop 1 review
- TTP review
- Data source review

Host Analyst: APT34 Exercise

Advanced

Publisher: SimSpace

Individual

2.5 hours

Description

Apply the knowledge gained in APT34 workshops, with less guidance, to identify all indicators, including possible changes in TTPs.

Outcomes

- TTP Review
- Scenario
- Host Analysis

Host Analyst: APT38 Workshop 1

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine APT38 TTPs through a defensive lens using the MITRE ATT&CK framework and known indicators of compromise.

Outcomes

- Identify host indicators of compromise linked to APT38.
- Characterize APT38 malicious activity.

Host Analyst: APT38 Workshop 2

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Examine a potential attack chain that uses APT38 TTPs, and conduct threat hunting to identify indicators of compromise.

Outcomes

- APT38 TTP Refresher
- APT38 Workshop Scenario

Host Analyst: APT38 Exercise

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Apply knowledge gained in APT38 workshops, with less guidance, to identify all indicators, including possible changes in TTPs.

Outcomes

- Identify host-based indicators of compromise linked to APT38.
- Detect APT38 malicious activity.

Host Analyst: APT40 Workshop 1

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Examine APT40 TTPs through a defensive lens using the MITRE ATT&CK framework and known indicators of compromise.

Outcomes

- Identify network indicators of compromise linked to APT40.
- Characterize APT40 malicious activity.
- Given an intrusion by APT40, determine network IOCs that are present.

Host Analyst: APT40 Workshop 2

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Examine a potential attack chain that uses APT40 TTPs, and conduct threat hunting to identify indicators of compromise.

Outcomes

- Identify host indicators of compromise linked to APT40.
- Characterize APT40 malicious activity.
- Given an intrusion by APT40, determine host IOCs that are present.

Host Analyst: APT40 Exercise

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Apply knowledge gained in the APT40 workshops, with less guidance, to identify all indicators, including possible changes in TTPs.

Outcomes

- Identify networking indicators of compromise attributed to APT40.
- Detect malicious activity indicative of APT40.
- Given an APT40 intrusion, determine which host IOCs are present.

ICS Foundations: Attacks

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to different ICS attack methodologies and frameworks, such as the MITRE ATT&CK framework and the DHS ICS Attack framework. In addition, various ICS-focused malware are discussed and used as examples of threats faced by ICS environments.

Outcomes

- Mitre ATT&CK framework
- Attack overview

ICS Foundations: Introduction

Foundational

Publisher: SimSpace

Individual

3.25 hours

Description

An introduction to industrial control systems, including the principles of ICS security and the similarities, differences. Also includes the general types of operational controls found in industrial control systems, and a discussion of the concepts of vulnerability and risk management in an ICS context.

Outcomes

- Describe industrial control systems, including the principles of ICS security and the similarities, differences, and correlations with the cybersecurity principles of confidentiality, integrity, and availability.
- Identify the general types of operational controls found in industrial control systems.
- Identify concepts of vulnerability and risk management in an ICS context.

ICS Foundations: Modbus-CLI and PLC Interaction

Foundational

Publisher: SimSpace

Individual

2 hours

Description

An overview of Modbus-CLI, a free and open source tool for interacting with PLCs over the Modbus TCP protocol. It covers installation, basic usage, important options, how to modify the tool for custom use, and offensive and defensive use.

Outcomes

- Use the Modbus-CLI (command line utility).
- Read and write values to PLCs.
- Understand and manipulate data communication.
- Review offensive use cases and potential defensive strategies.

ICS Foundations: Network Defense

Foundational

Publisher: SimSpace

Individual

3 hours

Description

Introduction to the concepts of incident response as applied to ICS environments, detailing strategies and techniques for detecting, containing, and recovering from cybersecurity events. The tools Elastic and GRASSMARLIN are used.

Outcomes

- Incident response preparation
- Anomaly detection
  - Malicious activity indicators
- Network intrusion detection systems
- Network security monitoring
- Containment
- Eradication

ICS Foundations: PLCs and Ladder Logic

Foundational

Publisher: SimSpace

Individual

2 hours

Description

An explanation of Ladder Logic, a fundamental language used for programming PLC, and a demonstration of how to use Ladder Logic to write a simple PLC program in OpenPLC Editor.

Outcomes

- Describe ladder logic.
- Identify examples of basic ladder logic diagrams, contacts, and coils.
- Use the OpenPLC Editor to create basic PLC programs.
- Load the program into the OpenPLC Runtime PLC simulator.

ICS Foundations: Protocols

Foundational

Publisher: SimSpace

Individual

9 hours

Description

Introduction to a variety of protocols used in ICS and IT environments, and an analysis of common IP-based ICS protocols using Wireshark.

Outcomes

- Identify protocols used in ICS and IT environments, focusing on lower-level protocols typical to industrial networks.
- State common threats facing ICS networks.
- Recommended mitigation tactics.
- Use Wireshark filters and features.
- Analyze Modbus traffic.
- Identify ICS packet data anomalies.

ICS Foundations: Ransomware

Foundational

Publisher: SimSpace

Individual

2 hours

Description

An introduction to cyber threat emulation (CTE) for a SamSam-style attack.

Outcomes

- Conduct a cyber threat emulation (CTE) for a SamSam-style attack.

Identifying Indicators of Compromise

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Under the framework of the Pyramid of Pain, which is a stratified glimpse of the potential indicators of a network intrusion, this module introduces you to several increasingly difficult-to-recognize artifacts of attempted and successful intrusions.

Outcomes

- Identify the nature, origin, and limitations of several indicators of compromise.
- Use deductive techniques and open-source research to identify Indicators of Compromise.

Integration Testing in CI

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

The practice, tools, and automation of integration testing in continuous integration (CI).

Outcomes

- Describe the impact of code libraries on software development.
- Install library packages with pip.
- Implement a container-based deployment environment.
- Interpret data from an automated integration testing pipeline.

Kibana Data Visualization

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Use Kibana's native search application to create data visualizations of a simulated network environment.

Outcomes

- Use Kibana's data aggregation tools to visualize trends in large datasets.
- Use Kibana to create a visualization that shows how DNS traffic on a network has changed over time.
- Combine multiple visualizations in a dashboard view.

Kibana: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Kibana is an open-source data visualizer application that enables search and visualization capabilities of a data set. Examine the interesting and powerful use of Kibana as the front end of an integrated Security Incident and Event Manager (SIEM).

Outcomes

- Use Kibana as a data visualization platform to identify the initial point of compromise on a network.
- Use Kibana as a data visualization tool to identify the destination of exfiltrated data on a network.

Kibana SIEM Application

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Use insights from data visualizations to investigate threats using the Kibana SIEM application.

Outcomes

- Investigate suspicious network activity using the Kibana SIEM.
- Use filters in the Kibana SIEM to examine data and identify downloaded files.

Linux Firewall

Foundational

Publisher: SimSpace

Individual

3 hours

Description

An introduction to the Linux firewall using iptables.

Outcomes

- Identify which iptables rule matches a packet.
- Evaluate iptables chains and policies.
- Configure the Linux firewall to allow remote system management access.
- Configure firewall rules to load on system boot.

Mind Maps

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Explores how to create and use mind maps for identifying tasks and creating milestones to achieve mission success.

Outcomes

- Discuss mind maps.
- Produce a mind map laying out tasks and milestones.

MITRE ATT&CK Framework

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Explore the MITRE ATT&CK framework tactics and how it relates to attack lifecycle phases. Explores the MITRE ATT&CK Navigator and walks through creating a new layer.

Outcomes

- Discuss the MITRE ATT&CK Framework.
- Discuss the MITRE ATT&CK Navigator.
- Create new MITRE ATT&CK Navigator layers.

MITRE ATT&CK Practical Use

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Use the ATT&CK framework to identify known adversarial threat activity. In conjunction with the ATT&CK framework, the Mordor Project is used to test a detection strategy or rule against malicious events for a given APT.

Outcomes

- Map threat activity to the MITRE ATT&CK matrix.

MITRE ATT&CK Threat Mapping

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

Covers mapping real-world threat actor activity onto the MITRE ATT&CK matrix.

Outcomes

- Discuss ATT&CK Navigator layers.
- Map threat actor activity onto the MITRE ATT&CK matrix using ATT&CK Navigator.

Modifying Zeek Scripts

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Zeek includes a robust scripting engine that enables customization that expands the usefulness of Zeek both as a command-line tool and as a network sensor. Learn the basics of Zeek scripting, including common use cases and how to write a custom script, execute that script, and further modify it to return additional data

Outcomes

- Identify use cases for Zeek scripting.
- Run a custom Zeek script.
- Modify a Zeek script.

Network Analyst Exercise: Network Threat Hunting

Intermediate

Publisher: SimSpace

Individual

3.5 hours

Description

Discover and scope an attack using threat hunting skills such as hypothesis development and pivoting in a lab environment.

Outcomes

- Combine network security monitoring and SIEM tools to investigate threats on a network.
- Explain the role of a hypothesis in threat hunting.
- Use a SIEM to investigate plausible hypotheses of adversary behavior.
- Determine the scope of a breach by pivoting off of related indicators, discovering previously unknown indicators, and using those to discover further infection.

Network Analyst Walkthrough: ASCII and JSON Logging

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

A walkthrough follow-on exercise for the module ASCII and JSON Logs: Interpreting and Processing.

Outcomes

- Use Linux built-ins to find indicators of compromise.

Network Analyst Walkthrough: Modifying Zeek Scripts

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

A walkthrough follow-on for the module Modifying Zeek Scripts that guides you through modifying and customizing Zeek scripts to identify anomalous network activity.

Outcomes

- Modify a Zeek script to extract certain file types from a packet capture.
- Use Zeek to parse a pcap file and identify anomalies from a packet capture file.
- Create a custom Zeek script to analyze and detect malicious packets from a packet capture.

Network Analyst Walkthrough: Packet Capture and Analysis

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

A walkthrough follow-on to the Packet Capture and Analysis module. Investigate a potential network compromise and determine basic facts about the break-in. Use packet capture analysis methodology to determine the initial point of compromise, the point of origin of the malware, the beaconing interval of the malware agent,
and more.

Outcomes

- Using packet capture analysis methodology, identify the following about a given packet capture file:
  - The initial point of compromise.
  - The malicious server's hostname and IP address.
  - The hostname and IP address of the point of data exfiltration.
  - The names of exfiltrated files.
  - The malware agent's beaconing interval.
  - The malware agent's web resources used during beaconing.
  - The name of the initial document that began the compromise.

Network Device Configuration

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Fundamentals of network devices, establishing network connections between devices, and managing and troubleshooting device connections.

Outcomes

- Identify the different types of network devices and their functions within a network.
- Using the command line interface, statically configure a host's IP address to communicate across different networks.
- Using the command line interface, configure a router for Dynamic Host Control Protocol (DHCP) to dynamically assign IP addresses within a subnet.
- Using the router command line interface, configure a router to enable Secure Shell (SSH).
- Using SSH, remotely configure the router for DHCP.
- Describe general troubleshooting steps for basic network device connectivity.

Network Firewalls

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Types of network firewalls and the analysis and creation of firewall rules.

Outcomes

- Differentiate between the various types of network firewalls, based on their features, advantages, and disadvantages.
- Analyze a set of firewall rules to identify how they are processed.
- Create firewall rules in pfSense.

Network Remediation: Introduction

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Remediating a network after an attack. Includes factors to consider and recommending options based on specific pcaps.

Outcomes

- Identify factors to consider when recommending remediation.
- Recognize the role attacker persistence plays in network remediation.
- Recommend remediation actions based on method of compromise.
- Given scenarios, recommend best course of action for remediation.

NetworkMiner: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

NetworkMiner makes artifact extraction an easy task by automating the process. An introduction to using the interface version of the tool on Windows and Linux.

Outcomes

- Identify the primary purpose of NetworkMiner for a blue team analyst.
- Use NetworkMiner to:
  - Identify hosts in network traffic.
  - Identify filenames of artifacts.
  - Determine the content of artifacts.
  - Find unencrypted email communication details.
  - Demonstrate artifact extraction from a pcap.

Open-Source Intelligence (OSINT) Techniques

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Explores various methods to conduct intelligence gathering through open sources.

Outcomes

- Collect intelligence via various open-source methods.
- Identify various tools and techniques to gather OSINT.

Operational Security 101

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Examines aspects of Operational Security (OPSEC) with a focus on cybersecurity.

Outcomes

- Describe OPSEC as it applies to defensive cyber operations.
- Identify various methods and techniques of ensuring OPSEC.

Parsing Network Traffic with Zeek

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

How and why to use Zeek to parse network traffic, both live and static via pcap files. Participate in a scenario exercise and parse three pcap files with malicious traffic. After parsing pcap files, analyze Zeek logs and describe which Indicators of Compromise are present within the captures.

Outcomes

- Configure Zeek to listen on a single network interface.
- Parse pcap data into Zeek logs.
- Analyze Zeek logs to identify suspicious activity.

PowerShell: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Use PowerShell to interact with a Windows operating system to complete beginner-level administrative tasks.

Outcomes

- Create, modify, and execute custom PowerShell scripts.
- Get help in PowerShell by using the Get-Help command.
- Interpret PowerShell elements including objects, aliases, variables, and arrays.

Secure Coding

Intermediate

Publisher: SimSpace

Individual

0.75 hours

Description

An introduction to the concept of secure coding that includes identifying some of the most common software security risks and providing programming countermeasures that are used in a secure code review.

Outcomes

- Describe the purpose and importance of secure coding.
- Apply secure coding best practices.
- Summarize common programming countermeasures.
- Perform a secure code review.

Secure SDLC: Deployment and Maintenance

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine the fifth and sixth phases of the software development life cycle (SDLC) and helpful tools and techniques for incorporating security into them. Review the most effective testing techniques for a CI/CD pipeline.

Outcomes

- Identify key security concerns when deploying an application.
- Describe how containerization, web application firewalls (WAF), and runtime application self-protection (RASP) secure application deployment.
- Test a WAF that is protecting an application.
- Recommend methods for incorporating security into application maintenance.

Secure SDLC: Development

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine the third phase of the software development life cycle (SDLC) and tools and techniques that are effective for secure development in the SDLC. Review how to incorporate them into a CI/CD pipeline.

Outcomes

- Assess different methods for catching bugs in the development phase.
- Analyze code to identify vulnerabilities.
- Deploy software security tools into a CI/CD pipeline.

Secure SDLC: Requirements and Design

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine the first and second phases of the software development life cycle (SDLC) and tools and techniques that are effective for secure requirements gathering and design in the SDLC. Review how to incorporate them into a CI/CD pipeline.

Outcomes

- Recommend techniques for building security into the first two phases of the SDLC.
- Identify appropriate security requirements for an application.
- Recognize correct threat modeling for an application.

Secure SDLC: Testing

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Examine the fourth phase of the software development life cycle (SDLC) and helpful tools and techniques for incorporating security in it. Review the most effective testing techniques for a CI/CD pipeline.

Outcomes

- Identify suitable security unit tests.
- Recognize the benefits of DAST.
- Contrast DAST and IAST.
- Conduct fuzz testing to identify vulnerabilities.
- Evaluate appropriate applications of penetration testing in a secure SDLC.
- Identify the role of SCA in securing an application's third-party packages.

Security Operations Center (SOC) Overview

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

An overview of a Security Operations Center, including the roles and functions of those who work in it, and the skills required for a SOC analyst.

Outcomes

- Define SOC.
- Describe the primary functions of the people working in a SOC.
- Identify the main tasks done in a SOC.
- Choose which SOC architecture is most appropriate for a given organization.
- Contrast the roles and responsibilities of the different levels of SOC analysts.

Security Testing

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Security testing concepts, as well as a hands-on demonstration of incorporating static, dynamic, and software composition analysis testing tools into a software development pipeline.

Outcomes

- Describe the importance of continually testing code for vulnerabilities.
- Define security requirements.
- Conduct a risk analysis.
- Formulate a test plan.
- Differentiate between white, black, and gray box testing.
- Compare and contrast various application security testing tools.
- Practice using security testing tools to scan code.
- Interpret results from a scan.
- Describe how to incorporate security testing into a development pipeline.

SIEM: Conceptual Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Review common SIEM functions, including dashboard composition and log aggregation. Use two common SIEM products, Splunk Enterprise Security and Elastic SIEM, to perform simple searches on a simulated corporate network and correlate log information.

Outcomes

- Describe a SIEM's core functions.
- Explain the SIEM's main function in the context of information security.
- Describe the components of a SIEM.
- Execute a simple search in Kibana to correlate information about user activity on the network.
- Execute a simple search in Splunk to correlate information about user activity on the network.

SIEM: Practical Introduction

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

An introduction to using Security Information and Event Management (SIEM) software, with hands-on labs that use Elastic Stack.

Outcomes

- Discuss how a SIEM deployment is commonly architected.
- Identify various parts and pieces of a SIEM solution.
- Identify methods to deploy log forwarders.

SIEM Walkthrough: Incident Response

Advanced

Publisher: SimSpace

Individual

1 hour

Description

A walkthrough follow-on for Elastic and Splunk SIEM modules: A suspected network breach has occurred on the SOMECORP network. Use everything you've learned about log analysis, event correlation, and indicators of compromise to identify the key facts about this malicious break-in.

Outcomes

- Using a Security Information and Event Management (SIEM) platform, identify key facts about a network intrusion:
  - Identify the network intrusion's point of origin on the internal network.
  - Identify portscanning against internal hosts.
  - Determine the adversary's initial foothold and privilege escalation method.
  - Identify the malicious domain used to install post-compromise malware.

Sigma: Introduction

Intermediate

Publisher: SimSpace

Individual

0.5 hours

Description

Leverage Sigma to turn indicators of compromise into a customized Kibana query to discover infected hosts.

Outcomes

- Use Sigma to identify key features of a malicious binary to write a SIEM-agnostic rule for detection.
- Convert the general Sigma rule into a Kibana-specific query to find malicious activity.
- Use Kibana to visualize the Intrusion Detection Signature (IDS) signatures going into the network and use this information to find malicious user behavior.

SIP Telephony

Intermediate

Publisher: SimSpace

Individual

0.75 hours

Description

An overview of the voice protocol and Session Initiation Protocol (SIP) and an explanation of SIP vulnerabilities and attacks.

Outcomes

- Understand the SIP protocol.
- Identify various SIP vulnerabilities.
- Locate SIP attack indicators using an Elastic Stack.

SOC: Incident Response

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

An explanation of Incident Response and how it works in a Security Operations Center (SOC).

Outcomes

- Define incident response.
- Describe how SOC analysts respond to incidents.
- Identify the typical tools used to perform incident response.
- Choose appropriate courses of action when presented with an incident response scenario.

SOC: Security Monitoring

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

An overview of the roles, responsibilities, and tools involved in the Security Monitoring function of a Security Operations Center (SOC).

Outcomes

- Define security monitoring.
- Describe how SOC analysts monitor the network and endpoints.
- Identify the typical tools used to perform security monitoring.
- Choose appropriate courses of action when presented with a security monitoring scenario.

SOC: Threat Hunting

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

An introduction to the role and functions of threat hunting in a Security Operations Center (SOC).

Outcomes

- Define threat hunting.
- Describe how SOC analysts hunt for threats.
- Identify typical tools used to perform threat hunting.
- Choose appropriate courses of action when presented with a threat hunting scenario.

Splunk Configuration and Data Ingestion

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Install and configure a basic Splunk instance on a local network. Load data into Splunk and extract custom fields to enhance Splunk Search and return more refined results.

Outcomes

- Install Splunk.
- Configure the Splunk web interface to use SSL.
- Import local compressed data into Splunk.
- Query data in Splunk for artifacts.

Splunk Enterprise Security

Advanced

Publisher: SimSpace

Individual

1.5 hours

Description

An introduction to Splunk Enterprise Security (ES), Splunk's SIEM offering. Covers the installation of Splunk ES and its basic use, including using built-in alerts to detect DNS exfiltration. Additionally, use Sigma to create a custom Splunk search to quickly identify infected network hosts.

Outcomes

- Identify the number of assets and identities in a static Assets & Identities configuration file.
- Use cross-correlated information to identify Indicators of Compromise on a network:
  - Use Enterprise Security correlation searches to identify DNS tunneling.
  - Use Suricata signatures to correlate events with a host to find unauthorized Peer to Peer (P2P) torrent client activity.
- Use Sigma to identify key features of a malicious binary to write a SIEM agnostic rule for detection.
- Convert the general Sigma rule into a Splunk specific query to find malicious activity.

Splunk Forwarders and Normalization

Foundational

Publisher: SimSpace

Individual

1 hour

Description

How Splunk Technology Add-ons pair with the Universal Forwarder to create CIM-compliant data. Install and configure the Splunk Universal Forwarder on a Windows VM and enable the Windows TA to view normalized data in real-time. Also, learn how TAs impact search-time by performing a custom CIM mapping.

Outcomes

- Create a new index to use with Splunk Technology Add-on.
- Enable monitoring and configure Splunk Technology Add-on.
- Install the Splunk Universal Forwarder on a Windows VM.
- Identify when a custom CIM is required.

Splunk Incident Investigation

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Taking on the position of a basic cyber protection analyst, use Splunk to navigate through an investigation of a realistic cyber incident.

Outcomes

- Perform the necessary steps to leverage Splunk as an investigation tool.
- Discuss the scope of the incident investigation.
- Analyze the incident investigation.

Splunk Overview

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

The Splunk Security Information and Event Management (SIEM) and its use in operational environments.

Outcomes

- Discuss Splunk architecture.
- Identify various methods of ingesting data.
- Identify how to configure the Splunk forwarder.

Splunk Post Incident Investigation Actions

Foundational

Publisher: SimSpace

Individual

1 hour

Description

How to operationalize Splunk to meet the needs of a cyber protection team, employing actions taken during the incident investigation lesson to create reports, alerts, and dashboards aimed at the identification of future malicious cyber activity.

Outcomes

- Operationalize Splunk concepts to identify malicious cyber activity.
- Create Splunk reports, alerts, and dashboards.

Splunk Searching

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Use Splunk for data searching and visualization. Become familiar with Splunk search terminology. Write Splunk queries, view events, build a transforming search, and optimize searches.

Outcomes

- Write advanced queries.
- Conduct anonymous and wildcard searches.
- Build a transforming search.
- Use search optimizations.

Suricata: Introduction

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

The installation and configuration of Suricata, a network security monitoring tool often used as an intrusion detection system. Includes ruleset management and briefly introduces custom rules.

Outcomes

- Identify situations in which IDS would be an effective tool for network security.
- Explain the difference between Suricata's main logging formats.
- Configure Suricata.
- Update and deploy rulesets for Suricata.
- Write and deploy a simple custom Suricata rule.

Suricata Rule Writing

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

Write rules using Suricata to catch malicious traffic. This covers the basic parts of a Suricata rule, techniques to minimize noise, using pcaps to develop rules, and Perl Compatible Regular Expressions.

Outcomes

- Identify reasons to use a Suricata rule.
- Identify the parts of a Suricata rule.
- Write a basic Suricata rule that is functional.
- Write rules that use progressively more advanced rule writing concepts.

System Monitor (Sysmon)

Foundational

Publisher: SimSpace

Individual

1 hour

Description

This module introduces System Monitor (Sysmon) from Windows SysInternals. It describes the steps to install and configure Sysmon and view its generated logs.

Outcomes

- Install Sysmon and view output.
- Create a custom configuration for Sysmon.
- Use Sysmon data to identify a threat.

Threat Hunting in Windows Files

Foundational

Publisher: SimSpace

Individual

1 hour

Description

How to analyze Windows files for indicators of malicious activity. Includes hands-on labs using magic numbers, examining basic steganography, and finding alternate data streams.

Outcomes

- Identify anomalies in digital signatures.
- Validate digital signatures.
- Identify files using a hex editor and magic bytes.
- Explain two methods of file obfuscation.
- Use two hashing methods to analyze files.
- Analyze alternate data streams.
- Identify the methods attackers use for file downloads.

Threat Hunting Physical Devices

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

A walkthrough follow-on for Elastic and Splunk SIEM modules: A suspected network breach has occurred on the SOMECORP network! You must use everything you've learned about log analysis, event correlation, and indicators of compromise to identify the key facts about this break-in.

Outcomes

- Gain a foothold in the Site.com internal network.
- Pivot into the Corp.lan internal network.
- Gain access to the Corp.lan domain controller as a domain administrator.

Threat Hunting with IOCs Exercise

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Use your threat hunting skills to uncover indicators of compromised and infected hosts.

Outcomes

- Identify network indicators of compromise.
- Pivot off of network indicators of compromise.
- Identify host indicators of compromise.
- Pivot off of host indicators of compromise.

Threat Hunting with IOCs Workshop

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Indicators of compromise in networks and hosts and how to use pivoting to threat hunt.

Outcomes

- Describe indicators of compromise.
- Explain types of network and host indicators.
- Describe how IOCs are used in threat hunting.
- Describe the Pyramid of Pain and where different indicators fit on it.
- Identify network indicators of compromise.
- Pivot off of network indicators of compromise.
- Identify host indicators of compromise.
- Pivot off of host indicators of compromise.

Threat Hunting with MITRE ATT&CK®

Foundational

Publisher: SimSpace

Individual

2.5 hours

Description

Gather and operationalize threat intelligence using the open-source tool Atomic Red Team in conjunction with the MITRE ATT&CK® framework.

Outcomes

- Identify APT TTPs using ATT&CK Navigator.
- Map APT activity to the MITRE ATT&CK framework.

Threat Modeling

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Learn to decompose, classify, and visualize threats to an IT system with STRIDE, OWASP Threat Dragon, and more!

Outcomes

- Classify a vulnerability using CVSS.
- Describe how to apply the OWASP Threat Modeling Process.
- Categorize a threat using STRIDE.
- Use OWASP Threat Dragon to create a threat diagram.

Unit Testing in CI

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Tools and techniques for sustainably increasing software development quality and speed: Test-driven development (TDD), unit testing in continuous integration, and test automation.

Outcomes

- Identify traits of an effective unit test.
- Describe the process and features of TDD.
- Create unit tests.
- Determine the advantages of pytest.
- Test software developed through TDD.
- Automate unit testing.

Volatility: Introduction

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

Learn memory forensic techniques by using one of the leading tools to investigate and identify the memory image of a compromised machine.

Outcomes

- Identify active processes in acquired memory image.
- Find relevant files in acquired memory image.
- Identify parameters and use patterns for the Volatility tool.

Vulnerability Remediation

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Provides the concepts relating to remediating or mitigating vulnerabilities, including CVSS, remediation options, and remediation plan development.

Outcomes

- Interpret a vulnerability's severity based on its Common Vulnerability Scoring System (CVSS) score.
- Develop a vulnerability remediation plan based on best practices and organizational risk appetite and tolerance.

Windows Event Forwarding

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An introduction to Windows Event Forwarding (WEF) which reads operational or administrative event logs and forwards the events to you via a subscription.

Outcomes

- Describe the purpose of Windows Event Forwarding.
- Describe the two WEF subscription types.
- Create a WEF subscription.

Windows Libraries: Introduction

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Describes the function and capabilities of the libraries for the Windows operating system, as well as attacks that utilize libraries.

Outcomes

- State the purpose of libraries within the Windows OS.
- Perform basic analysis of the functions of a library.
- Discuss the impact of malicious use of libraries in a defense context.

Windows Memory Analysis: Introduction

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Walk through the steps of memory acquisition, collecting volatile data from Windows systems. Learn foundational memory analysis techniques that aim to identify malicious code and rogue activity.

Outcomes

- Perform memory dump.
- Validate processes running in memory.
- Find relevant files.

Windows Processes: Introduction

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Learn about the composition of processes in the Windows operating system, and perform enumeration of those processes with UI and command line tools.

Outcomes

- Identify the fundamentals of several different OSs and their corresponding internals.
- Understand the use and function of processes within the Windows OS.
- Discuss the impact of the Windows OS and its corresponding internals on Defensive Cyberspace Operations (DCO).

YARA and Signature-Based Writing

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Use the powerful and flexible open-source pattern matching YARA tool, written in the C programming language, to run, write, and customize rules to identify and classify malware.

Outcomes

- Scan a file with YARA.
- Scan a directory with YARA.
- Identify common YARA use cases.
- Write a custom YARA rule.

Red Team Training

Red Team Training

Boot2Root Workshop 1

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Use industry tools to identify and exploit vulnerabilities to gain remote access and control of a network host. Targets are Linux OS, WordPress, and MySQL.

Outcomes

- Determine and analyze attack surfaces.
- Identify vulnerabilities.
- Execute exploits to gain access and privilege escalation.
- Document results.

Boot2Root Workshop 2

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Use industry tools to identify and exploit vulnerabilities to gain remote access and control of a network host. Targets are Linux OS and MySQL.

Outcomes

- Identify vulnerabilities.
- Execute exploits to gain access and privilege escalation.
- Document results.

Boot2Root Workshop 3

Intermediate

Publisher: SimSpace

Individual

4 hours

Description

Use industry tools to identify and exploit vulnerabilities to gain remote access and control of a network host. Target is Linux OS, and techniques include steganography, MIB manipulation, MD5 cracking, and open-source research.

Outcomes

- Determine and analyze attack surfaces.
- Identify vulnerabilities.
- Execute exploits to gain access and privilege escalation.
- Document results.

Boot2Root Workshop 4

Advanced

Publisher: SimSpace

Individual

2 hours

Description

Use industry tools to identify and exploit vulnerabilities to gain remote access and control of a network host. Targets are Linux OS and OpenNetAdmin.

Outcomes

- Determine and analyze attack surfaces.
- Identify vulnerabilities.
- Execute exploits to gain access and privilege escalation.
- Document results.

Credential Management and Harvesting

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Techniques for identifying and harvesting credentials in Windows. The hands-on lab provides multiple opportunities to harvest credentials, followed by a challenge lab.

Outcomes

- Identify the common locations of credentials in Windows.
- Describe what Mimikatz does.
- On a given system, escalate privileges to local Administrator by harvesting credentials.
- On a given system, dump SAM hashes with Mimikatz.
- Demonstrate hash cracking with John the Ripper.

Cyber Offense Walkthrough: Red Lightfoil

Foundational

Publisher: SimSpace

Individual

8 hours

Description

A red team companion to the Cyber Defense Challenge: Blue Lightfoil, providing a walkthrough of the attacker's actions.

Outcomes

- Conduct an attack which emulates APT41.
- Connect actions done from the red side with information found during the blue investigation.

Defeating CSRF Protections with XSS

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Common defense techniques against cross-site request forgery (CSRF) and demonstration of how to defeat them using cross-site scripting (XSS).

Outcomes

- Recognize when a CSRF token is present as a defensive measure.
- Execute a CSRF exploit to overcome CSRF tokens.
- Recognize when a SameSite cookie attribute is present as a defensive measure.
- Execute a CSRF exploit to circumvent a SameSite "strict" setting on session cookies.

Empire Installation, Configuration and Basic Use

Foundational

Publisher: SimSpace

Individual

2 hours

Description

This module introduces Empire, the open-source C2 platform, and its installation and basic usage.

Outcomes

- Identify the manual installation key components on Ubuntu.
- Identify OS level dependencies.
- Identify Empire configuration options and requirements.
- Identify key components for establishing baseline C2 communications.
- Identify key concepts for the Empire command line.
- Identify common troubleshooting installation and configuration Issues.

Enumeration: Introduction

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

An introduction to the enumeration phase of the penetration testing methodology. This module covers tools and techniques for enumeration of common network services.

Outcomes

- Use Nmap to fingerprint a remote OS.
- Use Netcat to perform banner grabbing.
- Use penetration testing tools to enumerate network services.

Exploit Public-Facing Application: MITRE ATT&CK® Red

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An overview of the LAMP stack and HTTP basics, with a lab that covers common web attacks (SQL injection, cross-site scripting, and local file inclusion).

Outcomes

- Given the description of a vulnerability, identify the appropriate attack to exploit it.
- Demonstrate how attackers leverage weaknesses in web applications to bypass authentication.
- Demonstrate how attackers leverage injection, cross-site scripting, and file inclusion attacks to compromise web-facing applications and extract data.

Initial Access

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

An introduction to gaining initial access to a remote system. This overview provides some of the standard methods of gaining initial access to a remote system and how to carry out some of those techniques.

Outcomes

- Apply phishing and spear-phishing tradecraft to conduct campaigns.
- Build weaponized documents to drop an initial payload.
- Use drive-by attack links in conjunction with spear-phishing to gain access.
- Utilize spear-phishing to conduct credential harvesting to gain valid account access.
- Identify components of social engineering and apply them to gain initial access.
- Apply the information gained by scanning to identify public-facing application vulnerabilities.

Invoke-PSImage: Steganography

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Employ steganography using Invoke-PSImage and embed a PowerShell script inside of a picture. After you use Invoke-PSImage in an attack, flip the role and try to find out what happened.

Outcomes

- State how Invoke-PSImage conceals malicious code.
- Use Invoke-PSImage to embed a malicious script into an image.
- Detect traces of Invoke-PSImage as a defender.

Kerberoasting: MITRE ATT&CK® Red

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to the Kerberos protocol and SecureAuthCorp™'s Impacket toolkit, a suite for interacting with Active Directory environments in Python. You will be able to use Kerberos to extract cryptographic material from a domain controller, and then prosecute this material to increase network presence in an Active Directory domain.

Outcomes

- Use impacket to extract AS-REP and TGS-REP values from a target.
- Use John the Ripper to recover weak passwords from this authentication data.

Lateral Movement

Intermediate

Publisher: SimSpace

Individual

4 hours

Description

An introduction to using the compromise of a single network device to expand access within a target network. In the context of a red team intrusion, use the credentialed lateral movement techniques of PsExec, WMI, WinRM, and scheduling remote tasks.

Outcomes

- Take over a Windows device using the following methods:
  - Co-opt SMB using PsExec and recovered passwords.
  - Windows Management Instrumentation (WMI) commands.
  - Co-opt SMB using recovered passwords, a lateral tool transfer, and creating a remote scheduled task.
  - Co-opt Windows Remote Management with PowerShell using recovered passwords.

Local File Inclusion (LFI): Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Local file inclusion (LFI), its relationship to other exploitations, and hands-on LFI exploit labs.

Outcomes

- Execute an LFI exploitation.
- Recognize vulnerabilities that LFI can exploit.
- Perform a directory traversal attack.
- Abuse file uploads and use LFI to gain RCE.
- Identify an RFI exploit.

Logic and Implementation Vulnerabilities

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

At a high level, learn about four of the OWASP Top 10 2017 web vulnerabilities. These vulnerabilities can be attributed to accidental misconfiguration or careless implementation mistakes, rather than directly to software vulnerabilities.

Outcomes

- Execute the reset of another user's password on a web service using weak authentication.
- Capture authentication information from an unencrypted exchange and replay it to access another user's account.
- Execute a brute-force search to access a hidden (otherwise unsecured) administrative interface through brute-force searching.
- Perform a data scraping from an exposed Elasticsearch database.

Metasploit Framework: Introduction

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Use MSFconsole for search functionality and database scanning. Includes a brief history of MSF and its uses as an offensive security tool, MSF functionality, and MSF command line interface via msfconsole.

Outcomes

- Use the db_nmap Metasploit module to enumerate a target host and determine its open ports.
- Stage and launch an exploit against a vulnerable web server using a Metasploit module to gain root-level access.
- Use the Meterpreter payload to perform post-compromise actions like credential harvesting.
- Use the auxiliary/analyze/crack_linux module to crack harvested credentials from within Metasploit Framework.
- Use the Metasploit SOCKS proxy server module and the proxychains command to perform a domain hashdump with secretsdump.py.

MSFvenom: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Pen testers and red teams often need to obtain a shell on a network machine and MSFvenom creates an encoded, customized shell payload tailored for the target and ready to deliver. Learn how to use MSFvenom as you select payloads and customize them. Prove your new skill by creating a payload that gives you a reverse shell on a network machine.

Outcomes

- Describe types of payloads available.
- Describe the function of common MSFvenom options for specifying payloads.
- Determine an appropriate payload for a given victim machine and OS.
- Generate a reverse-shell payload.
- Deploy a payload to get a reverse shell on a victim machine.

Network Configuration in Windows

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Manual and automated methods of network setup in a simplified Windows Active Directory (AD) environment, with a hands-on walkthrough of both methods.

Outcomes

- Statically configure a host's IP address.
- Configure a DHCP server to assign IP addresses dynamically.
- Review server logs to verify correct functioning.
- Use built-in Windows tools to test network connectivity.

Persistence

Foundational

Publisher: SimSpace

Individual

4 hours

Description

An introduction to "persistence", or surviving reboots and shutdowns, in the context of a red team intrusion solidifying their network presence. The Windows version of this module introduces the persistence techniques of registry "run" keys, scheduled tasks, and WMI.

Outcomes

- Install persistent malware on Windows using registry "Run keys".
- Install persistent malware on Windows using scheduled tasks.
- Install persistent malware on Windows using Windows Management Instrumentation.
- Install persistent malware on Windows as a Windows Service.
- Find examples of malicious scripts and executables configured to start on system startup on a Windows 10 virtual machine.

PowerShell Objects, Properties, and Methods

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

To automate tasks commonly used by analysts, build competence with PowerShell objects, properties, and methods.

Outcomes

- Manipulate objects using PowerShell.
- Manipulate properties using PowerShell.
- Manipulate methods using PowerShell.
- Create PowerShell functions.
- Export PowerShell functions.

PowerShell Script Creation Mechanics

Foundational

Publisher: SimSpace

Individual

1 hour

Description

A step-by-step guide demonstrating how to create PowerShell scripts and how to conceptualize them using pseudocode.

Outcomes

- Describe the process of developing a script.
- Employ PowerShell to construct a basic script.
- Discuss how scripting can be used as a network analysis tool.

Privilege Escalation

Intermediate

Publisher: SimSpace

Individual

2.5 hours

Description

How to overcome access control mechanisms in Windows using different techniques for gathering information and capitalizing on weaknesses to escalate your privileges.

Outcomes

- Identify the privileges of the current user.
- Describe what privilege escalation is.
- Exploit a vulnerable service to escalate user privileges.
- Conduct a DLL Hijacking attack to escalate user privileges.
- Exploit the domain controller to elevate a domain user to Domain Admin.

Protocol Basics

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

A primer on Ethernet, IP, TCP, UDP, ICMP, and ARP, and how protocol standards are established.

Outcomes

- Identify common service protocols, such as Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS).
- Identify common protocols and their functions.

Protocol Traffic Analysis Walkthrough

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Practical experience in protocol analysis through device discovery and using Wireshark to characterize and assess protocols and their uses within network traffic.

Outcomes

- Identify suspicious activity in Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP) web traffic captures.
- Analyze and break down packets to the byte level.

Ransomware Walkthrough: Scarlet Sunrise

Foundational

Publisher: SimSpace

Individual

8 hours

Description

This module examines host and network artifacts to investigate a cyber intrusion and ransomware attack.

Outcomes

- Gather evidence associated with the attack.
- Identify IOCs to inform intelligence feeds.
- Identify attacker infrastructure, such as domain names and IP addresses.
- Collect evidence to support subpoena and search warrant requests.
- Log evidence in an Incident Response timeline.

Removing Artifacts

Foundational

Publisher: SimSpace

Individual

2 hours

Description

Explore the various artifacts that can be left behind after an offensive network operation, and determine when and how to remove incriminating artifacts.

Outcomes

- Identify artifacts related to logging into a Windows workstation.
- Identify and remove artifacts related to logging into a Linux server.
- Identify console logging locations on Linux and Windows.
- Delete files securely after file identification.
- Determine appropriate techniques for hiding evidence of file deletion.

SQL and OS Injection: Introduction

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

SQL and OS injection vulnerabilities and exploitation with SQLmap and OS injection points.

Outcomes

- Describe SQL injection syntax.
- Describe the consequences of SQL injection.
- Explain how to exploit SQL injection to obtain authentication bypass.
- Explain how to exploit SQL injection to obtain database contents using SQLmap.
- Describe OS/command injection and consequences.
- Describe common syntax and OS injection points to test for.
- Explain how to use OS injection to read sensitive system files.

SQLi Attack Types

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

There are several variations of SQLi exploitation and data extraction that require more than the basic discovery and exploitation techniques. This module covers blind SQLi, out-of-band SQLi, and second-order SQLi.

Outcomes

- Verify the existence of blind SQLi vulnerabilities.
- Use Sqlmap to exploit blind SQLi vulnerabilities.
- Verify the existence of out of band SQLi vulnerabilities.
- Verify the existence of second-order SQLi vulnerabilities.
- Use Sqlmap to exploit second-order SQLi vulnerabilities.

sqlmap: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

The basics of sqlmap, an offensive tool used to detect and exploit SQL injection attacks on vulnerable web applications. Discover a vulnerable login form and exploit it with sqlmap to steal valid login credentials, as well as explore sqlmap's interactive shell option and attempt to obtain code execution on the target.

Outcomes

- Identify when to use sqlmap.
- Identify why manual input is sometimes better than sqlmap.
- Use common sqlmap input flags.
- Use sqlmap to scan a web application for injection vulnerabilities.
- Use sqlmap to extract data from a vulnerable database.
- Explore sqlmap shell options to enumerate potential host settings.

Supply Chain Compromise: MITRE ATT&CK® Red

Advanced

Publisher: SimSpace

Individual

4 hours

Description

Techniques involved in the Supply Chain Compromise (T1195), with three real-life case studies of compromises in the supply chain as well as a hands-on lab demonstrating how one could be conducted.

Outcomes

- Evaluate the attack surface of a generic supply chain.
- Use a software-based supply chain compromise to enumerate an internal network.
- Use a software-based supply chain compromise to take control of users of that software.

Threat Hunting with Splunk

Foundational

Publisher: SimSpace

Individual

2 hours

Description

This module provides a walkthrough of using Splunk to search for given IOCs.

Outcomes

- Identify evidence of compromise in a simulated enterprise network.

Vulnerability Enumeration

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An examination of the connection between scan results and existing vulnerabilities, highlighting several such datasets along the way.

Outcomes

- Identify existing vulnerabilities in a Server Message Block (SMB) server running on Windows XP SP0.
- Exploit found vulnerabilities in an SMB server running on Windows XP SP0.
- Identify a vulnerable application running on an HTTP server.
- Exploit a vulnerable application on an HTTP server.
- Identify a backdoor on an FTP server.
- Exploit an FTP server outfitted with a backdoor.

Web Application Fuzzing

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Introduces the idea of unstructured client requests to web applications, and some of the vulnerabilities that can ensue when these are not properly handled. Prominently featured is wfuzz, the Python fuzzing framework, but the lessons reach beyond the simple use of the tool.

Outcomes

- Enumerate hidden virtual hosts.
- Use a brute-force attack to obtain authentication information to access a web page.
- Identify a vulnerable header parameter in an insecure Internet of Things (IoT) device.

Web Vulnerabilities: Introduction

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Exploitation of web vulnerabilities with hands-on exploration of the most common weaknesses and vulnerabilities.

Outcomes

- Perform website exploration techniques to retrieve sensitive data from a web server.
- Perform exploitation techniques to gain remote code execution (RCE) on a simple web server.

Windows Droppers

Foundational

Publisher: SimSpace

Individual

4 hours

Description

Build a simple, disposable dropper to run a shellcode payload on a target Windows host.

Outcomes

- Compile a basic C++ dropper.
- Integrate Windows shellcode with a C++ dropper.

Wireshark: Introduction

Foundational

Publisher: SimSpace

Individual

1.5 hours

Description

Using Wireshark for packet capture analysis, with labs that use various filters and color-coding of rules.

Outcomes

- Identify Wireshark components.
- Define the purpose of various Wireshark functions.

XML External Entities (XXE) Attacks

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Explore XML External Entity (XXE) vulnerabilities, including how to leverage these vulnerabilities to extract sensitive information or compromise systems.

Outcomes

- Explain how to execute XXE injection attacks.
- Describe the impact of XXE attacks.
- Explain how to execute an XXE remote shell.
- Describe an XXE DoS attack.

Purple Team Training

Purple Team Training

Attacking with XSS

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

This module explores the impacts of the classic XSS vulnerability through various JavaScript walkthroughs and labs.

Outcomes

- Use enumeration to identify XSS vulnerabilities.
- Defeat XSS filters.
- Use XSS attacks to:
  - Modify a page
  - Intercept events
  - Exfiltrate data
  - Abuse the Same-Origin-Policy
  - Attack with externally hosted JavaScript

Basic Regular Expressions

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Introduction to regular expressions basics and extended regular expressions, with hands-on examples.

Outcomes

- Analyze basic and extended regular expressions to determine what strings they match.
- Create basic and extended regular expressions to match specific patterns.
- Create regular expressions that match specific patterns using the underlying regular expression engine.

Binary and Hex: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to binary and hexadecimal numbering, how and why the values are used in computing, and how to convert them.

Outcomes

- Perform basic arithmetic operations with binary and hexadecimal.
- Decode an IP address from binary into Base 10.
- Decode a MAC address from hexadecimal into binary.
- Identify why binary is used in computing.

Continuous Integration (CI) Overview

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

Fundamental principles for successful CI implementation.

Outcomes

- Recognize the components, terminology, and common tools of CI.
- Describe the practical and security benefits of CI.

Create or Modify System Process: MITRE ATT&CK® Purple

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

The sub-techniques of Create or Modify System Process (T1543), including this type of attack on Windows, macOS, and Linux. Create or modify system processes from the adversary's perspective and learn methods to detect these exploitation techniques.

Outcomes

- Create a malicious systemd service.
- Use Linux commands to audit persistent services.
- Use the Windows cmd line to create a malicious service.
- Detect persistent Windows services using Sysinternals Autoruns.

Cross-Site Request Forgery (CSRF): Introduction

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Cross-site request forgery (CSRF) vulnerabilities and how to exploit them.

Outcomes

- Create and launch a CSRF exploit that changes account information.
- Test anti-CSRF measures in a web application.

Cross-Site Scripting (XSS): Introduction

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

Three methods of cross-site scripting (XSS) attacks with an example of an XSS attack – session hijacking.

Outcomes

- Demonstrate a reflected XSS attack.
- Demonstrate a stored XSS attack.
- Demonstrate a DOM-based XSS attack.
- Explain how to hijack a session with an XSS attack.

Cyber Kill Chain®

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An overview of the Lockheed Martin Cyber Kill Chain®, including a practical exercise for "boot to root" exploitation against a vulnerable target machine. You will have the opportunity to execute all seven phases of the Cyber Kill Chain® in a hands-on environment.

Outcomes

- Given an attack scenario, provide the appropriate Cyber Kill Chain® phase that correlates with the attack.
- Demonstrate how attackers leverage every phase of the Cyber Kill Chain® to compromise a target system.
- Identify suspicious files or activities on a machine or target network.

Dirty COW

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

"Dirty COW" was a Linux kernel bug that affected operating systems that used a Linux kernel built between September 2007 and October 2016. This module explores ways it can be exploited to elevate any user to superuser privileges on an affected system, across several different Linux-based operating systems.

Outcomes

- Obtain superuser privileges on several Linux-based devices by taking advantage of Dirty COW.
- Choose the appropriate implementation of Dirty COW on a system-by-system basis to gain root privileges.

Files on Windows: Introduction

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

This module is a deep dive into what a file is on Windows systems and how the operating system reads that file in order to get the right application to launch the file.

Outcomes

- Identify file types with a hex editor.
- Count in binary.
- Use hex editor to fix file headers to recover file extensions.

Fuzzing: Memory Corruption Vulnerabilities

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Provides an introduction to the concept of fuzz testing and the use of a fuzzing framework.

Outcomes

- Describe the function and purpose of a fuzzer.
- Identify differences between fuzzing methodologies.
- Use a fuzzing framework to identify potential software bugs.

GDB: Introduction

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An introduction to debugging software with the GNU Debugger (GDB).

Outcomes

- Explain the role of symbols in a binary file.
- Set breakpoints using GDB.
- View variables in GDB.
- View CPU registers in GDB.
- Execute a program line-by-line.
- Debug a program.

Heap Overflows: Memory Corruption Vulnerabilities

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Introduces the concept of the heap overflow vulnerability, which includes details on how an attack is performed, and ways to protect against it.

Outcomes

- Describe the cause of a heap overflow.
- Perform a heap overflow attack.
- Explain methods of heap overflow prevention.

Indicator Removal on Host: MITRE ATT&CK® Purple

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

The techniques (T1070) that adversaries use to cover their actions. Examine each sub-technique through the eyes of an attacker, and then flip the script to detect the attack you conducted. After you detect your attack through the lens of a defender, implement a mitigation technique to prevent or provide early warning to a similar threat in the future.

Outcomes

- Clear Windows Event Logs, and detect and mitigate deletion.
- Remove all logs from /var/log on a Linux host, and detect and mitigate deletion.
- Clear command history in Bash and Powershell, and detect and mitigate deletion.
- Delete the file used to spawn connection from Meterpreter, and detect and mitigate file deletion.
- Use `net use` to map a share, collect data, and delete the share after use.
- Detect and mitigate network share removal.
- Upload a backdoor and match its timestamp to another binary to blend in, and detect and mitigate timestomping.

Insecure Deserialization and SSTI

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

Trusting user input is the root of many web vulnerabilities. This module covers two vulnerabilities that arise from trusting user input resulting in code being injected into the back-end web application.

Outcomes

- Locate an insecure deserialization vulnerability.
- Perform an exploit of an insecure deserialization vulnerability.
- Locate an SSTI vulnerability.
- Perform an exploit of an SSTI vulnerability.

Linux Configuration and Logging: Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Configuration and logging are the first line of defense against attackers. Identify Linux file types, directory structure, logs, and configuration files.

Outcomes

- Obtain the file type for a Linux file.
- Identify configuration file types and location.
- Identify log types and location.
- Use three methods to view configuration or log files.

Linux Internals

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Gain situational awareness on a target system by being able to manually gather baseline configuration data from Linux devices, including processes, services, and important file locations.

Outcomes

- Identify Linux processes and services.
- Identify important file paths and locations.
- Baseline a system.
- Detect anomalies.

Local Permissions on Windows

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An explanation of the six basic Windows permissions on a local machine for both users and groups, and their impact on access to files and folders.

Outcomes

- Identify the six Windows permissions.
- Explain/describe the six Windows permissions.
- Assign permissions for groups and users.
- Identify misconfigured permissions.
- Identify appropriate access controls for a given application.

Memory Corruption Vulnerabilities: Introduction

Advanced

Publisher: SimSpace

Individual

1 hour

Description

The fundamental concepts of memory corruption vulnerabilities, including the system components that are directly impacted and exploited by memory corruption vulnerabilities.

Outcomes

- Describe the system components targeted by memory corruption attacks.
- Explain the differences between assembly and machine languages.
- Describe the purpose of interpreted languages.
- Describe the purpose of compiled languages.

Nmap: Introduction

Foundational

Publisher: SimSpace

Individual

0.75 hours

Description

An overview of Nmap use cases and installation. Use Nmap to conduct network scans on a live range to validate a network diagram.

Outcomes

- Scan a network with Nmap.
- Identify hosts on a network.
- Detect open ports on network hosts.
- Optimize scan timing.

Open-Source Intelligence (OSINT): Introduction

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to the world of Open Source Intelligence. Open-Source Intelligence (OSINT) is a methodology of collecting data from publicly available sources and using contextual awareness and understanding to bring meaning to the data.

Outcomes

- Describe the purpose of OSINT.
- Identify sources and targets of OSINT.
- Navigate the OSINT Framework.
- Gather and interpret information gathered via OSINT.

OSI Model

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

The layers of the Open System Interconnection (OSI) model and interconnected network protocols.

Outcomes

- Understand the difference between the OSI Model and the TCP/IP Model:
  - Successfully identify relevant protocols per OSI layer.
  - Identify the usefulness of each step of the OSI model.

Packet Capture and Analysis

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Use Wireshark, a prominent open-source network analyzer tool, to capture network traffic, analyze a TCP stream, examine packet headers, extract objects from a TCP stream, and draw conclusions based on packet statistics.

Outcomes

- Start and run Wireshark to capture traffic on an interface.
- Analyze the composition of traffic on a network by examining the Wireshark Statistics menu item.
- Utilize the Wireshark Export Objects feature to extract requested HTTP resources from traffic on a network.
- Use Wireshark to analyze and identify a point of compromise on a live network.
- Analyze captured traffic to determine basic facts about a potential intrusion.

Perl Compatible Regular Expressions (PCRE)

Foundational

Publisher: SimSpace

Individual

1 hour

Description

The advanced features included in Perl Compatible Regular Expressions (PCRE) syntax, with examples and hands-on labs.

Outcomes

- Analyze PCRE regular expressions to determine what strings they match.
- Create PCRE to match strings following complex requirements.
- Create regular expressions that match specific patterns using the underlying regular expression engine.

Reverse Shells

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An examination of reverse shells, which are exploit payloads built to give a hacker a target-to-attacker connection that provides an interactive command-and-control session with the exploited device, in a variety of languages including Bash, PHP, Python, Perl, and the Windows cmd.exe.

Outcomes

- Use reverse shells written in several different programming languages.
- Select, from a variety of payloads, the most appropriate one for a given exploitation event.
- Decide on the next-best alternative for a chosen payload in case of failure.

Stack Overflows: Memory Corruption Vulnerabilities

Advanced

Publisher: SimSpace

Individual

1 hour

Description

Learn the fundamentals of stack overflow attacks and how to defend against them.

Outcomes

- Describe the cause of a stack overflow.
- Perform a stack overflow attack.
- Explain methods of stack overflow prevention.

Steal or Forge Kerberos Tickets: MITRE ATT&CK® Purple

Advanced

Publisher: SimSpace

Individual

2 hours

Description

Use powerful tools to extract Kerberos tickets by abusing the mechanisms of the Kerberos protocol.

Outcomes

- List components that make Kerberos an insecure protocol.
- Identify the characteristics of a Pass-the-Ticket attack.
- Demonstrate how to exploit the process with AS-REP roasting.
- Describe how to exploit a service account to steal and crack its credentials.
- Demonstrate how to escalate privileges and recover a krbtgt account's NTLM hash to forge a Golden Ticket.
- Describe how to exploit an application server and recover credentials to forge a Silver Ticket.
- Identify methods of detecting and mitigating sub-techniques.

Unsecured Credentials: MITRE ATT&CK® Purple

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

The sub-techniques of an unsecured credentials exploitation, including plain text password recovery, registry password harvesting, Group Policy Preference password decryption, and more. Perform credential harvesting from the adversary's perspective with offensive tools, and learn methods to mitigate this exploitation technique.

Outcomes

- Identify and describe the sub-techniques of ATT&CK TTP: Unsecured Credentials.
- Identify the risks associated with each sub-technique.
- Describe mitigation techniques for each sub-technique.
- Enumerate and recover unsecured credential sets through recursive file searching, enumeration scripts, and post-exploitation modules.
- Use acquired plain text credentials to move laterally across a target network.
- Decrypt a Group Policy Preference (GPP) encrypted password using the Kali Linux native gpp-decrypt tool.
- Use compromised private key credentials to move laterally across a target network.

Web Application Exploitation

Foundational

Publisher: SimSpace

Individual

1 hour

Description

Two infamous web application exploits: struts-pwn and Drupalgeddon2. Review examples of how each has been used. Assume the role of a cyber adversary to scan, enumerate, and exploit these web applications to gain unauthorized access to a server. Additionally, explore basic indicators of compromise (IOC).

Outcomes

- Identify the primary methods by which struts-pwn and Drupalgeddon2 can compromise a vulnerable web server.
- Identify live hosts on a network by performing a basic Nmap ping-sweep.
- Using open-source intelligence and directory and service enumeration scanning techniques, identify websites that use Apache Struts and Drupal.
- Select the best uses of the Searchsploit tool from a given list.
- Obtain a user shell on a vulnerable host by identifying, preparing, and launching web application exploits.

Windows Command Line and Administration

Foundational

Publisher: SimSpace

Individual

1 hour

Description

An introduction to using the Command Prompt window, as well as basic commands and fundamental administrative tasks, such as adding users and groups.

Outcomes

- Use at least two methods to open a Command Prompt window.
- Create a new directory in a relative or absolute path.
- Use Help to construct a command that utilizes parameters.
- Add a new user.
- Delete a user.
- Add a user to a local group.

Windows Internals: Introduction

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

An entry-level look at basic concepts on how Windows works on the inside, including core elements of services, drivers, and processes on Windows.

Outcomes

- Identify running processes on Windows.
- Find drivers running on Windows.
- Query and find service information on Windows.

Windows Logging and Monitoring

Foundational

Publisher: SimSpace

Individual

1 hour

Description

This module covers Windows logging and enables you to identify common event logs in Windows and gain an understanding of Windows security auditing. It also prepares you to configure and identify verbose PowerShell logs.

Outcomes

- Explain the function, types, and locations of Windows logs.
- Explain the basic purpose of audit policy.
- Configure Security Logging.
- Conduct basic forensic investigations using Windows logs.
- Configure PowerShell Logging.
- Use PowerShell Logging to investigate a malicious process.

Windows Logging: Introduction

Foundational

Publisher: SimSpace

Individual

2 hours

Description

The function and location of various Windows logs, the function of Audit Policy, and the difference between forensic and alert-based uses of logs. Also, how logs can be used to investigate an attack on a network.

Outcomes

- Explain the function, types, and locations of Windows logs.
- Explain the basic purpose of the audit policy.
- Describe the difference between alert-based and forensic uses of Windows logs.
- Conduct basic forensic investigations using Windows logs.

Windows Registry: Introduction

Foundational

Publisher: SimSpace

Individual

0.5 hours

Description

This module explains the Windows registry and why it exists, and covers principles about the registry which could lead to security issues.

Outcomes

- Edit the registry to change a setting.
- Scan the registry and list startup tasks.
- Identify how the registry can pose a security risk.

XXE Attacks and SSRF Vulnerabilities

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

XML External Entity attacks can face interesting challenges when attempting to retrieve files more complicated than /etc/passwd or when the results of the XML parsing are not shown to the user. This module describes how to face these challenges to exploit XXE vulnerabilities. It also shows how to capitalize on access that XXE attacks give to exploit SSRF vulnerabilities.

Outcomes

- Exploit blind XXE vulnerabilities.
- Perform a retrieval of arbitrary files via XXE vulnerabilities on PHP web apps.
- Reach an internal application using SSRF vulnerabilities.

Cyber Crisis Training

CurveBall: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

A how-to guide for the CurveBall vulnerability, or CVE-2020-0601, including a walkthrough and methods to prevent an incident.

Outcomes

- Explain two types of attacks that can be accomplished by exploiting CurveBall.
- Complete the process of forging a web certificate that passes validation.
- Forge a signed executable that runs and returns a reverse shell.

Dirty Pipe: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

Dirty Pipe (CVE-2022-0847) is a Linux local privilege escalation exploit that allows unprivileged users to write arbitrary data to locations on the Linux file system regardless of access rights. This module covers Dirty Pipe from the offensive and defensive perspectives and includes hands-on exploitation labs.

Outcomes

- Identify the call to kernel resources that exposes the vulnerability.
- Describe the steps which reproduce this vulnerability through the splice syscall.
- Describe mitigations for the Dirty Pipe exploit.

Follina Defense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

The background of CVE-2022-30190 Follina, a Microsoft Office vulnerability, along with detection and mitigation.

Outcomes

- Detect an exploitation of Follina using Sysmon logs.
- Mitigate Follina by modifying the registry.

Follina Offense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

1.5 hours

Description

The background of CVE-2022-30190 Follina, a Microsoft Office vulnerability, along with an explorations of the vectors needed to create a malicious document that utilizes the exploit to run commands on a target device.

Outcomes

- Create a malicious document (“maldoc”) that uses CVE-2022-30190 to exploit a target user.
- Use variations of CVE-2022-30190 that alter the manner of user interaction required to trigger the exploit.

Log4Shell Defense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An explanation of the Log4Shell exploit from a defensive perspective. Includes background and hands-on mitigation. Learn how Log4j (CVE-2021-44228) functions and potential mitigation techniques.

Outcomes

- Identify the vulnerability in the Log4j package that allows exploitation.
- Locate vulnerable Log4j installations.
- Apply mitigations for the Log4Shell exploit.

Log4Shell Offense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

1 hour

Description

An explanation of the Log4Shell exploit from an offensive perspective. Includes background and hands-on exploitation. Learn how Log4j (CVE-2021-44228) functions and use it against vulnerable targets in a range.

Outcomes

- Perform the steps to stage the Log4Shell exploit.
- Perform the exploit.

PrintNightmare Defense: Legacy Threat

Advanced

Publisher: SimSpace

Individual

1.5 hours

Description

An outline of the “PrintNightmare” exploit (CVE-2021-34527) from a defensive/protector perspective. Includes background information on CVE-2021-34527 as well as details on some confusion surrounding the publication of the vulnerability.

Outcomes

- Identify indicators of a potential attack using CVE-2021-34527 and the Elastic SIEM.
- Explain various mitigations for CVE-2021-34527 and their impact on a domain.

PrintNightmare Offense: Legacy Threat

Advanced

Publisher: SimSpace

Individual

1 hour

Description

An outline of the “PrintNightmare” exploit (CVE-2021-34527) from an offensive/attacker perspective. Includes background information on CVE-2021-34527 as well as details on some confusion surrounding the publication of the vulnerability.

Outcomes

- Use CVE-2021-34527 to elevate privileges on a Windows 10 workstation.
- Use CVE-2021-34527 to remotely take control of a Windows domain controller.

ProxyLogon Defense: Legacy Threat

Advanced

Publisher: SimSpace

Individual

1 hour

Description

An outline of the “ProxyLogon” exploit (CVE-2021-26855) from a detection and mitigation perspective. Due to a server-side request forgery vulnerability, this exploit allows an attacker to send arbitrary HTTP requests and authenticate as the Microsoft Exchange server.

Outcomes

- Detect ProxyLogon in a lab environment.
- Explain how to mitigate ProxyLogon.

ProxyLogon Offense: Legacy Threat

Advanced

Publisher: SimSpace

Individual

1 hour

Description

An outline of the “ProxyLogon” exploit (CVE-2021-26855) from an offensive/attacker perspective. Due to a server-side request forgery vulnerability, this exploit allows an attacker to send arbitrary HTTP requests and authenticate as the Microsoft Exchange server.

Outcomes

- Gain a foothold on an Exchange server using ProxyLogon.
- Perform post-compromise activity after using ProxyLogon for code execution.

PwnKit Defense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

2.5 hours

Description

How to detect and prevent PwnKit in your environment. Includes background information on the Linux local privilege escalation exploit, discovering vulnerabilities and detecting PwnKit exploitation.

Outcomes

- Prevent PwnKit exploits by removing the SUID bit from /usr/bin/pkexec.
- Verify a system is not vulnerable to PwnKit by testing a PwnKit exploit.
- Observe PwnKit exploits using Auditd rules.
- Observe PwnKit exploits using /var/log/secure.

PwnKit Offense: Legacy Threat

Intermediate

Publisher: SimSpace

Individual

2 hours

Description

How attackers use PwnKit, a Linux local privilege escalation exploit, to gain superuser privileges in Linux. Includes background, and a walkthrough of running a PwnKit exploit.

Outcomes

- Obtain superuser privileges on a Ubuntu 20.04 device using CVE-2021-4034.
- Obtain superuser privileges on a CentOS 7 device using CVE-2021-4034.

Zerologon: Legacy Threat

Foundational

Publisher: SimSpace

Individual

2 hours

Description

This presents the “Zerologon” exploit: CVE-2020-1472. A high-visibility exploit, Zerologon lets any attacker with a foothold in the domain accelerate straight to domain administrator privileges. Includes a brief walkthrough of how the exploit works, then how to use it, how to detect it, and what to do to mitigate it.

Outcomes

- Use CVE-2020-1472 to elevate to domain administrator on a Windows domain controller.
- Repair the damage done to the domain controller using the exploit proof-of-concept.
- Identify Windows Event Logs potentially related to using the exploit proof-of-concept.
- Identify solutions to remediate the domain after a cataclysmic attack.

SECURE WITH CONFIDENCE

simspace.com info@simspace.com

SIMSPACE