TryHackMe Journal - Ian K. Marusak

Instructions

(1) Review the sample journal entry provided below
(2) Scroll down to find the name of the room you have been assigned/are working on
(Pro Tip: Turn on "Outline View" so you can navigate more easily - go to View → Show Outline)
(3) Complete the required rooms on TryHackMe, compiling notes as you work through the room. This might include:
  (a) Commonly used Code/Commands
  (b) Definitions/Explanations of important terms and concepts
  (c) Screenshots of useful diagrams
(4) Once you've completed the module, capture 2-4 important takeaways.
(5) After you get the hang of things, delete these instructions and the sample you were provided!

Instructions
- Entry 1- SAMPLE
  - Room Name: Linux Fundamentals 1
- Entry 1
  - Room Name: Linux Fundamentals 1
- Entry 2
  - Room Name: Linux Fundamentals 2
- Entry 3
  - Room Name: Linux Fundamentals 3
- Entry 4
  - Room Name: Intro to Logs
- Entry 5
  - Room Name: Wireshark Basics
- Entry 6
  - Room Name: Windows Fundamentals 1
- Entry 7
  - Room Name: Windows Fundamentals 2
- Entry 8
  - Room Name: Windows Fundamentals 3
- Entry 9
  - Room Name: Windows Forensics 1
- Entry 10
  - Room Name: Windows Forensics 2
- Entry 11
  - Room Name: Intro to Log Analysis

Entry 12
    Room Name: Splunk Basics
Entry 13
    Room Name: Incident Handling with Splunk
Entry 14
    Room Name: Splunk 2
Entry 15
    Room Name: Splunk 3
Extra Rooms
Extra Rooms Pt. 2
Extra Rooms Pt.3
Extra Rooms Pt. 4
Extra Rooms Pt. 5

Entry 1- SAMPLE

Room Name: Linux Fundamentals 1

Date Completed: 12/20/2023
Notes During the Room:

- Similar to how you have different versions of Windows (7, 8 and 10), there are many different versions/distributions of Linux.

Command	Description
echo	Output any text that we provide
whoami	Find out what user we're currently logged in as!

Command	Full Name

ls	listing
cd	change directory
cat	concatenate
pwd	print working directory

Symbol / Operator	Description
&	This operator allows you to run commands in the background of your terminal.
&&	This operator allows you to combine multiple commands together in one line of your terminal.
>	This operator is a redirector - meaning that we can take the output from a command (such as using cat to output a file) and direct it elsewhere.
>>	This operator does the same function of the `>` operator but appends the output rather than replacing (meaning nothing is overwritten).

Important Takeaways

- Linux is an OS, like Windows. There are many different versions of Linux that serve different purposes.
- Linux systems rely more heavily on the command line to do tasks, like navigate the file system.
- Same basic commands while working with files are ls, cd, cat and pwd

Entry 1

Room Name: Linux Fundamentals 1

Date Completed: 10/26/24
Notes During the Room: Linux is an operating system, like Windows or MacOS, but it’s used everywhere—smartphones, cars, servers, and more. Linux Basics: Get familiar with Linux's history and why it's so widely used. Basic Commands, navigating files, learning to move around and manage files in Linux, finding files & Operators, practice finding files and using simple shortcuts to make tasks faster.

Important Takeaways:
Hands-On Practice

Entry 2

Room Name: Linux Fundamentals 2

Date Completed: 10/26/24
Notes During the Room:
Linux is a widely used, lightweight operating system that powers many everyday devices and critical infrastructures. It’s open-source, with multiple versions (distributions) like Ubuntu and Debian, each suited to specific tasks.

Important Takeaways:
Linux is versatile and operates in various settings, from websites to industrial systems, due to its open-source nature. Different distributions of Linux, like Ubuntu, offer flexible setups for servers, desktops, and low-resource environments.

Entry 3

Room Name: Linux Fundamentals 3

Date Completed: 10/26/24
Notes During the Room:
Just keep learning the system

Important Takeaways:

Entry 4

Room Name: Intro to Logs

Date Completed: 10/26/24
Notes During the Room:
Logs serve as critical records of past events, offering insights that help strengthen security and protect assets. Effective log analysis is essential to detect patterns and respond to potential threats promptly.
Logs capture system activity in detail, including events like logins, file access, and network connections, and are essential for understanding and responding to digital incidents. By analyzing logs, patterns emerge that help answer crucial questions about what happened, when, where, who was involved, and the impact of these actions.

Important Takeaways:
Learning to analyze logs and understanding logging tools and techniques enable swift detection of incidents and bolster readiness against threats. This training covers the significance of logs, different logging methods, and practical skills to counter adversaries through log analysis.
In this scenario, a systems administrator at SwiftSpend Financial uses logs to identify an adversary's actions on a web server, using limited sudo privileges and log analysis tools. Logs provide valuable insights through contextual correlation, transforming individual entries into a coherent narrative that can guide effective response actions.

Entry 5

Room Name: Wireshark Basics

Date Completed: 11/23/24
Notes During the Room:The Wireshark Basics room on TryHackMe is part of the SOC Analyst 1 path, teaching foundational skills in network and packet analysis using Wireshark. This walkthrough covers key tasks like tool overview, packet dissection, navigation, and filtering to build practical knowledge for SOC roles. Additional resources, including live and on-demand training, are available to deepen understanding.
Important Takeaways:
Wireshark is a critical tool for SOC analysts, enabling real-time packet capture and protocol analysis. Mastering packet navigation and display filters is essential for efficiently analyzing network traffic. Hands-on practice and continued training help reinforce skills for real-world applications.

Entry 6

Room Name: Windows Fundamentals 1

Date Completed:
Notes During the Room:
The desktop and taskbar simplify navigation by providing quick access to files, applications, and settings.
The file system is organized hierarchically, with folders and file extensions indicating content types.
User Account Control (UAC) restricts unauthorized system changes by requiring administrative approval.
The Control Panel and Settings app allow users to manage system configurations and preferences.
Task Manager is a critical tool for monitoring processes, managing startup programs, and resolving performance issues.
Important Takeaways:
Navigation tools like the taskbar and desktop streamline workflow.
The file system structure is essential for managing and accessing data.
UAC is a vital security feature that prevents unauthorized changes.
The Control Panel and Settings app are central hubs for managing system settings.
Task Manager is indispensable for monitoring and optimizing system performance.

Entry 7

Room Name: Windows Fundamentals 2

Date Completed: 11/25/24
Notes During the Room:
System Configuration (msconfig) is used to manage startup processes, troubleshoot boot issues, and configure services.
Computer Management integrates tools like Event Viewer, Disk Management, and Shared Folders for system administration.
Resource Monitor provides real-time data on system performance, including CPU, memory, disk, and network usage.
Event Viewer logs system events, which are critical for diagnosing errors or monitoring security incidents.
Device Manager ensures hardware devices are properly installed and functional by managing drivers.
Important Takeaways:
System Configuration is essential for customizing and troubleshooting system startup.
Computer Management centralizes administrative tools for easier access and control.
Resource Monitor is invaluable for diagnosing and optimizing resource usage.
Event Viewer helps monitor and diagnose system and security events.
Device Manager is critical for maintaining hardware functionality.

Entry 8

Room Name: Windows Fundamentals 3

Date Completed: 11/29/24
Notes During the Room:
Windows Update: Provides security patches and updates through mandatory cycles like "Patch Tuesday," ensuring devices remain secure and up to date.
Windows Defender: Includes real-time protection, ransomware safeguards, and cloud-delivered updates, with options to customize scans and manage threats.
Firewall & Network Protection: Manages traffic via Domain, Private, and Public profiles, supported by SmartScreen and exploit protection to block malicious activity.
Core Isolation & BitLocker: Core Isolation secures critical processes, while BitLocker and TPM offer robust encryption and device security.
Volume Shadow Copy Service (VSS): Creates restore points for recovery but requires offline backups to defend against ransomware attacks.
Important Takeaways:
Regular updates and patches are critical for protecting against vulnerabilities.
Windows Defender and Controlled Folder Access proactively guard against threats and malware.
Firewalls and SmartScreen block unauthorized network and web activity.
Core Isolation, Memory Integrity, and BitLocker secure processes and sensitive data.
Offline backups are essential to ensure recovery when restore points are compromised.

Entry 9

Room Name: Windows Forensics 1

Date Completed: 11/29/24
Notes During the Room:Computer forensics for Windows focuses on analyzing digital artifacts, particularly registry data, to uncover evidence of user activities such as file access, program execution, and device connections. The Windows Registry is a key database containing system configurations and user preferences, with specific keys and hives offering detailed forensic insights. Tools like KAPE, Registry Explorer, and Eric Zimmerman's utilities are used to extract, clean, and analyze registry data efficiently. Artifacts like ShimCache, AmCache, and ShellBags help reconstruct user actions, program usage, and external device connections. Effective analysis relies on proper data acquisition, including handling transaction logs and backups to ensure integrity and accuracy.
Important Takeaways:Windows systems generate and store a wealth of data that can be analyzed for forensic purposes, from identifying user activity to tracking connected devices. The Windows Registry plays a critical role in investigations, storing information about the system, user accounts, and recently accessed files or programs. Specialized tools streamline the extraction and interpretation of registry data, making it easier to locate significant forensic artifacts. Key artifacts like ShimCache and AmCache provide detailed information about program execution and system usage. Accurate forensic investigations require careful acquisition and processing of registry data to maintain data integrity and reliability.

Entry 10

Room Name: Windows Forensics 2

Date Completed: 11/30/24
Notes During the Room:Windows forensics involves investigating file systems (FAT, exFAT, NTFS) and artifacts like prefetch files, Jump Lists, and Timeline databases to trace user activity and program execution. NTFS offers advanced features like journaling, access controls, and a Master File Table (MFT), making it an essential focus for forensic analysis. Tools such as Autopsy, MFT Explorer, and Eric Zimmerman's utilities streamline the examination of forensic artifacts and system logs. Deleted files can often be recovered using tools like Autopsy, as long as their disk space has not been overwritten. Logs from USB devices, browser history, and shortcut files provide additional insights into external device usage and local file access.
Important Takeaways:Understanding file systems like NTFS is critical for effective forensic investigations due to their advanced features and comprehensive data storage. Tools like Eric Zimmerman's utilities and Autopsy are invaluable for parsing artifacts and recovering data without altering evidence. Forensic artifacts, such as prefetch files, Jump Lists, and Timeline databases, help reconstruct program execution and user behavior. Deleted files and data in unallocated disk space can often be recovered, highlighting the importance of proper imaging and analysis. External device logs and browser activity further enhance the ability to track system use and identify unauthorized access.

Entry 11

Room Name: Intro to Log Analysis

Date Completed: 12/4/24
Notes During the Room: Sigma is a YAML-based open-source tool designed for detecting log events, creating SIEM searches, and identifying threats by applying structured rules to log data. It simplifies threat detection by standardizing log event searches, specifying log sources, and including conditions like identifying failed SSH logins or handling false positives. Yara, on the other hand, is a pattern-matching tool widely used for malware analysis and log parsing, capable of detecting text, binary, and regex-based patterns such as IPv4 addresses. Both tools enable efficient log analysis workflows, offering unique capabilities tailored for specific use cases like SIEM integration with Sigma or granular pattern detection with Yara.
Important Takeaways:Sigma provides a structured approach to log event detection and SIEM integration, making it essential for streamlining threat analysis and identifying specific log patterns. Yara enhances analysis with

Entry 12

Room Name: Splunk Basics

Date Completed: 12/15/24

Notes During the Room: Splunk is a powerful SIEM tool that collects, processes, and analyzes log data from diverse sources like web servers, firewalls, and endpoints. Its core components include the Forwarder for data collection, the Indexer for data processing and storage, and the Search Head for querying and visualization. The interface consists of panels like the Splunk Bar, Apps Panel, Explore Splunk, and Dashboard, providing streamlined navigation and customization. Users can ingest logs through various methods, including uploading files directly, assigning source types, and indexing data for future analysis. Hands-on practice with Splunk's tools and challenge rooms like "Incident Handling with Splunk" and "PoshEclipse" sharpens skills in investigating security incidents.
Important Takeaways: Splunk simplifies log management and enhances visibility for incident detection and response. Mastering Splunk's components and SPL empowers effective investigations and threat hunting.

Entry 13

Room Name: Incident Handling with Splunk

Date Completed: 12/15/24
Notes During the Room: The Delivery Phase investigation revealed that the attacker used malware to gain initial access, with the file hash c99131e0169171935c5ac32615ed6261 identified as malicious and associated with the Poison Ivy group. This malware communicated with the C2 server at 23.22.63.114 and resolved the domain prankglassinebracket.jumpingcrab.com. Behavioral analysis showed that the malware established outbound connections, modified system configurations for persistence, and employed evasion techniques like obfuscation. Logs confirmed the delivery mechanism involved phishing or malicious links, with DNS and HTTP traffic providing evidence of communication with attacker infrastructure. Tools like ThreatMiner, VirusTotal, and Hybrid-Analysis highlighted the malware's activity, MITRE ATT&CK techniques, and potential secondary attack vectors.
Important Takeaways: The malware was delivered via phishing or malicious links and established communication with known malicious domains.
Behavioral analysis confirmed advanced tactics like obfuscation, persistence, and privilege escalation.
The domain prankglassinebracket.jumpingcrab.com served as a key C2 server in the attack.
Blocking identified domains, IPs, and training users on phishing risks is critical for prevention.
Logs and OSINT tools were vital in correlating malware activity with attacker infrastructure.

Entry 14

Room Name: Splunk 2

Date Completed: 1/21/205
Notes During the Room: Throughout this course, the focus was on developing investigative skills using the Splunk platform to analyze real-world datasets, specifically the BOTSv2 dataset. The exercises covered scenarios involving Advanced Persistent Threats (APTs), spear phishing campaigns,

ransomware, and unusual activity in corporate environments. Key tools and techniques included using Splunk Search Processing Language (SPL) to filter, refine, and extract actionable insights from massive datasets.

The course emphasized iterative searching, leveraging Interesting Fields, and correlating events across various data sources like HTTP, SMTP, and SSL logs. Participants explored how to identify indicators of compromise (IOCs), uncover attacker behavior, and trace malicious activity, such as file downloads, encrypted traffic, and command-and-control (C2) communications. External tools like CyberChef, VirusTotal, and Hybrid Analysis played a crucial role in supplementing Splunk searches, especially for decoding data and analyzing malware metadata. Exercises were designed to simulate real-world threat detection scenarios, requiring both technical skills and critical thinking.

Important Takeaways: This course underlined the importance of a systematic approach to threat detection and analysis. Mastering Splunk queries and understanding data relationships are critical for investigating APT activity. External tools complement internal analysis by providing deeper insights into malware and anomalies. Attention to detail, such as recognizing unusual filenames or correlating time-based events, can reveal critical pieces of evidence. Overall, the skills gained are directly applicable to real-world cybersecurity operations, particularly in SOC environments and incident response workflows.

Entry 15

Room Name: Splunk 3

Date Completed: 1/26/25
Notes During the Room: This room was a deep dive into the BOTSv3 dataset, providing challenges that required mastery of Splunk queries and analytical techniques. From identifying malicious activity on endpoints to uncovering command and control communications, the exercises emphasized both technical skills and creative problem-solving. Leveraging different source types like `stream:smtp`, `stream:http`, `XmlWinEventLog`, and `osquery`, the tasks simulated real-world scenarios to improve threat detection and investigation techniques. Exploring diverse paths to reach the same conclusions reinforced flexibility and adaptability in Splunk.

Additionally, focusing on specific fields like `CommandLine`, `dest_port`, `uri`, and `host` demonstrated the importance of narrowing down results for actionable insights. The dataset's comprehensive nature allowed for broader exploration, uncovering hidden patterns and additional indicators of compromise beyond the given challenges.

Important Takeaways:
This room showcased the importance of structured query building and iterative refinement in Splunk. The hands-on experience with BOTSv3 not only improved technical proficiency but also reinforced the

need to think creatively when analyzing large datasets. Mastering Splunk-fu involves both technical rigor and curiosity, and this exercise encouraged both.

EXTRA ROOMS

Room Name: Intro to Cloud Security

Date Completed: 12/22/24
Notes During the Room:
Cloud security involves a comprehensive strategy to protect data, applications, and infrastructure through various layers. Access management is a key element, ensuring that only authorized individuals perform tasks within their designated permissions, supported by role-based access control and multi-factor authentication. Policies provide governance by setting clear rules and conditions for user and resource actions. Network security safeguards cloud environments using tools like Security Groups and Network ACLs, complemented by vendor-specific solutions such as DNS Firewall and Network Firewall. Storage security ensures the protection of data both at rest and in transit through encryption, geographical restrictions, and role-based authorization. Disaster recovery strategies, including Cold, Warm, and Hot DR, ensure business continuity by tailoring recovery methods to meet specific operational needs. Monitoring and logging, enabled by tools like AWS CloudTrail and GuardDuty, provide real-time visibility into cloud operations, while automated patch management through AWS Systems Manager keeps resources updated and secure.
Important Takeaways:Cloud security is a layered and evolving process designed to address the unique risks associated with cloud environments. Encryption is essential for securing data both during transit and while stored, ensuring its confidentiality and integrity. Disaster recovery plans, such as Cold, Warm, and Hot DR, offer flexibility in balancing cost and recovery time, allowing organizations to maintain continuity during crises. Regular updates and patch management are critical to minimizing vulnerabilities and maintaining a strong security posture. Monitoring and logging tools are indispensable for detecting and responding to threats in real-time, ensuring ongoing protection. By leveraging the robust security tools and features offered by cloud providers, organizations can effectively safeguard their infrastructure while adapting to emerging threats in the dynamic cloud landscape.

Room Name: Intro to LAN

Date Completed: 12/22/2024
Notes During the Room:The OSI Model is a seven-layer framework that defines how devices communicate over a network. Each layer has a specific role, working together to ensure data is transmitted and received accurately and efficiently. Starting from the bottom, the Physical Layer handles the raw transmission of data as signals through hardware like cables and switches. The Data Link Layer manages MAC addresses and error detection, enabling reliable communication within local networks

Important Takeaways:This layered approach makes it easier to troubleshoot network issues by isolating problems to specific layers. TCP is ideal for tasks requiring accuracy, such as file transfers, while UDP is better for speed-critical applications like streaming. Encryption and standardization at the Presentation Layer ensure secure and compatible communication, while the Application Layer provides users with a seamless interface to interact with networked systems. Understanding the OSI Model is essential for network design and optimization.

Room Name: Packets & Frames

Date Completed: 12/22/24
Notes During the Room:Ports in networking are essential for facilitating data transfer, acting as channels between devices. They are represented by numerical values ranging from 0 to 65535, with common ports (0-1024) reserved for standardized protocols to ensure consistent communication. Examples include FTP on Port 21 for file sharing, SSH on Port 22 for secure system access, HTTP on Port 80 for web browsing, and HTTPS on Port 443 for encrypted communication. Custom ports outside this range can also be configured for specific applications, but standard ports ensure predictability and interoperability.
Important Takeaways:Ports provide a structured way for devices and applications to communicate over a network, with common ports supporting universal protocols and custom ports enabling flexibility. In the practical challenge, connecting to IP address 8.8.8.8 on port 1234 highlights the process of using ports to establish communication, demonstrating their importance in network functionality and application reliability. Successfully connecting and receiving a flag reinforces the understanding of how ports work in real-world scenarios.

Room Name: Extending Your Network

Date Completed: 12/22/2024
Notes During the Room:A router connects networks and facilitates the transfer of data between them using the process of routing, which operates at Layer 3 of the OSI model. Routing involves finding optimal paths for data delivery based on factors such as shortest route, reliability, and medium speed. Routers are configured through an interactive interface for tasks like port forwarding and firewalling. A switch is a networking device that connects multiple devices using Ethernet cables, operating at Layer 2 or Layer 3 of the OSI model. Layer 2 switches forward data based on MAC addresses, while Layer 3 switches perform additional routing tasks using IP addresses. VLANs on Layer 3 switches allow network segmentation for improved security and control over device communication.
Important Takeaways:Routers are crucial for inter-network communication and operate at Layer 3, using routing protocols to determine optimal paths for data. Switches connect devices within a network and can operate at Layer 2 for basic frame forwarding or at Layer 3 for routing capabilities. VLANs on Layer 3 switches provide network segmentation, enhancing security by isolating communication between different groups of devices while maintaining shared access to resources like the internet.

Room Name: DNS in Detail

Date Completed: 12/22/2024

Notes During the Room:DNS requests begin with the computer checking its local cache for previously resolved domain names. If no result is found, the query is sent to a Recursive DNS Server, typically provided by the ISP. Recursive servers also have a cache; if they lack the answer, they escalate the query to the Root DNS Server. The Root DNS Server identifies the appropriate TLD Server based on the domain extension, such as .com or .org. The TLD Server then directs the query to the Authoritative DNS Server, which holds all DNS records for the requested domain. Finally, the resolved information is returned to the Recursive DNS Server, cached for future use, and relayed to the original client. Responses include a TTL value, which specifies how long the record should be cached before expiration.
Important Takeaways:DNS caching at various levels reduces the need for repeated queries, improving efficiency and speed. The Recursive DNS Server, often provided by ISPs, is responsible for handling initial queries and caching responses. The Root DNS Server, TLD Server, and Authoritative DNS Server work together to resolve domain names to their corresponding records. The TTL (Time To Live) value determines how long a DNS record can be cached locally before requiring a new lookup. The DNS resolution process ensures users can access websites and services using human-friendly domain names instead of IP addresses.

Room Name: HTTP in Detail

Date Completed: 12/22/2024
Notes During the Room:Cookies are small pieces of data stored on your computer by a web server using the Set-Cookie header. Cookies are sent back to the web server with every request, enabling the server to remember information about the user, such as authentication or preferences. Cookies are particularly useful because HTTP is stateless and cannot remember previous interactions without them.
Important Takeaways:Cookies typically store tokens (unique secret codes) rather than clear-text data like passwords, ensuring security. You can view cookies in your browser’s developer tools under the "Network" tab, where requests and responses are detailed, including any cookie data sent or received.

EXTRA ROOMS PT.2

Room Name: How Websites Work

Date Completed: 12/29/2024
Notes During the Room: HTML injection occurs when a website fails to sanitize user input, allowing attackers to insert malicious HTML or JavaScript into the page. This happens because user inputs are directly displayed without filtering, letting attackers manipulate the website’s appearance or functionality. Developers must sanitize all user inputs to prevent malicious code execution, which is critical to maintaining both frontend and backend security. In the example provided, a malicious link to an external website could be injected into a vulnerable input field, showcasing the potential risks.
Important Takeaways: Always validate and sanitize user inputs to prevent vulnerabilities like HTML injection that comprise a website's security and functionality.

Room Name: Putting it all together

Date Completed: 12/31/2024
Notes During the Room: HTTP protocol. It can host multiple websites with different domain names by using virtual hosts, which match HTTP headers to configuration files. Static content, like images and CSS, remains unchanged, while dynamic content, such as blog updates or search results, is generated by backend languages like PHP or Python. Backend processes handle interactivity and data processing but are hidden from the client, who only sees the resulting HTML.
Important Takeaways: Web servers use virtual hosts to manage multiple sites, serve both static and dynamic content, and rely on backend languages to provide interactive features without exposing their underlying code.

Room Name: **Pentesting Fundamentals**

Date Completed: 12/31/2024
Notes During the Room: The post-exploitation stage begins once unauthorized access to a system is achieved, focusing on maintaining access and escalating privileges. Privilege escalation allows access to higher-level functions and sensitive files, enabling broader control of the system. Attackers may extract sensitive data and use the compromised system to pivot to other machines within the network. Covering tracks and documenting findings are essential components of this stage to simulate real-world attacker behavior and maintain a thorough report.
Important Takeaways: Post-exploitation is critical for understanding the potential impact of a breach, involving privilege escalation, data extraction, network pivoting, and stealthy operations to assess vulnerabilities comprehensively.

Room Name: Security Principles

Date Completed: 12/31/2024
Notes During the Room: Threat modeling identifies and mitigates potential threats and vulnerabilities in IT systems using frameworks like STRIDE, which addresses risks such as spoofing, tampering, and information disclosure. Incident Response (IR) is a structured process to handle security breaches, consisting of six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Both threat modeling and IR emphasize preparation, continuous review, and mitigation strategies to safeguard systems and maintain business continuity. Effective implementation requires a focus on threat intelligence, asset identification, and proper training to ensure resilience against attacks.

Important Takeaways: Key takeaways include the importance of using models like STRIDE to enhance system security by addressing common threats, and the critical role of incident response in mitigating risks and ensuring business continuity. Regular review, preparation, and training are essential components of maintaining a strong security posture.

Room Name: Walking An Application

Date Completed: 12/31/2024

Notes During the Room: The Network tab in Developer Tools tracks all external requests made by a webpage and is useful for analyzing data exchange. On the Contact page, filling out and submitting the form triggers an AJAX request, sending the data in the background without reloading the page. By monitoring this activity, you can locate the specific request generated by the form submission and examine its details. The flag is found within the response data of this request, visible in the Response tab.
Important Takeaways: The Network tab in Developer Tools tracks all external requests made by a webpage and is useful for analyzing data exchange. On the Contact page, filling out and submitting the form triggers an AJAX request, sending the data in the background without reloading the page. By monitoring this activity, you can locate the specific request generated by the form submission and examine its details. The flag is found within the response data of this request, visible in the Response tab.

Room Name: Content Discovery

Date Completed: 1/1/2025
Notes During the Room: Automated discovery uses tools to find hidden content on websites by making numerous requests to check for directories or files, relying on wordlists for common names. Wordlists are text files containing frequently used terms, like directory names, and an excellent resource for these is SecLists by Daniel Miessler. Tools like ffuf, dirb, and gobuster are commonly used for this purpose, with each providing different ways to scan websites and uncover hidden paths or files. Running these tools on the target website revealed hidden content such as directories and log files.

Important Takeaways: Automated discovery tools combined with curated wordlists are essential for efficiently identifying hidden resources on websites, often exposing critical paths or files.

Room Name: Subdomain Enumeration

Date Completed: 1/1/2025
Notes During the Room: Subdomain enumeration involves identifying subdomains for a domain to expand the attack surface and uncover potential vulnerabilities. Various methods like brute force, OSINT, and virtual host enumeration automate the discovery process, using tools like Sublist3r and dnsrecon. Certificate Transparency logs and search engine filters also assist in identifying hidden or previously unknown subdomains. Tools like `ffuf` further enhance enumeration by testing host headers with predefined wordlists to reveal subdomains hosted on shared servers.

Important Takeaways: The key takeaway is that subdomain enumeration is a critical cybersecurity process that utilizes multiple automated tools and techniques to discover potential vulnerabilities associated with subdomains.

Room Name: Authentication Bypass

Date Completed: 1/1/2025

Notes During the Room: Authentication vulnerabilities, such as plain text cookies and logic flaws, can allow attackers to escalate privileges, gain unauthorized access, or manipulate session data. Plain text cookies can be altered to modify roles, and encoding/decoding methods like base64 and hashing algorithms can reveal critical information. Tools like curl help test and exploit these weaknesses, such as bypassing privilege checks or manipulating reset processes. Understanding encoding and hashing methods enables security testers to decode and manipulate data for penetration testing.
Important Takeaways: Authentication vulnerabilities, when combined with weak session handling or encoding practices, can be exploited for unauthorized access and privilege escalation, making it crucial to secure these processes.

Room Name: IDOR

Date Completed: 1/1/2025
Notes During the Room: The username for user ID 1 is retrieved from the API by changing the `id` parameter to 1 and inspecting the JSON response. Similarly, the email address for user ID 3 is found by altering the `id` parameter to 3 in the same request and reviewing the data returned.
Important Takeaways: By manipulating parameters like `id` in API requests, it's possible to uncover sensitive information if an IDOR vulnerability exists. This highlights the importance of proper server-side validation.

Room Name: File Inclusion

Date Completed: 1/1/2025
Notes During the Room: The steps provided guided you through identifying and exploiting file inclusion vulnerabilities to capture the flags and gain RCE. Local File Inclusion (LFI) allowed you to access sensitive files like `/etc/flag1`, `/etc/flag2`, and `/etc/flag3` by manipulating URL parameters to traverse the file system. Remote File Inclusion (RFI) was exploited to execute the `hostname` command by including a malicious PHP file hosted on your server.
Important Takeaways: Understanding input validation weaknesses and proper payload crafting is critical for exploiting and protecting against file inclusion vulnerabilities in web applications.

EXTRA ROOMS PT.3

Room Name: Intro to SSRF

Date Completed: 1/5/2025
Notes During the Room: The SSRF room introduces the concept of Server-Side Request Forgery, where an attacker can manipulate a server to make requests to resources the attacker chooses. This vulnerability is dangerous because it can allow access to internal files, credentials, or even internal networks. There are two types of SSRF: regular, where the attacker sees the response, and blind, where there’s no direct feedback. Developers often use deny lists or allow lists to block dangerous requests, but these can be bypassed through tricks like alternative localhost references, directory traversal, or open redirects.

Important Takeaways: Understanding SSRF is essential because it shows how attackers can exploit server-side weaknesses to gain unauthorized access. Knowing where SSRF vulnerabilities appear, such as in URL parameters, and how to bypass security measures like deny lists and allow lists is key to protecting applications. The practical exercise demonstrated how to manipulate input fields to access restricted directories and decode base64 content to retrieve hidden flags, reinforcing how SSRF attacks work in real-world scenarios.

Room Name: Intro to Cross-site Scripting

Date Completed: 1/5/2025
Notes During the Room: Cross-site scripting (XSS) attacks are a form of injection where attackers embed malicious JavaScript into a web application, targeting other users' browsers. Reflected XSS involves injecting a script via a URL, while Stored XSS embeds malicious code that stays in the site's database. DOM-based XSS executes scripts directly within the user's browser through JavaScript interactions. Blind XSS is similar to Stored XSS but involves scenarios where attackers can't see the results themselves, often targeting administrative users with crafted payloads. I learned how to craft and adjust XSS payloads to bypass filters and adapt to various website scenarios.

The Blind XSS lab demonstrated how to create a support ticket payload that exfiltrates staff members' cookies to an attacker's listener using Netcat. By understanding how to set up a listener and construct the JavaScript payload to capture cookies, I saw how XSS can lead to session hijacking and unauthorized access. Successfully receiving the cookies via the listener confirmed the vulnerability's impact.

Important Takeaways: XSS vulnerabilities pose serious risks to web applications, including session hijacking, data theft, and unauthorized actions. Crafting and testing payloads is essential to understanding how to detect and prevent XSS attacks. Blind XSS can target administrative users, making it critical to secure all input fields and monitor for unexpected callbacks in web applications.

Room Name: **Command Injection**

Date Completed: 01/08/2025

Notes During the Room: In this room, I explored the concept of command injection, which is a web vulnerability that allows an attacker to execute system commands through an application. I learned how attackers can exploit functions in various programming languages, such as PHP and Python, to pass harmful input into the operating system. The room covered two main types of command injection: **blind** and **verbose**. Blind command injection occurs when there’s no direct output from the application, while verbose command injection provides clear feedback on the executed command. I practiced using payloads like `whoami`, `ls`, and `cat` to test for this vulnerability. Additionally, I learned how input sanitisation can help prevent command injection by ensuring user input is safe before processing it.

I also experimented with different ways to detect and exploit this vulnerability on a Linux-based system. Using shell operators like `;` and `&&`, I was able to combine commands and gain system information. I applied the practical element by identifying the user running the application and retrieving the contents of the flag file in `/home/tryhackme/flag.txt`. Testing these payloads showed me how versatile

command injection attacks can be and how important it is to implement secure coding practices to mitigate these risks.

Important Takeaways: Command injection is a critical web vulnerability that can give attackers direct access to the operating system through a vulnerable application. It can be detected in two ways: blind or verbose, depending on whether the output is visible. Preventing command injection involves careful input sanitisation and avoiding vulnerable functions. Through practical exercises, I've gained insight into how payloads can be used to test for this vulnerability, retrieve sensitive data, and understand the risk that poorly handled user input can pose to an application.

Room Name: SQL Injection

Date Completed: 01/08/2025
Notes During the Room: SQL Injection, also called SQLi, is a vulnerability where attackers manipulate database queries to access, modify, or delete data without permission. It occurs when user input is inserted into SQL queries without proper validation. A database is structured using tables with rows (records) and columns (fields) to store information, and SQL is the language used to communicate with databases. SQL commands like SELECT, INSERT, UPDATE, and DELETE allow interaction with the stored data. SQL Injection can take forms such as In-Band, Blind, and Out-of-Band, depending on how attackers execute and receive query results. In practical exercises, queries like UNION and SLEEP() helped identify vulnerabilities and retrieve data. Remediation involves prepared statements to separate queries from user inputs, input validation to restrict entries, and escaping special characters to avoid breaking queries.
Important Takeaways: SQL Injection is a critical security risk that can expose or compromise entire databases if input validation is weak. Developers must use secure coding practices, such as prepared statements, input validation, and escaping user input, to prevent SQL Injection attacks. Understanding SQL query structures and common injection techniques is essential for identifying vulnerabilities and protecting web applications.

EXTRA ROOMS PT. 4

Room Name: Burp Suite Basics

Date Completed: 1/21/2025
Notes During the Room: The room introduced the foundational aspects of Burp Suite, focusing on configuring the proxy, intercepting HTTP/S traffic, and understanding how to manipulate requests. I learned how to add targets to the scope to manage traffic effectively and explored a practical example of bypassing client-side filters to execute a reflected XSS attack. Using the Burp Proxy, I gained hands-on experience in capturing, modifying, and forwarding requests, emphasizing its critical role in manual testing. The integration of features like URL encoding and scoping settings simplified handling complex tasks and traffic filtering.
Important Takeaways: This session built a strong foundation for using Burp Suite in web application penetration testing. The ability to intercept and modify traffic, combined with scoping and practical examples like XSS exploitation, underscores the tool's power and importance. These skills will be invaluable for more advanced testing tasks in subsequent modules.

Room Name: Burp Suite: Repeater

Date Completed: 1/21/2025
Notes During the Room: Throughout the Burp Suite Repeater room, I learned how to manipulate and resend captured requests effectively. The tool’s intuitive interface allowed me to customize requests, experiment with headers, and observe responses in various formats, such as Pretty, Raw, Hex, and Render. By using Inspector, I was able to make higher-level changes, such as modifying query parameters and headers, which streamlined testing tasks. Practical exercises, like adding headers and exploiting SQL Injection vulnerabilities, showcased Repeater's real-world applications in testing endpoints and identifying security weaknesses. I also practiced crafting SQL queries to retrieve sensitive data, reinforcing my understanding of manual exploitation techniques.

Important Takeaways: Burp Suite Repeater is a powerful module for manual testing, enabling precise control over requests and responses. Its ability to handle repetitive tasks, combined with advanced features like Inspector and response visualization, makes it invaluable for identifying vulnerabilities such as SQL Injection. This room provided me with practical skills to confidently use Repeater in real-world security testing scenarios.

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

EXTRA ROOMS PT. 5

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:
Notes During the Room:

Important Takeaways:

Room Name:

Date Completed:

Notes During the Room:

Important Takeaways: