Week 2: Exploitation, Web Application Testing, and Advanced Networking

INT302: Kali Linux Tools and System Security – Lab 7: Practical Use Cases for Wireshark in Real-World Scenarios

Lab Overview

In this lab, participants will explore practical use cases for Wireshark in incident response and threat hunting scenarios. You will learn how to use Wireshark to analyze network traffic during security incidents, identify malicious activities, and gather evidence for forensic investigations.

Lab Objectives

By the end of this lab, you will be able to:

1. Use Wireshark to analyze network traffic in the context of an incident.
2. Identify indicators of compromise (IoCs) and malicious activities within network traffic.
3. Implement threat hunting techniques using Wireshark for proactive security measures.
4. Generate detailed reports of your findings to aid in incident response efforts.

Tools Used

- **Wireshark**: A graphical network protocol analyzer.
- **Tshark**: The terminal-based version of Wireshark.

Prerequisites

- Completion of Lab 6: Advanced Packet Analysis Techniques.
- Basic understanding of network security concepts.

Lab Steps

Step 1: Incident Response Analysis

1.Scenario Setup:

- You are part of the incident response team tasked with investigating a suspected data breach in your organization.
- Capture network traffic during the incident using Wireshark to analyze the packets and identify any suspicious activities.

2.Initial Traffic Inspection:

- Use Wireshark to open the captured traffic file.
- Apply filters to focus on traffic patterns during the incident. Key filters to consider:
- Ip.addr == <suspected IP> to focus on a suspected source.
- Tcp.port == <port number> to analyze specific application traffic.

Exercise 1:

- Describe the overall network traffic during the incident. Are there any noticeable spikes or anomalies? What potential indicators of compromise did you identify? _____

3. Extracting Suspicious Packets:

Look for specific indicators of compromise (IoCs) such as:

1. Unusual outbound connections to unknown IP addresses.
2. Repeated failed login attempts or suspicious authentication attempts.
3. Malicious payloads or command-and-control (C2) traffic.

Exercise 2:

- Identify a specific packet that raises suspicion. Provide details about the packet, including source and destination IPs, ports, and protocol. What makes this packet suspicious? _____

Step 2: Threat Hunting Techniques

1. **Proactive Threat Hunting:**

- Use Wireshark to perform proactive threat hunting within your network environment.
- Set up capture filters to monitor for specific behaviors or protocols often associated with threats (e.g., suspicious DNS queries or unusual traffic on uncommon ports).

Capture Filter Example:

To capture traffic on port 53 (DNS):

Tcp port 53 or udp port 53

Exercise 3:

- Implement a capture filter to monitor DNS traffic. Analyze the captured packets and summarize any findings related to unusual queries or connections. _____

2.Analyzing Suspicious DNS Traffic:

- Focus on DNS query packets to identify potential domain generation algorithms (DGAs) or connections to known malicious domains.

Exercise 4:

- Identify any DNS packets that may indicate a connection to a suspicious or malicious domain. Provide details about the domain queried and any associated IP addresses. _____

3.Detecting Anomalous Traffic Patterns:

- Examine the captured traffic for unusual patterns, such as:

1.Large data transfers to unknown destinations.

2.Outbound traffic during non-business hours.

Exercise 5:

- Document any anomalous traffic patterns you discovered. What does this suggest about potential malicious activity? _____

Step 3: Reporting Findings

Creating an Incident Report:

- Compile your findings into a detailed incident report. Include:
- Summary of the incident.
- Timeline of events.
- Indicators of compromise identified.
- Recommendations for remediation and prevention.

Exercise 6:

- Prepare an incident report based on your analysis. Include any relevant packet captures, screenshots, and detailed explanations of the findings. _____

2.Presentation of Findings:

- Present your findings to your peers or instructor, focusing on the analysis process and the conclusions drawn from the packet data.
- Discuss the importance of proactive threat hunting and incident response in maintaining network security.

Exercise 7:

- Create a presentation slide deck summarizing your lab experience, findings, and recommendations for improving incident response capabilities. _____

Conclusion

In this lab, you explored practical use cases for Wireshark in real-world scenarios, including incident response and threat hunting. By applying the skills you learned, you enhanced your ability to analyze network traffic and identify malicious activities, contributing to a more robust cybersecurity posture.

Next Steps

In the next lab, we will focus on advanced malware analysis techniques, exploring how to dissect and analyze malware behaviors using various tools.

INT302: Kali Linux Tools and System Security – Lab 8: Web Application Security Testing with Burp Suite and OWASP ZAP

Lab Overview

In this lab, participants will learn how to use Burp Suite and OWASP ZAP (Zed Attack Proxy) to perform web application security testing. These tools will enable you to identify vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and more.

Lab Objectives

By the end of this lab, you will be able to:

1. Configure and set up Burp Suite and OWASP ZAP for web application testing.
2. Perform basic web application scanning and vulnerability assessment.
3. Identify and exploit common vulnerabilities in web applications.
4. Document and report findings effectively.

Tools Used

- Burp Suite: A web application security testing tool.
- OWASP ZAP: An open-source web application security scanner.

Prerequisites

- Basic understanding of web technologies (HTML, HTTP, etc.).
- Familiarity with the OWASP Top Ten vulnerabilities.

Lab Steps

Step 1: Setting Up Burp Suite

1.Launch Burp Suite:

- Start Burp Suite from your Kali Linux environment.
- Choose the Community edition for this lab.

2.Configure Browser to Use Burp Proxy:

- Set up your browser (Firefox or Chrome) to route traffic through Burp Suite:
- Go to your browser settings.
- Configure the proxy settings to use 127.0.0.1 and port 8080.

3.Intercepting Traffic:

- Ensure that the “Intercept” feature is turned on in Burp Suite.

- Visit any web application, like http://testphp.vulnweb.com, to observe how Burp Suite captures and displays the traffic.

Exercise 1:

- Document the HTTP request and response headers for the home page of the target application. What information do you find in these headers? _____ **Step 2: Using Burp Suite for Vulnerability Scanning**

1.Spidering the Application:

- Use the Spider tool in Burp Suite to crawl the application and gather all available URLs. • Right-click on the target site in the site map and select "Spider this host."

Exercise 2:

- List the URLs discovered during the spidering process. Did you find any hidden or interesting pages? _____

2.Active Scanning:

- After spidering, select the site and choose "Scan" to start an active scan.
- Review the scan results to identify any vulnerabilities found.

Exercise 3:

- What vulnerabilities were detected by Burp Suite? Choose one vulnerability and explain how it could be exploited. _____

Step 3: Setting Up OWASP ZAP

1.Launch OWASP ZAP:

- Start OWASP ZAP from your Kali Linux environment.

2.Configure Proxy Settings:

- Similar to Burp Suite, configure your browser to route traffic through OWASP ZAP using 127.0.0.1 and port 8080.

3.Intercepting Traffic:

- Visit the same web application used in Burp Suite while OWASP ZAP is running.

Exercise 4:

- Capture and analyze the traffic with OWASP ZAP. What differences do you notice compared to Burp Suite? _____

Step 4: Using OWASP ZAP for Vulnerability Scanning

1.Automated Scanner:

- Utilize the “Quick Start” feature to run an automated scan on the target web application.
- Monitor the alerts generated by ZAP during the scan.

Exercise 5:

- Review the vulnerabilities identified by OWASP ZAP. Which tools detected the same vulnerabilities? What are the potential impacts of these vulnerabilities? _____

2.Active Scan:

- Perform an active scan by selecting the target site and initiating the scan.
- Review the detailed reports generated.

Exercise 6:

- Compare the findings of OWASP ZAP with Burp Suite. Which tool provided more detailed information? Which tool do you prefer for vulnerability scanning? Why? _____ **Step 5: Manual Testing Techniques**

1.Fuzzing:

- Use both tools to perform fuzzing against input fields in the web application (e.g., login forms, search fields).
- Attempt to inject various payloads to test for common vulnerabilities like SQL injection or XSS.

Exercise 7:

- Document any successful injections or errors encountered during fuzzing. What techniques were effective? _____

2.Review and Documentation:

Create a report summarizing your findings from both tools, including:

- Identified vulnerabilities.
- Suggested mitigations.
- Screenshots of significant findings.

Exercise 8:

- Prepare a report detailing the vulnerabilities discovered, your methodology, and recommendations for securing the application. _____

Conclusion

In this lab, you gained hands-on experience using Burp Suite and OWASP ZAP for web application security testing. You learned how to identify vulnerabilities and apply various testing techniques to assess the security of web applications effectively.

INT302: Kali Linux Tools and System Security – Lab 9: Information Gathering with Recon-ng and Shodan

Lab Overview

In this lab, participants will learn how to use Recon-ng, a powerful reconnaissance framework, and Shodan, a search engine for internet-connected devices. This lab will provide students with practical skills in gathering intelligence about targets and understanding the security landscape of connected devices.

Lab Objectives

By the end of this lab, you will be able to:

1. Set up and navigate Recon-ng for conducting reconnaissance.
2. Utilize Shodan to discover information about devices connected to the internet.
3. Extract valuable intelligence for penetration testing and security assessments.
4. Analyze and document findings effectively.

Tools Used

- Recon-ng: A full-featured Web Reconnaissance framework written in Python.
- Shodan: A search engine that lets users find specific types of computers connected to the internet using a variety of filters.

Prerequisites

- Basic understanding of reconnaissance techniques and tools.
- Familiarity with command-line operations in Linux.

Lab Steps

Step 1: Setting Up Recon-ng

1.Launch Recon-ng:

- Open your terminal in Kali Linux.
- Type recon-ng to start the framework.

2.Creating a New Workspace:

Create a new workspace for this lab:

- Workspaces create Lab9_Workspace

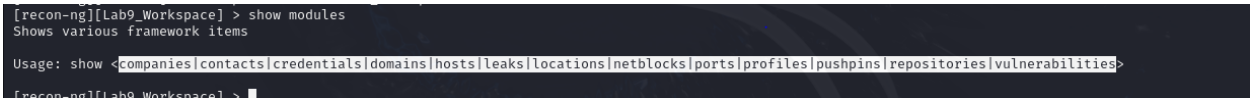
3.Exploring Modules:

List available modules in Recon-ng:

- Show modules
- Focus on reconnaissance modules such as domains, contacts, and social media.

Exercise 1:

- List the modules that can be used for domain reconnaissance. What are some key modules you might consider?
  companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities



Step 2: Using Recon-ng for Information Gathering

1.Adding a Domain:

Add a target domain to your workspace:

- Add domains <target-domain>
- Replace <target-domain> with a live domain, e.g., example.com.

2.Running Modules:

Use the whois module to gather registration information:

- Use recon/domains-hosts/whoisRun
- Explore other modules for gathering information such as social_media, contacts, etc.

Exercise 2:

- Document the registration details obtained from the whois module. What information did you find useful? _____

3.Automating Data Gathering:

Use additional modules for automated data collection, such as:

- Use recon/hosts-hosts/resolve
- Run

Exercise 3:

- What new information was discovered about the target domain? List the subdomains or IP addresses obtained. _____

Step 3: Setting Up Shodan

1.Creating a Shodan Account:

- Go to the Shodan website and create a free account to obtain an API key.
- Copy your API key for later use.

2.Installing Shodan CLI (if not already installed):

- Pip install shodan

3.Configuring Shodan:

- In your terminal, configure Shodan with your API key:
- Shodan init <YOUR_API_KEY>

Exercise 4:

- Verify that your API key is working by running:
- Shodan info

Step 4: Using Shodan for Device Discovery

1.Searching for Devices:

Use Shodan to find devices related to your target domain:

- Shodan search <target-domain>

Example:

Shodan search example.com

Exercise 5:

- What devices were discovered related to the target domain? Provide a brief description of the findings. _____

2.Advanced Searches:

Utilize advanced search filters, such as:

- Port: Find devices on specific ports (e.g., port:22 for SSH).
- Country: Limit searches to specific countries (e.g., country:US).

Exercise 6:

- Perform an advanced search using two different filters. Document the results and discuss what types of devices you found. _____ **Step 5: Analyzing and Reporting Findings**

1.Combining Data:

- Compare the information gathered from Recon-ng and Shodan. Identify overlaps and unique findings.

2.Documenting Your Findings:

Create a report summarizing your findings, including:

- Target domain details.
- Devices discovered via Shodan.
- Insights gained from Recon-ng modules.

Exercise 7:

In your report, outline the methodologies used, tools employed, and key insights. Discuss how this information could be useful in a penetration testing engagement. _____

Conclusion

In this lab, you gained hands-on experience using Recon-ng and Shodan for information gathering. You learned how to collect and analyze data from multiple sources to inform penetration testing and security assessments.