# Final Engagement

## Attack, Defense & Analysis of a Vulnerable Network

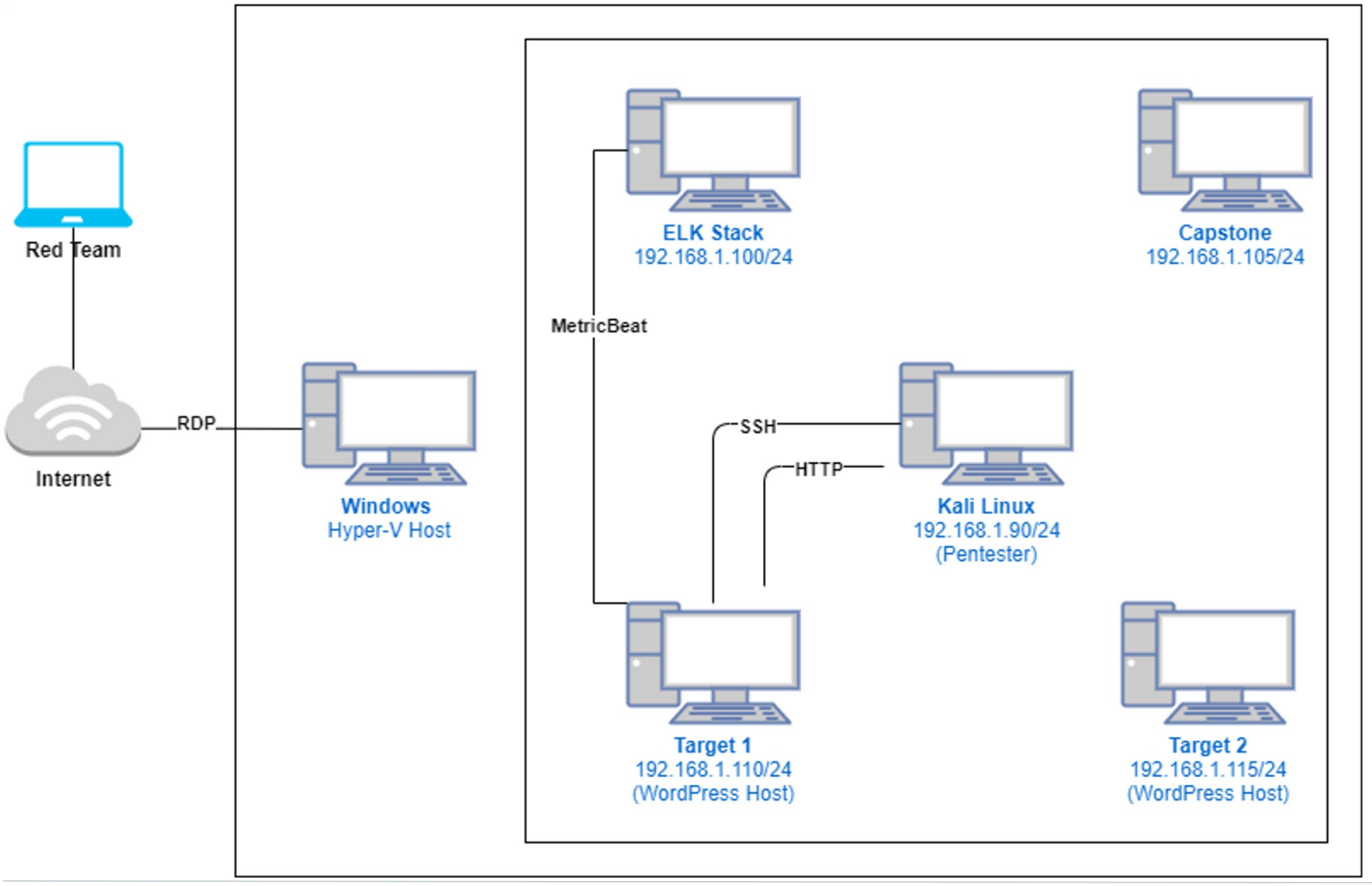
# Table of Contents

This document contains the following resources:


- **Network Topology & Critical Vulnerabilities**
- **Exploits Used**
- **Defensive Alerts & Hardening Techniques**
- **Network Traffic & Analysis**

# Network Topology
# & Critical Vulnerabilities

# Network Topology




**Network**
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

**Machines**
IPv4: 192.168.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Stack

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

# Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

| Vulnerability | Description | Impact |
|---|---|---|
| Wordpress Username Enumeration CVE-2009-2335 | WUE is the process in which attackers remotely enumerate valid usernames for a defined attack surface. | This allows attackers to find valid username information based on failed login attempts. Many Vendors dispute the significance of this issue due to “user convenience” concerns. |
| Brute Force Vulnerability CVE-2020-14494 | A BFV consists of an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. | This allows attackers to run values, such as passwords, through software that will guess predetermined strings until a favorable response returns. |
| Least Privilege Violation CWE-272 | A LPV is the concept that access should be allowed only when it is absolutely necessary to the function of a given system, and only for the minimal necessary amount of time. | Not implementing LPV results in sensitive information to be at risk for attackers to discover once in a system. In this case, read access to the wp-config.php file allowed our team to infiltrate the mySQL database for password hashes of current employees. |
| Privilege Escalation CWE-269 | A misconfigured sudoers file can allow root privilege loopholes given to binary programs. | Allowing root privileges to binary programs can give system users root access to the system without the need for a password. |