Project 3: System Hardening Plan

Group 2

April 29, 2025

Contents

Requested Access Time Slot

- **Date:** Sunday, April 27, 2025
- **Start Time:** 2:00 PM
- **Duration:** 8 hours (Estimated End: 10:00 PM)

1 System Configuration Overview

1.1 Operating Systems Selection

- **Server 1 (Target):** Metasploitable 2 (Instructor Provided Base)
- **Server 2 (Firewall):**
  - OS: IPFire
  - File: `ipfire-2.27.i586-full-core162.iso`
  - Link: [ISO Download Link/Reference Provided Separately]
  - Rationale: Dedicated, lightweight firewall distribution suitable for constrained hardware. Provides Web GUI, IPS capabilities (Suricata/Snort), and robust firewalling.
- **Server 3 (IDS/IPS Host):**
  - OS: Debian Linux (NetInstall)
  - File: `debian-12.10.0-i386-netinst.iso`
  - Link: [ISO Download Link/Reference Provided Separately]
  - Rationale: Minimal, stable base for i386 architecture. Excellent platform for running Suricata IDS and potentially associated analysis tools (e.g., EveBox).

Note: Selected OS versions are compatible with the specified hardware limitations.

User Account Credentials

Server 1 (Metasploitable 2 - Post Hardening)

- **Primary Access (`Group2`):** `Gr0upTw0-/:` (FTP, SSH, Telnet)
- **Admin Backup (`secadmin`):** `SecAdm1n-/:Temp` (Initial - will be replaced by script with a logged random password)

Server 2 (IPFire Firewall)

- **SSH Access (`Group2`):** `Gr0upTw0-/:` (Requires manual creation post-install)
- **Web GUI Admin (`admin`):** `IPF1reAdm-/:G2`
- **Console Root (`root`):** `IPF1reR00t-/:G2`

Server 3 (Debian/Suricata IDS)

- **SSH Admin (`Group2`):** `Gr0upTw0-/:` (To be created with sudo rights)
- **Console Root (`root`):** `Deb1anR00t-/:G2` (Set during installation)

Security Note: Passwords contain special characters. Ensure careful entry. The `secadmin` password on MS2 will be randomized by the hardening script.

2 Network Architecture

2.1 Logical Topology

→ **Nodes:** External Network (Internet) → Router/Modem (NAT/Gateway) → Firewall (IPFire - Server 2) → Internal Switch → {Target (MS2 - Server 1), IDS (Debian - Server 3)}

→ **Connections:**

1. External Router/Modem to Firewall WAN (RED Interface)
2. Firewall LAN (GREEN Interface) to Internal Switch
3. Internal Switch to Target Server (MS2)
4. Internal Switch to IDS Server (Monitoring Interface)

→ **Traffic Flow Assumption:** The Internal Switch must support port mirroring (SPAN) to direct a copy of traffic destined for the Target Server (MS2) to the IDS Server's monitoring interface. The firewall (IPFire) acts as the gateway for the internal network segment.

Port Forwarding Configuration

Total Ports Requested: 9 (Limit: 10) | WAN Port Range: 35000-60000
Assumed Internal IPs (Examples - Confirm with Instructor):

- Target Server (MS2): `192.168.1.100`
- Firewall Server (IPFire GREEN): `192.168.1.101`
- IDS Server (Debian): `192.168.1.102`

Forwarding Rules (External WAN Port → Internal LAN IP:Port):

WAN Port	Internal Destination	Service	Status
`35001`	`192.168.1.100:21`	MS2 FTP	Mandatory
`35002`	`192.168.1.100:22`	MS2 SSH	Mandatory
`35003`	`192.168.1.100:80`	MS2 HTTP	Mandatory
`35004`	`192.168.1.101:222`	IPFire SSH	Mandatory
`35005`	`192.168.1.102:22`	Debian SSH	Mandatory
`35006`	`192.168.1.101:444`	IPFire Web GUI (HTTPS)	Required (Mgmt)
`35007`	`192.168.1.100:23`	MS2 Telnet	Required (Project)
`35008`	`192.168.1.102:5636`	IDS Alert UI (e.g., EveBox)	Optional Service
`35009`	`192.168.1.100:8180`	MS2 Tomcat HTTP	Target Service

Note: IPFire uses port 222 for SSH by default; port 444 is the default HTTPS port for its Web GUI.

3 System Hardening Strategy

3.1 Server 1: Metasploitable 2 Remediation

Primary Method: Execution of a custom Bash script automating the following tasks.

- **Updates:** Apply system updates (`apt-get update/upgrade`).
- **Backdoor Removal:** Verify and remove known vulnerabilities (Ingreslock, VSFTPD backdoor, UnrealIRCd backdoor).
- **Credentials:**
  - Change default DB passwords (PostgreSQL, MySQL).
  - Create `Group2` user with specified credentials.
  - Randomize passwords for `secadmin`, `msfadmin`, `user`, etc., logging the new `secadmin` password.
- **Service Hardening:**
  - SSH: Disable root login, enforce Protocol 2, configure allowed users.
  - Apache: Disable directory listing, potentially minimal `.htaccess` rules.
- **Local Firewall:** Configure `iptables` (Default drop, allow required services, rate-limit SSH).
- **Permissions:** Review and restrict file permissions on critical files.
- **Monitoring/Logging:** Basic script to log logins/listening ports.
- **Banners:** Implement security warning banners for login services.

3.2 Server 2: IPFire Firewall Configuration

Primary Method: Manual configuration via Console and Web GUI.

- **Initial Setup:** Configure RED (WAN) and GREEN (LAN) interfaces, set strong `root/admin` passwords.
- **Firewall Rules:** Implement default DENY on RED interface. Create explicit ALLOW rules only for the forwarded ports specified in Section 3. Potentially restrict outbound traffic from GREEN.
- **IPS Configuration:** Enable and configure IPS (Suricata engine) using appropriate rulesets (e.g., ET Open). Tune based on alerts.
- **Secure Access:** Ensure Web GUI uses HTTPS. Create `Group2` user for SSH access (port 222) and configure SSH daemon securely.
- **Updates:** Keep system updated via Pakfire package manager.

3.3 Server 3: Debian IDS Host Setup

Primary Method: Manual configuration via Console/SSH.

- **Base OS:** Minimal netinstall, apply all updates.
- **OS Hardening:**
  - Firewall: Configure `ufw` or `iptables` (Default deny, allow SSH, necessary outbound).
- SSH: Secure `sshd`$_{c}onfig, create$`Group2`$userwithsudorights, disablerootlogin.$
- **Suricata Installation & Configuration:**
  - Install Suricata package.
  - Configure `suricata.yaml`: Define `HOME`$_{N}ET, setsniffinginterface, configurelogging($`eve.json`$).Man$
    Use`suricata-update`$tofetchandenablerelevantrules(e.g., ETOpen).$
  - Enable Suricata service to start on boot.
- **(Optional) Alert Interface:** Install and configure web UI (e.g., EveBox) accessible via forwarded port `35008`.

Deliverables Compliance Checklist

☒ Comprehensive Written Plan Submitted

☒ OS Selection Defined (IPFire, Debian i386) with Version Info

☒ OS Download References Included/Provided

☒ OS Selections Meet Hardware Constraints

☒ User Account Credentials Defined per Server (Meets Intent)

☒ Network Topology Clearly Described (Nodes & Connections)

☒ Port Forwarding List Provided (9/10 Ports)

☒ Port Forwarding Format & Range Correct

☒ Mandatory Ports Included in Forwarding Rules

☒ System Hardening Strategy Outlined per Server

☒ Requested Time Slot Specified