SEC+
Lesson 9:
Evaluate Network Security Capabilities

Lesson 9

Topic 9A

Network Security Baselines

Benchmarks and Secure Configuration Guides

- Secure baseline
  - Collection of standard configurations and settings for operating systems, network devices, software, cloud instances, patching and updates, access controls, logging, monitoring, password policies, encryption, endpoint protection, and many others
- Center for Internet Security (CIS)
- Security Technical Implementation Guides (STIGs)
- Vendor provided guidance

Benchmarks and Secure Configuration Guides

- Configuration management
- Help manage, deploy, and measure compliance with established secure baselines
  - Puppet
  - Chef
  - Ansible
- Security Content Automation Protocol (SCAP)
  - OpenSCAP
  - CIS-CAT Pro
  - SCAP Compliance Checker (SCC)

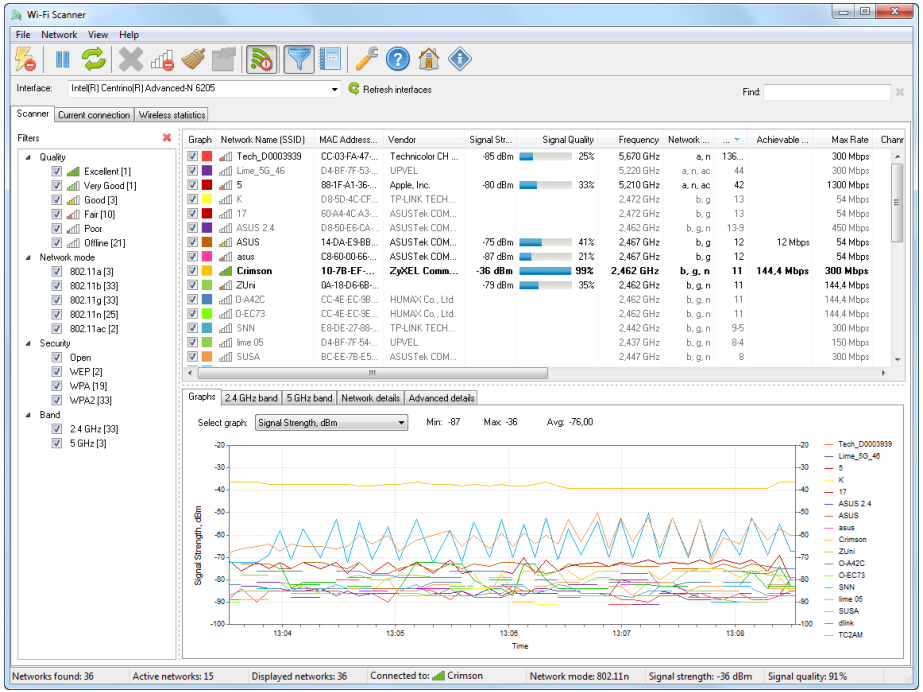
Switches and Routers

- Examples of changes designed to improve security:
- Change Default Credentials
- Disable Unnecessary
- Use Secure Management Protocols
- Implement Access Control Lists (ACLs)
- Enable Logging and Monitoring
- Configure Port Security
- Strong Password
- Physically Secure Equipment

Server Hardware and Operating Systems

- Examples of changes designed to improve security:
  - Change Default Credentials
  - Disable Unnecessary Services
  - Apply Software Security Patches and Updates Regularly
  - Least Privilege Principle
  - Use Firewalls and Intrusion Detection Systems (IDS)
  - Secure Configuration using CIS or STIG baselines
  - Strong Access Controls
  - Enable Logging and Monitoring
  - Use Antivirus and Antimalware Solutions
  - Physical Security of server equipment racks, server rooms, and datacenters

Wireless Network Installation Considerations

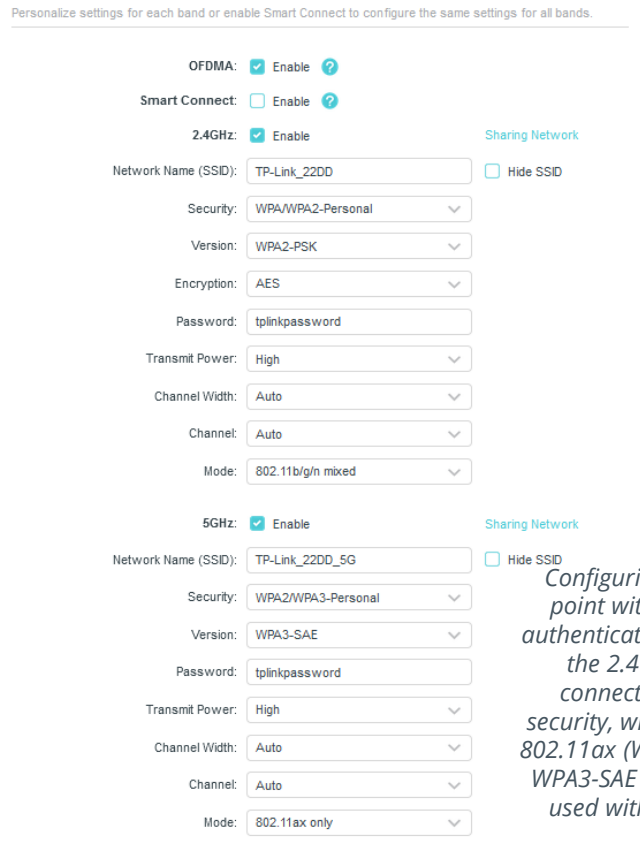


Example output from Lizard System's Wi-Fi Scanner tool. (Screenshot courtesy of Lizard Systems.)

- Wireless Access Point (WAP) Placement
- Site Surveys and Heat Maps

Wireless Encryption

- Open
- WEP
- WPS
- WPA & WPA2
- WPA3
  - Device Provisioning Protocol (DPP) a.k.a. “Easy Connect” to replace WPS
  - Simultaneous Authentication of Equals (SAE)
  - Enhanced Open

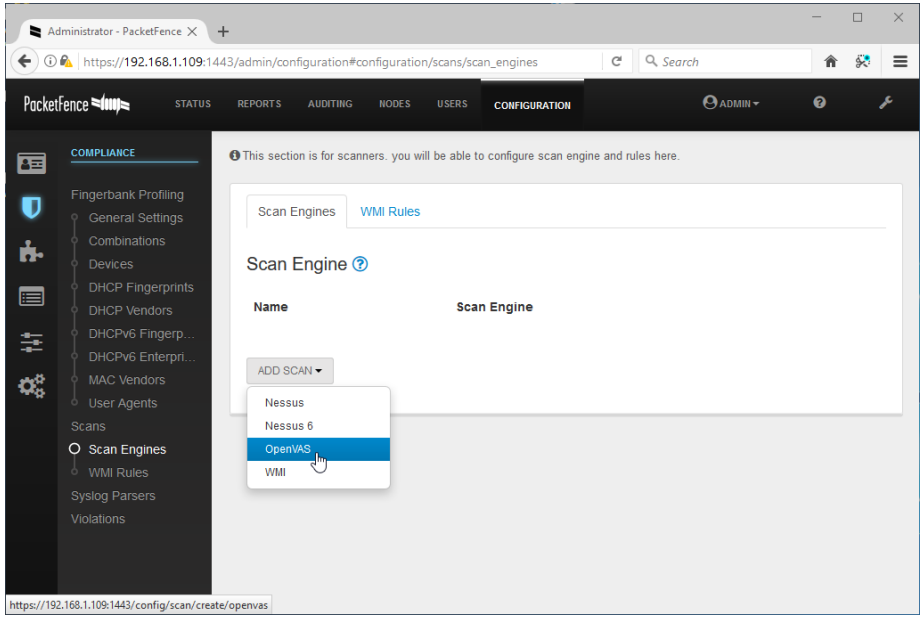


Configuring a TP-LINK SOHO access point with wireless encryption and authentication settings. In this example, the 2.4 GHz band allows legacy connections with WPA2-Personal security, while the 5 GHz network is for 802.11ax (Wi-Fi 6) capable devices using WPA3-SAE authentication. (Screenshot used with permission from TP-Link Technologies.)

Wi-Fi Authentication Methods

- WPA2 Pre-Shared Key Authentication
- WPA3 Personal Authentication
- WPA2/WPA3-Enterprise
  - RADIUS
  - EAP

Network Access Control



PacketFence supports the use of several scanning techniques, including vulnerability scanners, such as Nessus and OpenVAS, Windows Management Instrumentation (WMI) queries, and log parsers. (Screenshot used with permission from packetfence.org.)

- Authenticates users/devices before allowing them access to the network
- Agent versus agentless

Network Security Baselines

- Benchmarks and Secure Configuration Guides
- Wireless Network Installation Considerations
- Wireless Encryption
- Wi-Fi Authentication Methods
- Network Access Control

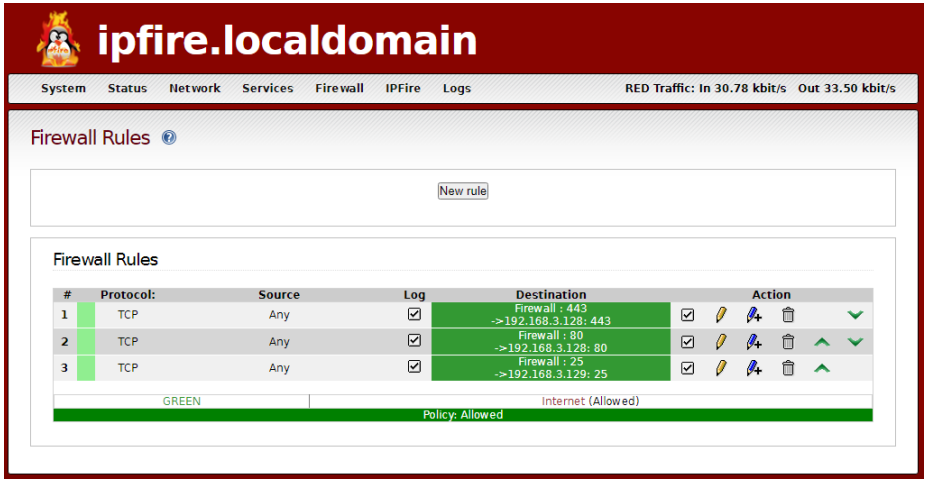
Lesson 9

Topic 9B

Network Security Capability Enhancement

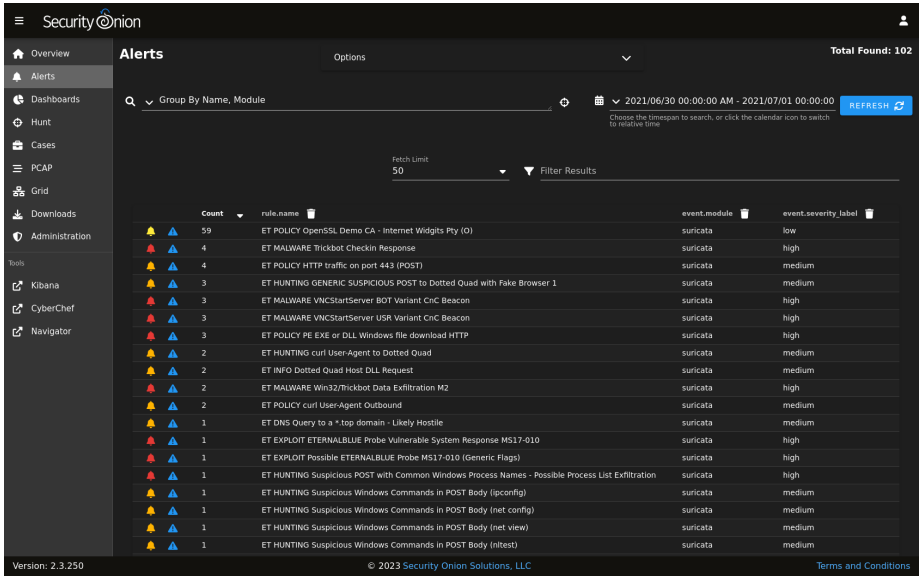
Access Control Lists

- ACL
  - List of permissions associated with a network device, such as a router or a switch, that controls traffic at a network interface level
- Firewall Rule
  - Dictates how inbound or outbound network traffic for specific IP addresses, IP ranges, or network interfaces
- Screened Subnet
  - A neutral zone, separating public-facing servers from sensitive internal network resources



Sample firewall rules configured on IPFire. This ruleset allows any HTTP, HTTPS, or SMTP traffic to specific internal addresses. (Screenshot used with permission from IPFire)

Intrusion Detection and Prevention Systems

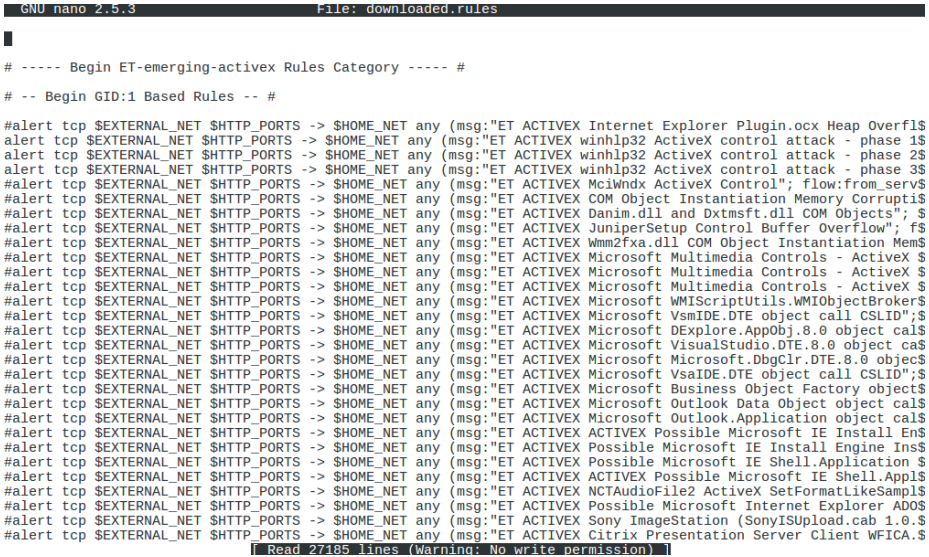


The Security Onion Alerts dashboard displaying several alerts captured using the Emerging Threats (ET) ruleset and Suricata. (Screenshot used with permission from Security Onion.)

- Host-based
- Network-based
- Both look for suspicious patterns or activities that could indicate a network or system intrusion
- They differ in their responses to perceived threats
- Snort
- Suricata
- OSSEC

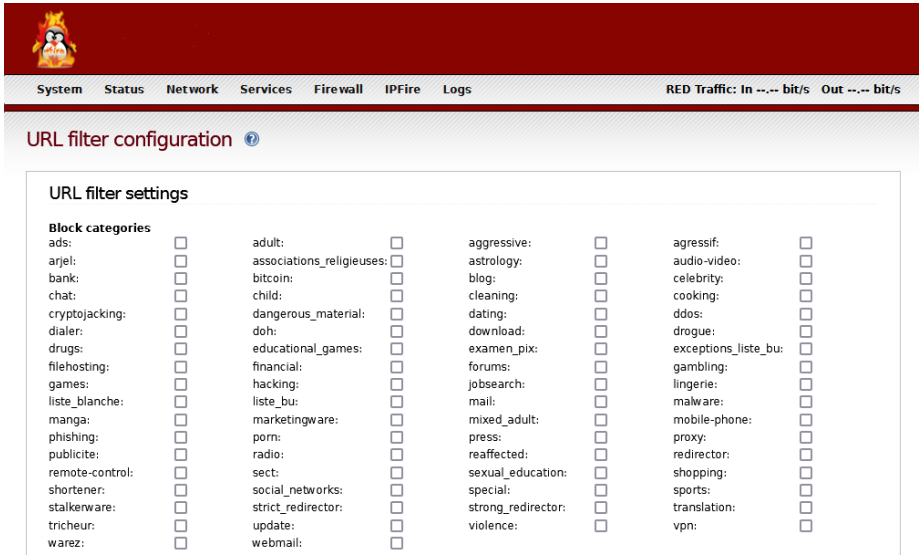
IDS and IPS Detection Methods

- Signature-Based Detection
- Anomaly-based detection
- Trend Analysis
- Behavioral-based detection
  - Network Behavior and Anomaly Detection (NBAD)
  - User and Entity Behavior Analytics (UEBA)



Snort rules file supplied by the open-source Emerging Threats community feed.

Web Filtering



Web filter content categories using the IPFire open-source firewall. (Screenshot used with permission from IPFire.)

- Block users from accessing malicious or inappropriate websites
- Enforce compliance with acceptable use
- Block malware
- Protection from phishing attacks
- Agent-Based Filtering
- Centralized Web Filtering
- URL Scanning
- Content Categorization
- Block Rules
- Reputation-Based Filtering
- Decrypting and inspecting HTTPS traffic

Network Security Capability Enhancement

- Access Control Lists
- Intrusion Detection and Prevention Systems
- IDS and IPS Detection Methods
- Web Filtering

Lesson 9

Summary