



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

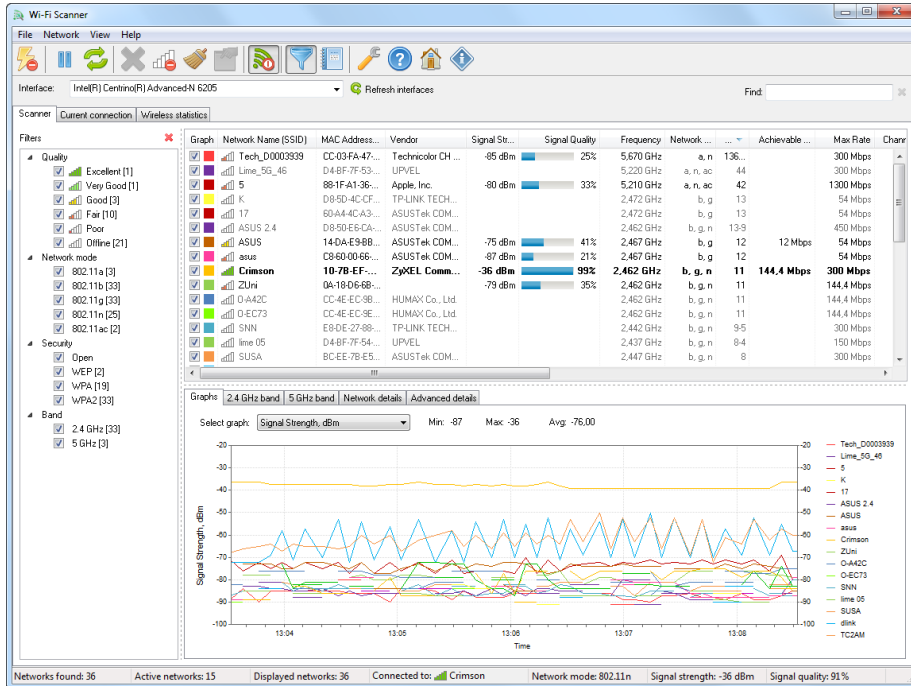
- Examples of changes designed to improve security:
- Change Default Credentials
- Disable Unnecessary
- Use Secure Management Protocols
- Implement Access Control Lists (ACLs)
- Enable Logging and Monitoring
- Configure Port Security
- Strong Password
- Physically Secure Equipment

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

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



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

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

Personalize settings for each band or enable Smart Connect to configure the same settings for all bands.

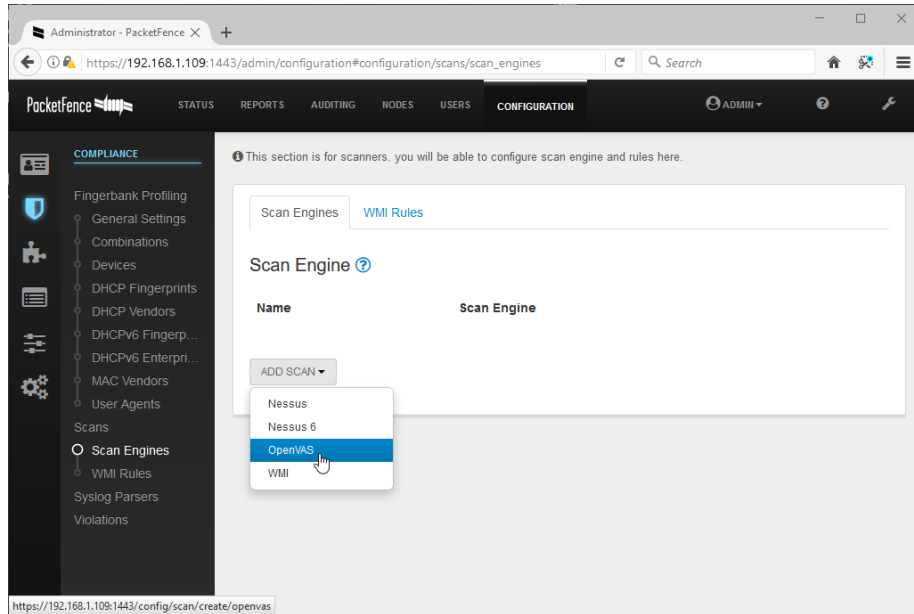
The screenshot shows the wireless settings for a TP-Link SOHO access point. It is divided into two sections: 2.4GHz and 5GHz. At the top, there are checkboxes for OFDMA (checked), Smart Connect (unchecked), and a 'Sharing Network' checkbox (unchecked). The 2.4GHz section has '2.4GHz' checked and 'Sharing Network' checked. The 5GHz section has '5GHz' checked and 'Sharing Network' checked. Both sections have a 'Hide SSID' checkbox (unchecked). The 2.4GHz settings are: Network Name (SSID): TP-Link_22DD, Security: WPA/WPA2-Personal, Version: WPA2-PSK, Encryption: AES, Password: tlinkpassword, Transmit Power: High, Channel Width: Auto, Channel: Auto, Mode: 802.11b/g/n mixed. The 5GHz settings are: Network Name (SSID): TP-Link_22DD_5G, Security: WPA2/WPA3-Personal, Version: WPA3-SAE, Password: tlinkpassword, Transmit Power: High, Channel Width: Auto, Channel: Auto, Mode: 802.11ax only.

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



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

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.)

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

The screenshot displays the IPFire web interface for 'ipfire.localdomain'. The top navigation bar includes 'System', 'Status', 'Network', 'Services', 'Firewall', 'IPFire', and 'Logs'. The 'Firewall' section is active, showing 'RED Traffic: In 30.78 kbit/s Out 33.50 kbit/s'. Below the navigation, there is a 'Firewall Rules' section with a 'New rule' button. A table lists three firewall rules:

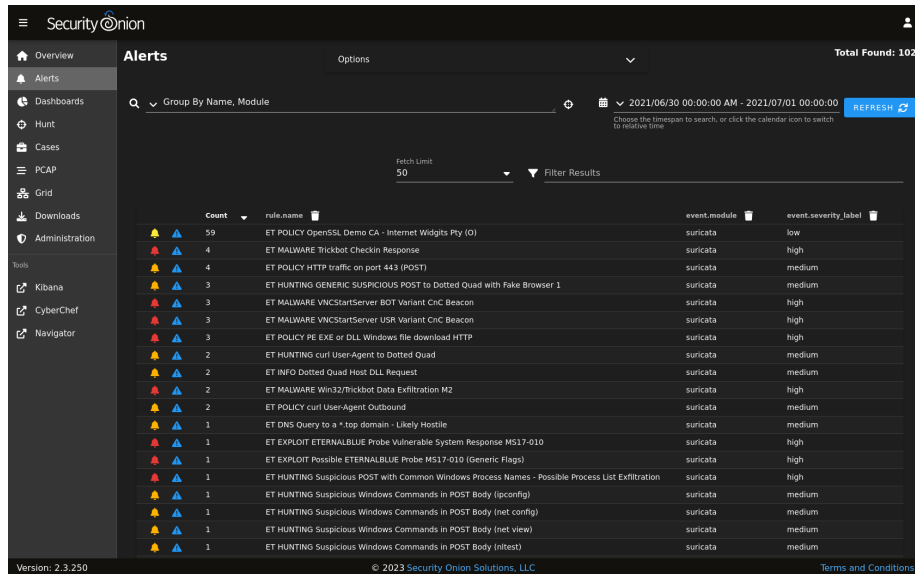
| # | Protocol | Source | Log | Destination | Action |
|---|----------|--------|-------------------------------------|--|-------------------------------------|
| 1 | TCP | Any | <input checked="" type="checkbox"/> | Firewall : 443 ->192.168.3.128: 443 | <input checked="" type="checkbox"/> |
| 2 | TCP | Any | <input checked="" type="checkbox"/> | Firewall : 80 ->192.168.3.128: 80 | <input checked="" type="checkbox"/> |
| 3 | TCP | Any | <input checked="" type="checkbox"/> | Firewall : 25 ->192.168.3.129: 25 | <input checked="" type="checkbox"/> |

At the bottom, a green bar indicates the status: 'GREEN' and 'Policy: Allowed Internet (Allowed)'.

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

- 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



The screenshot shows the Security Onion Alerts dashboard. The interface includes a sidebar with navigation options like Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, and Administration. The main area displays a table of alerts with columns for Count, rule_name, event_module, and event_severity_label. The table shows 102 total alerts found, with a fetch limit of 50. The alerts are sorted by rule name and include various Emerging Threats (ET) and Suricata rules.

| Count | rule_name | event_module | event_severity_label |
|-------|---|--------------|----------------------|
| 59 | ET POLICY OpenSSL Demo CA - Internet Widgits Pty (o) | suricata | low |
| 4 | ET MALWARE Trickbot Checkin Response | suricata | high |
| 4 | ET POLICY HTTP traffic on port 443 (POST) | suricata | medium |
| 3 | ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 | suricata | medium |
| 3 | ET MALWARE VNCStartServer BOT Variant CnC Beacon | suricata | high |
| 3 | ET MALWARE VNCStartServer USR Variant CnC Beacon | suricata | high |
| 3 | ET POLICY PE EXE or DLL Windows file download HTTP | suricata | high |
| 2 | ET HUNTING curl User-Agent to Dotted Quad | suricata | medium |
| 2 | ET INFO Dotted Quad Host DLL Request | suricata | medium |
| 2 | ET MALWARE Win32/Trickbot Data Exfiltration M2 | suricata | high |
| 2 | ET POLICY curl User-Agent Outbound | suricata | medium |
| 1 | ET DNS Query to a *top domain - Likely Hostile | suricata | medium |
| 1 | ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010 | suricata | high |
| 1 | ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags) | suricata | high |
| 1 | ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration | suricata | high |
| 1 | ET HUNTING Suspicious Windows Commands in POST Body (ipconfig) | suricata | medium |
| 1 | ET HUNTING Suspicious Windows Commands in POST Body (net config) | suricata | medium |
| 1 | ET HUNTING Suspicious Windows Commands in POST Body (net view) | suricata | medium |
| 1 | ET HUNTING Suspicious Windows Commands in POST Body (nbtstat) | suricata | medium |

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

IDS and IPS Detection Methods

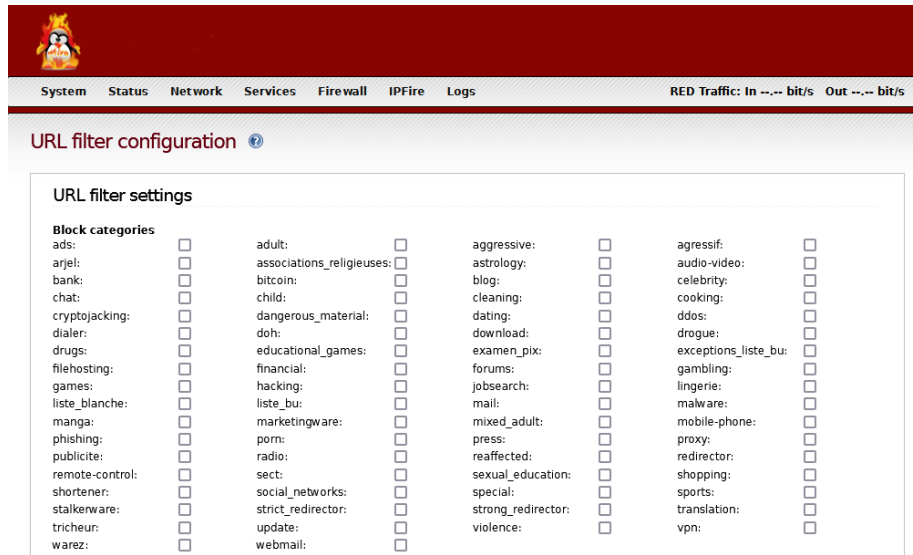
- Signature-Based Detection
- Anomaly-based detection
- Trend Analysis
- Behavioral-based detection
 - Network Behavior and Anomaly Detection (NBAD)
 - User and Entity Behavior Analytics (UEBA)

```
GNU nano 2.5.3 File: downloaded.rules
# ----- Begin ET-emerging-activex Rules Category ----- #
# -- Begin GID:1 Based Rules -- #
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Internet Explorer Plugin.ocx Heap Overflr
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 1$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 2$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 3$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX MciWndx ActiveX Control"; flow:from_serv$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object Instantiation Memory Corrupti$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Danim.dll and Dxtmsft.dll COM Objects"; $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX JuniperSetup Control Buffer Overflow"; f$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Wmm2fxa.dll COM Object Instantiation Mem$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft WMIScriptUtils.WMIObjectBroker$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsmIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft DExplore.AppObj.8.0 object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VisualStudio.DTE.8.0 object ca$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Microsoft.DbgClr.DTE.8.0 objec$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsaIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Business Object Factory object$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook Data Object object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook.Application object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Install En$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Install Engine Inss$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Shell.Application $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Shell.Apple$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX NCTAudioFile2 ActiveX SetFormatLikeSampl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft Internet Explorer ADOS$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Sony ImageStation (SonyISUpload.cab 1.0.$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Citrix Presentation Server Client WFICA.$
Read 27185 lines (warning: No write permission)
```

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

Web Filtering

- 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



The screenshot shows the IPFire web filter configuration interface. At the top, there is a navigation menu with tabs for System, Status, Network, Services, Firewall, IPFire, and Logs. The IPFire tab is active, and the page title is "URL filter configuration". Below the title, there is a "URL filter settings" section with a "Block categories" heading. This section contains a grid of 40 categories, each with a checkbox. The categories are arranged in four columns and ten rows. The categories are: ads, arjel, bank, chat, cryptojacking, dialer, drugs, filehosting, games, liste_blanche, manga, phishing, publicite, remote-control, shortener, stalkerware, tricheur, warez, adult, associations_religieuses, bitcoin, child, dangerous_material, educational_games, financial, hacking, liste_bu, marketingware, porn, radio, sect, social_networks, strict_redirector, update, webmail, aggressive, astrology, blog, cleaning, dating, download, examen_pix, forums, jobsearch, mail, mixed_adult, press, reaffected, sexual_education, special, strong_redirector, violence, agressif, audio-video, celebrity, cooking, ddos, drogue, exceptions_liste_bu, gambling, lingerie, malware, mobile-phone, proxy, redirector, shopping, sports, translation, and vpn.

| Block categories | | | | | | | |
|------------------|--------------------------|---------------------------|--------------------------|--------------------|--------------------------|----------------------|--------------------------|
| ads: | <input type="checkbox"/> | adult: | <input type="checkbox"/> | aggressive: | <input type="checkbox"/> | agressif: | <input type="checkbox"/> |
| arjel: | <input type="checkbox"/> | associations_religieuses: | <input type="checkbox"/> | astrology: | <input type="checkbox"/> | audio-video: | <input type="checkbox"/> |
| bank: | <input type="checkbox"/> | bitcoin: | <input type="checkbox"/> | blog: | <input type="checkbox"/> | celebrity: | <input type="checkbox"/> |
| chat: | <input type="checkbox"/> | child: | <input type="checkbox"/> | cleaning: | <input type="checkbox"/> | cooking: | <input type="checkbox"/> |
| cryptojacking: | <input type="checkbox"/> | dangerous_material: | <input type="checkbox"/> | dating: | <input type="checkbox"/> | ddos: | <input type="checkbox"/> |
| dialer: | <input type="checkbox"/> | educational_games: | <input type="checkbox"/> | download: | <input type="checkbox"/> | drogue: | <input type="checkbox"/> |
| drugs: | <input type="checkbox"/> | financial: | <input type="checkbox"/> | examen_pix: | <input type="checkbox"/> | exceptions_liste_bu: | <input type="checkbox"/> |
| filehosting: | <input type="checkbox"/> | hacking: | <input type="checkbox"/> | forums: | <input type="checkbox"/> | gambling: | <input type="checkbox"/> |
| games: | <input type="checkbox"/> | liste_bu: | <input type="checkbox"/> | jobsearch: | <input type="checkbox"/> | lingerie: | <input type="checkbox"/> |
| liste_blanche: | <input type="checkbox"/> | marketingware: | <input type="checkbox"/> | mail: | <input type="checkbox"/> | malware: | <input type="checkbox"/> |
| manga: | <input type="checkbox"/> | porn: | <input type="checkbox"/> | mixed_adult: | <input type="checkbox"/> | mobile-phone: | <input type="checkbox"/> |
| phishing: | <input type="checkbox"/> | radio: | <input type="checkbox"/> | press: | <input type="checkbox"/> | proxy: | <input type="checkbox"/> |
| publicite: | <input type="checkbox"/> | sect: | <input type="checkbox"/> | reaffected: | <input type="checkbox"/> | redirector: | <input type="checkbox"/> |
| remote-control: | <input type="checkbox"/> | social_networks: | <input type="checkbox"/> | sexual_education: | <input type="checkbox"/> | shopping: | <input type="checkbox"/> |
| shortener: | <input type="checkbox"/> | strict_redirector: | <input type="checkbox"/> | special: | <input type="checkbox"/> | sports: | <input type="checkbox"/> |
| stalkerware: | <input type="checkbox"/> | update: | <input type="checkbox"/> | strong_redirector: | <input type="checkbox"/> | translation: | <input type="checkbox"/> |
| tricheur: | <input type="checkbox"/> | webmail: | <input type="checkbox"/> | violence: | <input type="checkbox"/> | vpn: | <input type="checkbox"/> |
| warez: | <input type="checkbox"/> | | | | | | |

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

Network Security Capability Enhancement

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

CompTIA Security+ Exam SY0-701

Lesson 9



Summary