CompTIA Security+ Exam SY0-701

Lesson 9

Evaluate Network Security Capabilities

Lesson 9

Topic 9A

Network Security Baselines

Benchmarks and Secure Configuration Guides (1 of 2)

- 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 (2 of 2)

- 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)

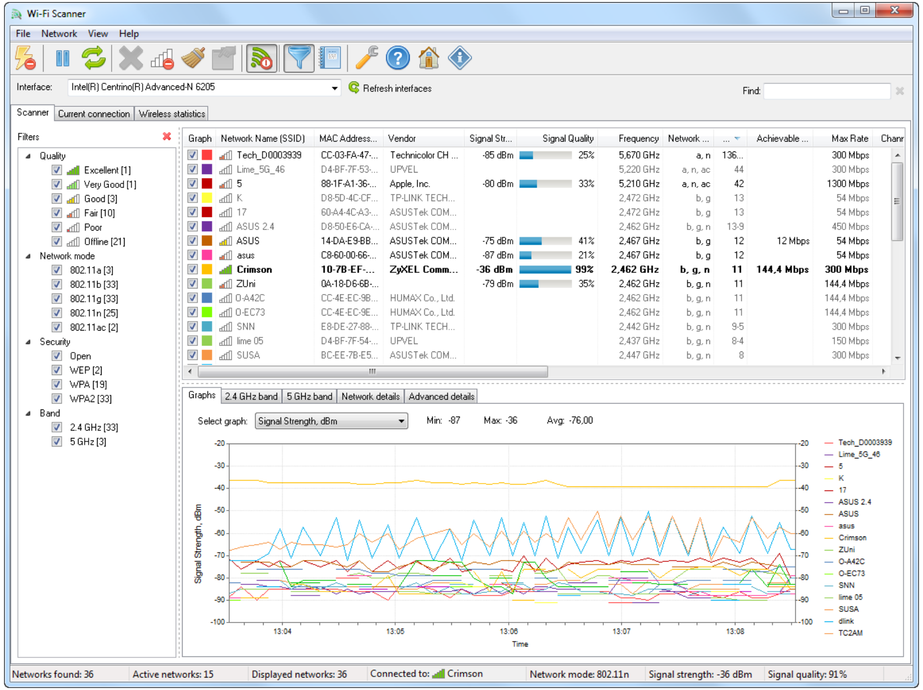
Switches and Routers

- 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



Interface: Intel(R) Centrino(R) Advanced-N 6205 Refresh interfaces Find:

- Quality
  - ☑ Excellent [1]
  - ☑ Very Good [1]
  - ☑ Good [3]
  - ☑ Fair [10]
  - ☑ Poor
  - ☑ Offline [21]
- Network mode
  - ☑ 802.11a [3]
  - ☑ 802.11b [33]
  - ☑ 802.11g [33]
  - ☑ 802.11n [25]
  - ☑ 802.11ac [2]
- Security
  - ☑ Open
  - ☑ WEP [2]
  - ☑ WPA [19]
  - ☑ WPA2 [33]
- Band
  - ☑ 2.4 GHz [33]
  - ☑ 5 GHz [3]

Graph	Network Name (SSID)	MAC Address...	Vendor	Signal Str...	Signal Quality	Frequency	Network ...	...	Achievable ...	Max Rate	Chanr
☑	Tech_D0003939	CC-03-FA-47-...	Technicolor CH ...	-85 dBm	25%	5,670 GHz	a, n	136...		300 Mbps	
☑	Lime_5G_46	D4-BF-7F-53-...	UPVEL			5,220 GHz	a, n, ac	44		300 Mbps	
☑	5	88-1F-A1-36-...	Apple, Inc.	-80 dBm	33%	5,210 GHz	a, n, ac	42		1300 Mbps	
☑	K	D8-5D-4C-CF...	TP-LINK TECH...			2,472 GHz	b, g	13		54 Mbps	
☑	17	60-A4-4C-A3-...	ASUSTek COM...			2,472 GHz	b, g	13		54 Mbps	
☑	ASUS 2.4	D8-50-E6-CA-...	ASUSTek COM...			2,462 GHz	b, g, n	13-9		450 Mbps	
☑	ASUS	14-DA-E9-BB...	ASUSTek COM...	-75 dBm	41%	2,467 GHz	b, g	12	12 Mbps	54 Mbps	
☑	asus	C8-60-00-66-...	ASUSTek COM...	-87 dBm	21%	2,467 GHz	b, g	12		54 Mbps	
☑	**Crimson**	**10-7B-EF-...**	**ZyXEL Comm...**	**-36 dBm**	**99%**	**2,462 GHz**	**b, g, n**	**11**	**144,4 Mbps**	**300 Mbps**	
☑	ZUni	0A-18-D6-6B-...		-79 dBm	35%	2,462 GHz	b, g, n	11		144,4 Mbps	
☑	O-A42C	CC-4E-EC-9B...	HUMAX Co., Ltd.			2,462 GHz	b, g, n	11		144,4 Mbps	
☑	O-EC73	CC-4E-EC-9E...	HUMAX Co., Ltd.			2,462 GHz	b, g, n	11		144,4 Mbps	
☑	SNN	E8-DE-27-88-...	TP-LINK TECH...			2,442 GHz	b, g, n	9-5		300 Mbps	
☑	lime 05	D4-BF-7F-54-...	UPVEL			2,437 GHz	b, g, n	8-4		150 Mbps	
☑	SUSA	BC-EE-7B-E5...	ASUSTek COM...			2,447 GHz	b, g, n	8		300 Mbps	

Select graph: Signal Strength, dBm Min: -87 Max: -36 Avg: -76,00

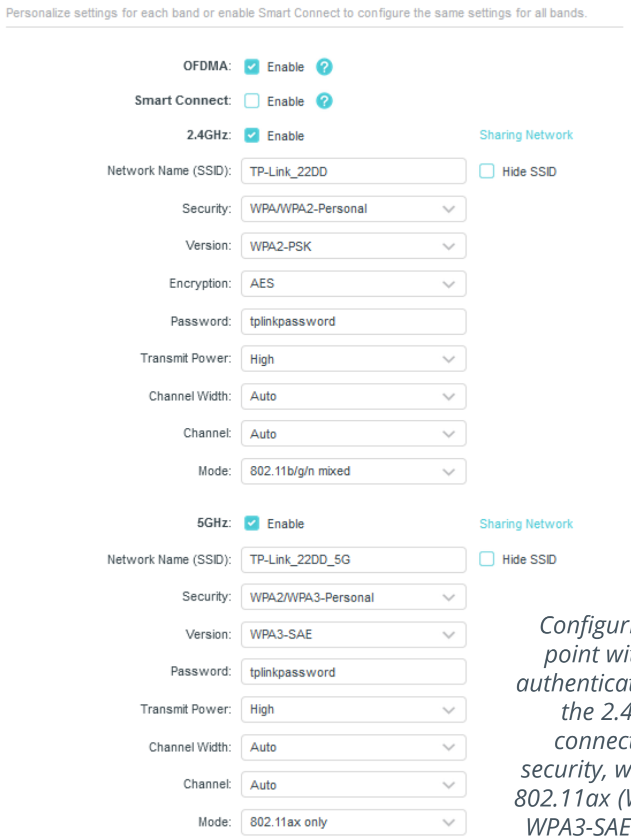
Networks found: 36 | Active networks: 15 | Displayed networks: 36 | Connected to: Crimson | Network mode: 802.11n | Signal strength: -36 dBm | Signal quality: 91%

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



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

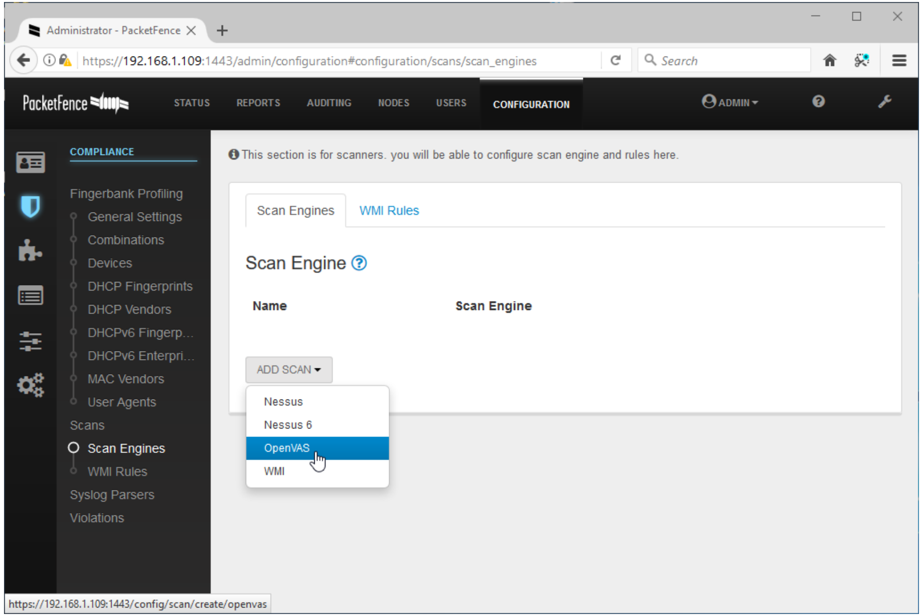
OFDMA:	☑ Enable	
Smart Connect:	□ Enable	
2.4GHz:	☑ Enable	Sharing Network
Network Name (SSID):	TP-Link_22DD	□ Hide SSID
Security:	WPA/WPA2-Personal	
Version:	WPA2-PSK	
Encryption:	AES	
Password:	tplinkpassword	
Transmit Power:	High	
Channel Width:	Auto	
Channel:	Auto	
Mode:	802.11b/g/n mixed	
5GHz:	☑ Enable	Sharing Network
Network Name (SSID):	TP-Link_22DD_5G	□ Hide SSID
Security:	WPA2/WPA3-Personal	
Version:	WPA3-SAE	
Password:	tplinkpassword	
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



This section is for scanners. you will be able to configure scan engine and rules here.

Scan Engine

Name	Scan Engine

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

Review Activity: Network Security Baselines

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

Lab Activity

- Assisted Lab: Understanding Security Baselines

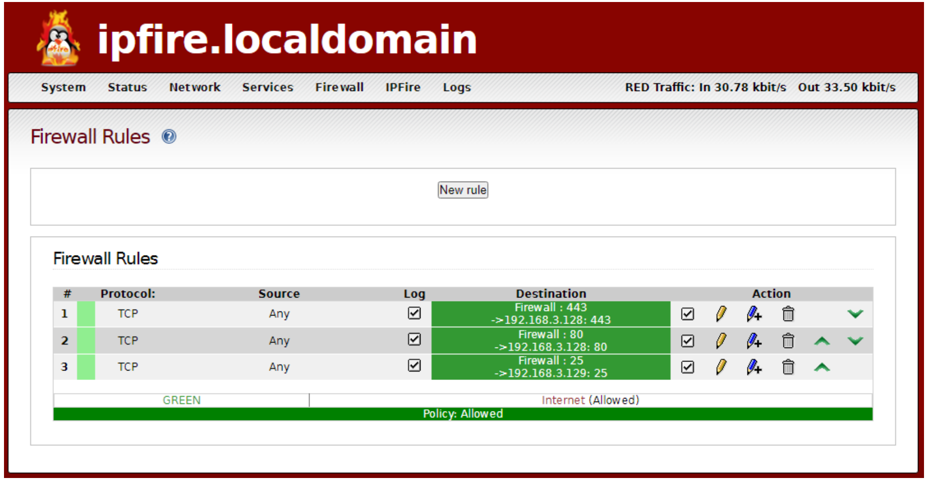
Lesson 9

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



RED Traffic: In 30.78 kbit/s Out 33.50 kbit/s

Firewall Rules

Firewall Rules

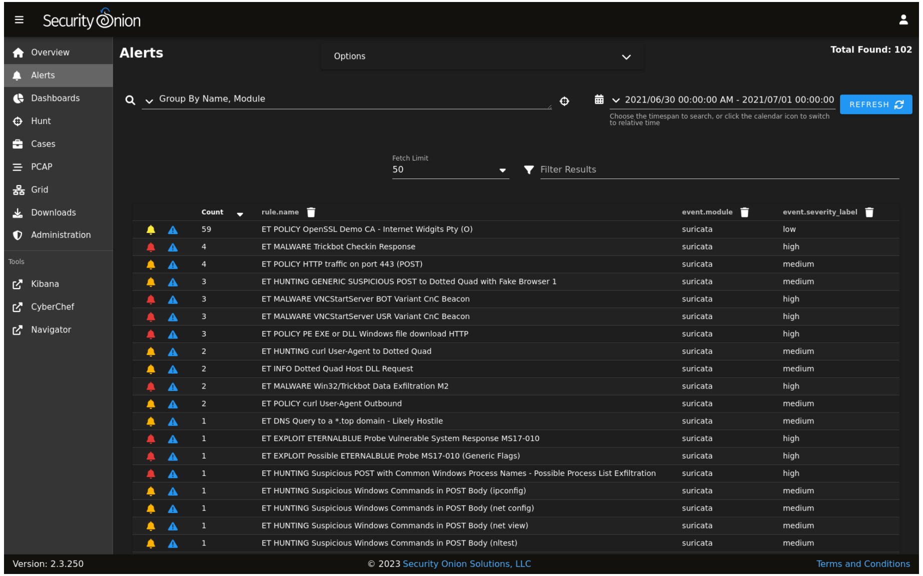
#		Protocol:	Source	Log	Destination	Action
1	🟩	TCP	Any	☑	Firewall : 443 ->192.168.3.128: 443	☑
2	🟩	TCP	Any	☑	Firewall : 80 ->192.168.3.128: 80	☑
3	🟩	TCP	Any	☑	Firewall : 25 ->192.168.3.129: 25	☑

GREEN | Internet (Allowed)

Policy: 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



Alerts

Total Found: 102

Group By Name, Module

2021/06/30 00:00:00 AM - 2021/07/01 00:00:00

Choose the timespan to search, or click the calendar icon to switch to relative time

Fetch Limit: 50

Filter Results

		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 (nltest)	suricata	medium

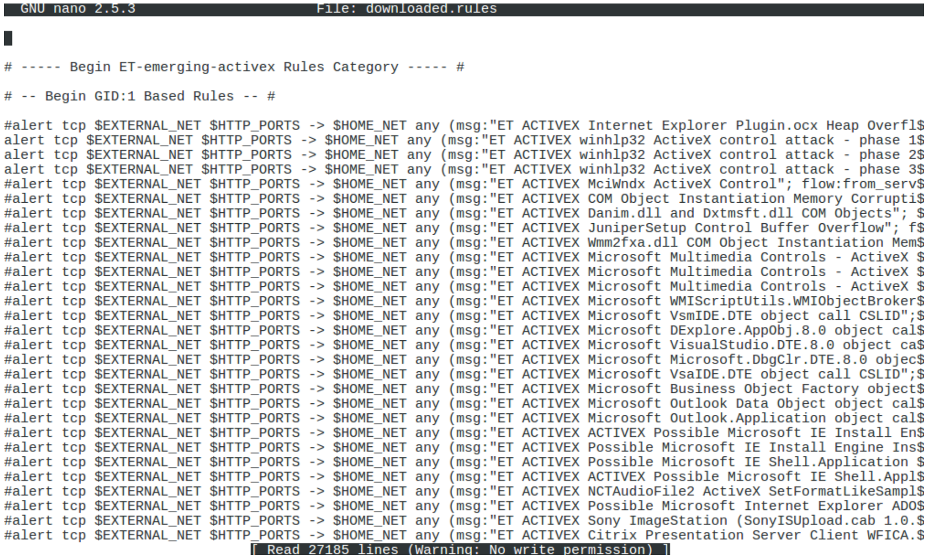
Version: 2.3.250 © 2023 Security Onion Solutions, LLC Terms and Conditions

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

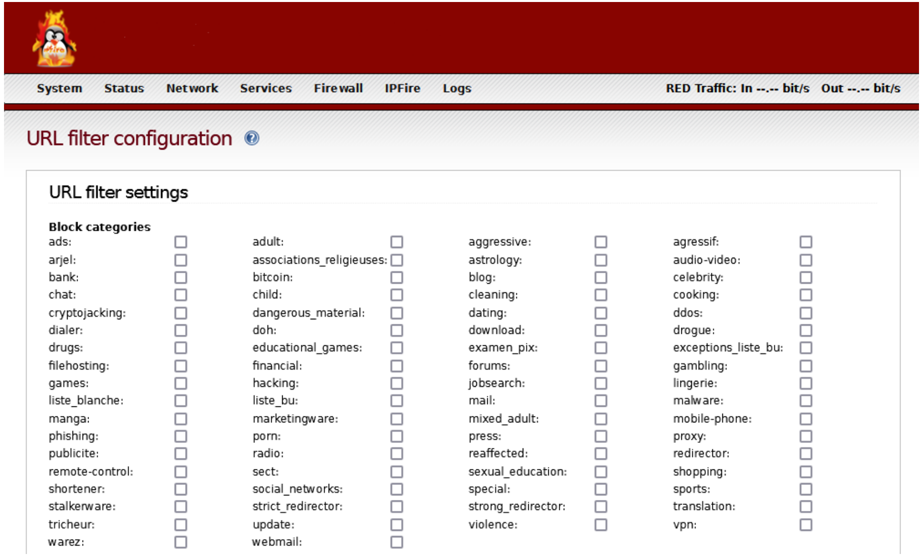
- Signature-Based Detection
- Anomaly-based detection
- Trend Analysis
- Behavioral-based detection
  - Network Behavior and Anomaly Detection (NBAD)
  - User and Entity Behavior Analytics (UEBA)



```
  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 -> $HOME_NET any (msg:"ET ACTIVEX Internet Explorer Plugin.ocx Heap Overfl$
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 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 -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Install Engine Ins$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Shell.Application $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Shell.Appl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX NCTAudioFile2 ActiveX SetFormatLikeSampl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft Internet Explorer ADO$
#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) ]
```

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

Web Filtering



URL filter configuration

URL filter settings

Block categories

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

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

Review Activity: Network Security Capability Enhancement

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

Lab Activity

- Applied Lab: Implementing a Firewall

CompTIA Security+ Exam SY0-701

Lesson 9

Summary