Initial defense:

Implement Suricata on pfsense ✅

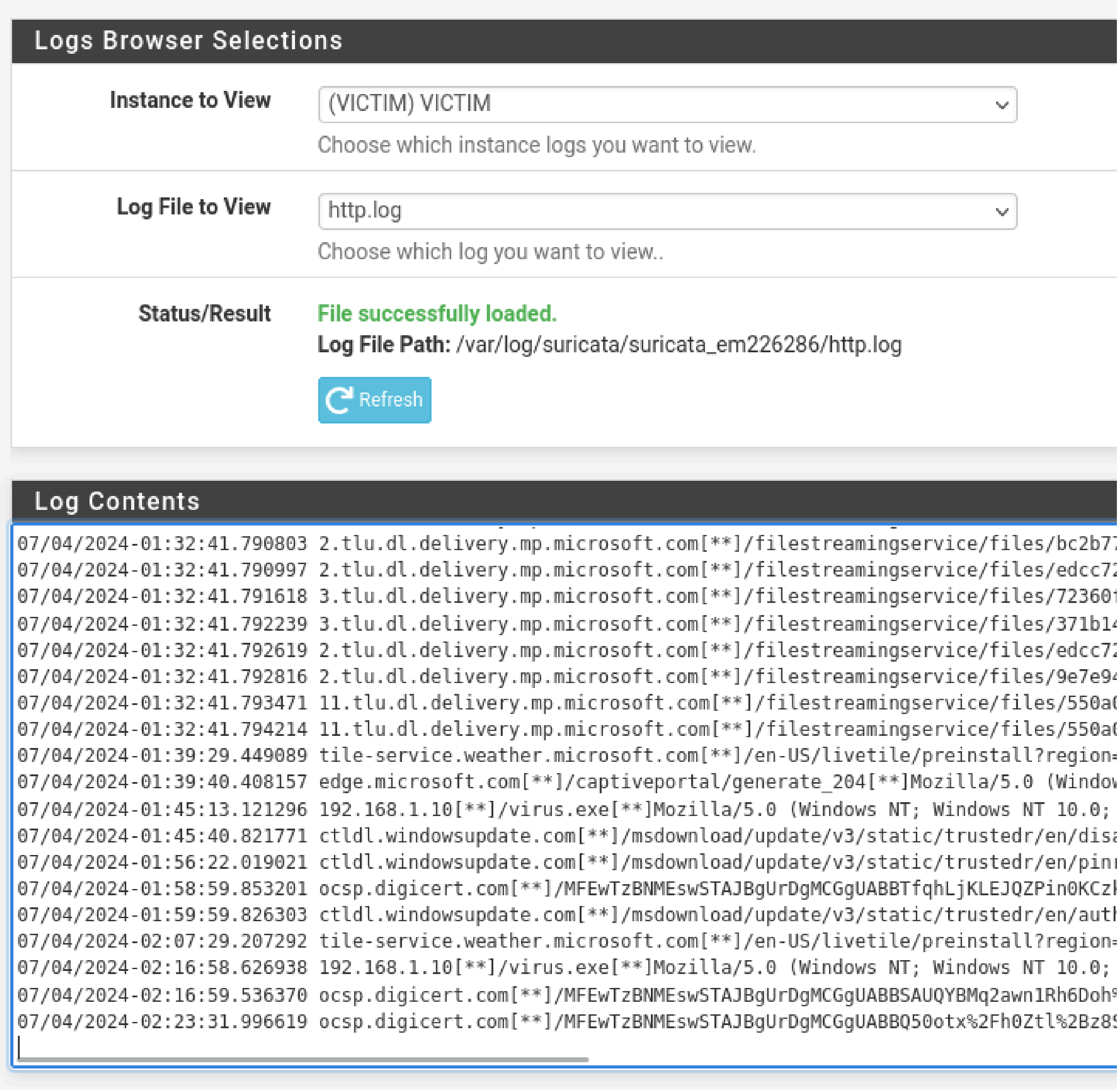
Emerging Threats Open (ET Open) rulesets

Implement security onion minimal ✅

1.

Initial defense for reverse shell payload

1. **Introduce Suricata on pfsense router software to serve as NIDS/IPS system**



Logs Browser Selections

Instance to View: (VICTIM) VICTIM

Choose which instance logs you want to view.

Log File to View: http.log

Choose which log you want to view..

Status/Result: File successfully loaded.

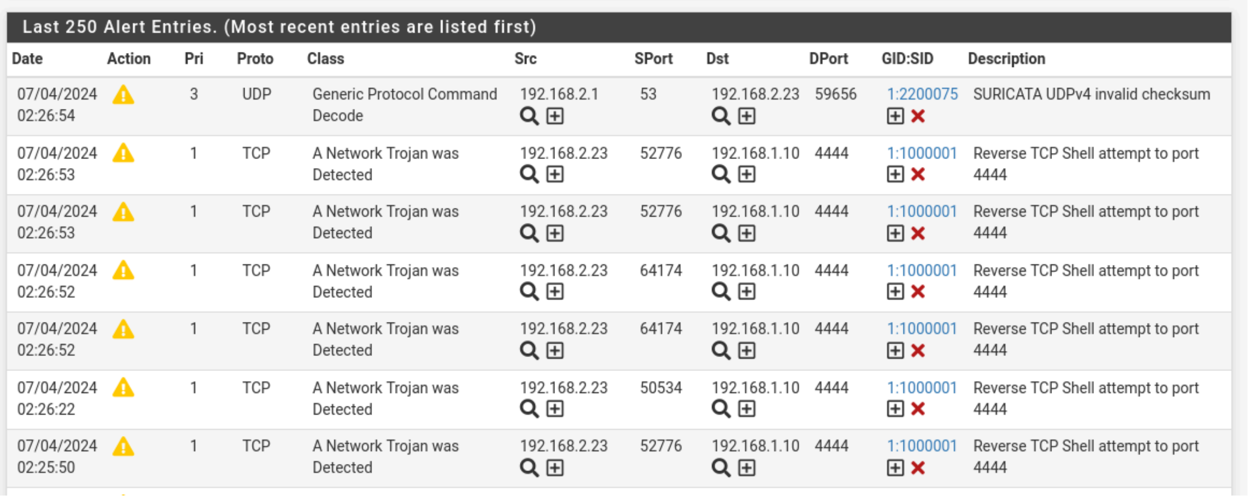
Log File Path: /var/log/suricata/suricata_em226286/http.log

Log Contents

```
07/04/2024-01:32:41.790803 2.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/bc2b7
07/04/2024-01:32:41.790997 2.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/edcc7
07/04/2024-01:32:41.791618 3.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/72360
07/04/2024-01:32:41.792239 3.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/371b1
07/04/2024-01:32:41.792619 2.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/edcc7
07/04/2024-01:32:41.792816 2.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/9e7e9
07/04/2024-01:32:41.793471 11.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/550a
07/04/2024-01:32:41.794214 11.tlu.dl.delivery.mp.microsoft.com[**]/filestreamingservice/files/550a
07/04/2024-01:39:29.449089 tile-service.weather.microsoft.com[**]/en-US/livetile/preinstall?region
07/04/2024-01:39:40.408157 edge.microsoft.com[**]/captiveportal/generate_204[**]Mozilla/5.0 (Windo
07/04/2024-01:45:13.121296 192.168.1.10[**]/virus.exe[**]Mozilla/5.0 (Windows NT; Windows NT 10.0;
07/04/2024-01:45:40.821771 ctldl.windowsupdate.com[**]/msdownload/update/v3/static/trustedr/en/dis
07/04/2024-01:56:22.019021 ctldl.windowsupdate.com[**]/msdownload/update/v3/static/trustedr/en/pin
07/04/2024-01:58:59.853201 ocsp.digicert.com[**]/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCz
07/04/2024-01:59:59.826303 ctldl.windowsupdate.com[**]/msdownload/update/v3/static/trustedr/en/aut
07/04/2024-02:07:29.207292 tile-service.weather.microsoft.com[**]/en-US/livetile/preinstall?region
07/04/2024-02:16:58.626938 192.168.1.10[**]/virus.exe[**]Mozilla/5.0 (Windows NT; Windows NT 10.0;
07/04/2024-02:16:59.536370 ocsp.digicert.com[**]/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh
07/04/2024-02:23:31.996619 ocsp.digicert.com[**]/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8
```

2. Create alert for tracking attack machine's IP 192.168.1.xx

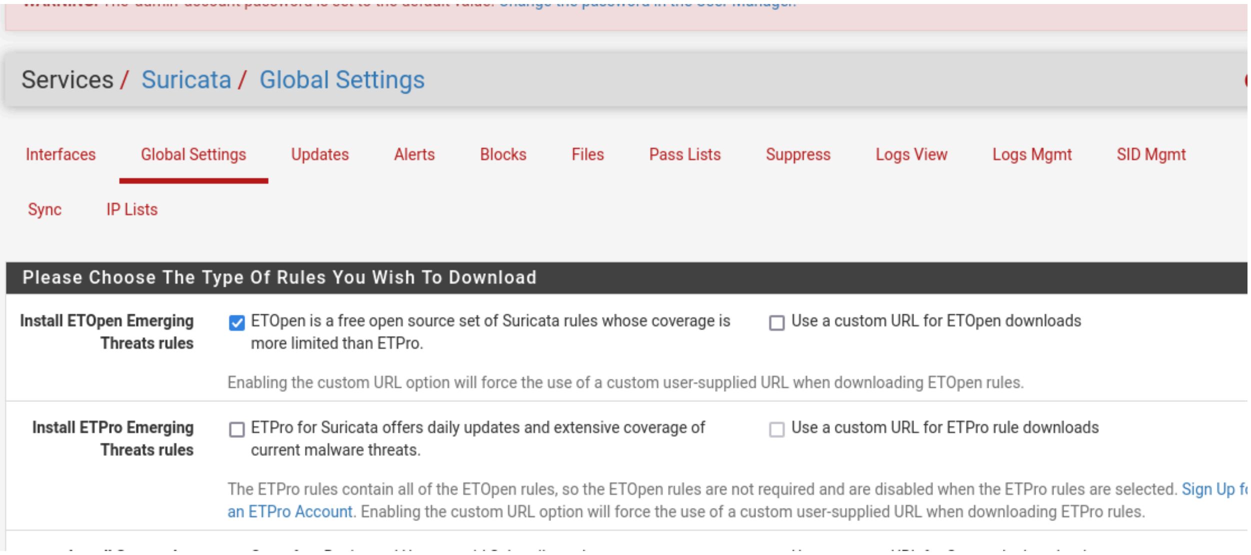
Ex. "alert tcp 192.168.2.23 any -> 192.168.1.10 4444 (msg:"Reverse TCP Shell attempt to port 4444"; sid:1000001; rev:2; classtype:trojan-activity; flow:established,to_server;)"



Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/04/2024 02:26:54	⚠	3	UDP	Generic Protocol Command Decode	192.168.2.1	53	192.168.2.23	59656	1:2200075	SURICATA UDPv4 invalid checksum
07/04/2024 02:26:53	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	52776	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444
07/04/2024 02:26:53	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	52776	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444
07/04/2024 02:26:52	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	64174	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444
07/04/2024 02:26:52	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	64174	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444
07/04/2024 02:26:22	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	50534	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444
07/04/2024 02:25:50	⚠	1	TCP	A Network Trojan was Detected	192.168.2.23	52776	192.168.1.10	4444	1:1000001	Reverse TCP Shell attempt to port 4444

3. **Introduce ETOpen Emerging Threats rule which is free open source set of Suricata rules to give coverage on potential malicious traffic**



WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Services / Suricata / Global Settings

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules ☑ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro. □ Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Install ETPro Emerging Threats rules □ ETPro for Suricata offers daily updates and extensive coverage of current malware threats. □ Use a custom URL for ETPro rule downloads

The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. Sign Up fo an ETPro Account. Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.