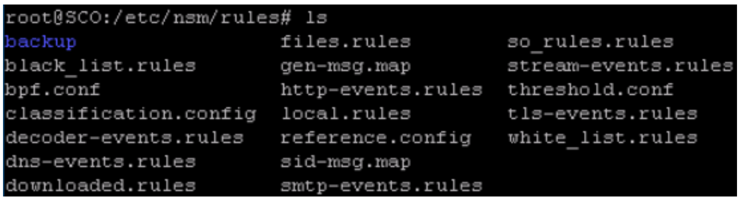
CEN4088.01 Lab 10 Due xx/xx/19

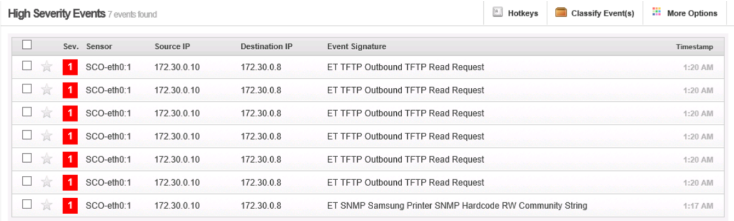
Brandon Thompson 5517

December 4, 2019



```
root@SCO:/etc/nsm/rules# ls
backup                  files.rules        so_rules.rules
black_list.rules        gen-msg.map        stream-events.rules
bpf.conf                http-events.rules  threshold.conf
classification.config   local.rules        tls-events.rules
decoder-events.rules    reference.config   white_list.rules
dns-events.rules        sid-msg.map
downloaded.rules        smtp-events.rules
```

Figure 1: Contents of `/etc/nsm/rules/+ folder.`

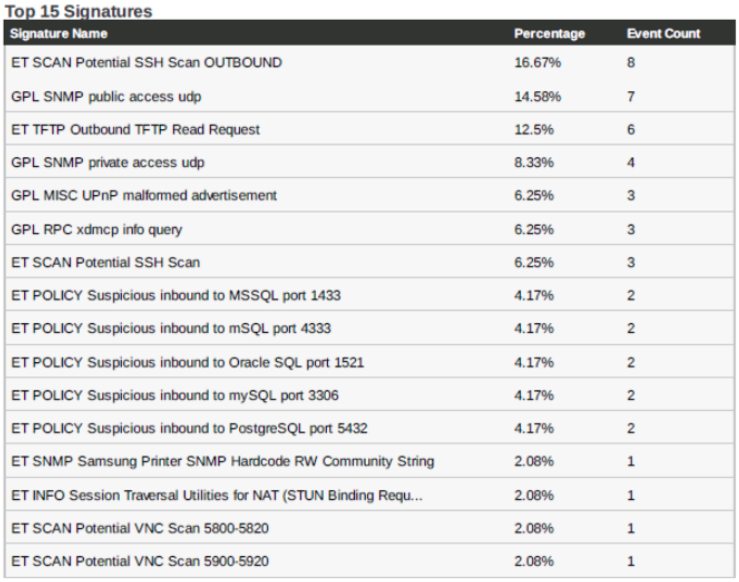


High Severity Events 7 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET TFTP Outbound TFTP Read Request	1:20 AM
□	☆	1	SCO-eth0:1	172.30.0.10	172.30.0.8	ET SNMP Samsung Printer SNMP Hardcode RW Community String	1:17 AM

Figure 2: Snorby list of high security vulnerabilities.

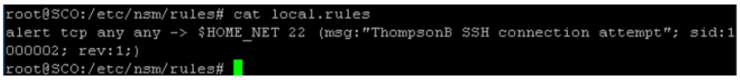
- OS-Windows Microsoft Windows UPnP malformed advertisement: Buffer overflow in Universal Plug and Play (UPnP) on Windows 98,98SE, ME, and XP allows remote attackers to execute arbitrary code via a notify directive with a long location URL.
- GPL SNMP public access udp: Snort saw an SNMP packet which was accessing the "public" SNMP community.
- ET POLICY Suspicious inbound to PostgreSQL port 5432: Snort detected suspicious activity associated with PostgreSQL port 5432.



Top 15 Signatures

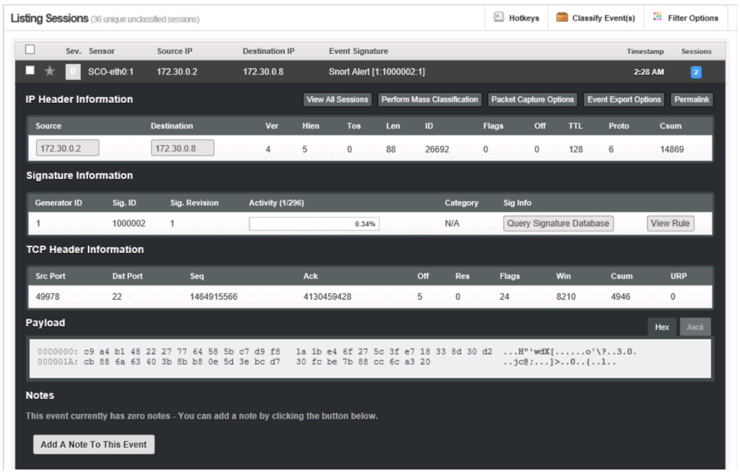
Signature Name	Percentage	Event Count
ET SCAN Potential SSH Scan OUTBOUND	16.67%	8
GPL SNMP public access udp	14.58%	7
ET TFTP Outbound TFTP Read Request	12.5%	6
GPL SNMP private access udp	8.33%	4
GPL MISC UPnP malformed advertisement	6.25%	3
GPL RPC xdmcp info query	6.25%	3
ET SCAN Potential SSH Scan	6.25%	3
ET POLICY Suspicious inbound to MSSQL port 1433	4.17%	2
ET POLICY Suspicious inbound to mSQL port 4333	4.17%	2
ET POLICY Suspicious inbound to Oracle SQL port 1521	4.17%	2
ET POLICY Suspicious inbound to mySQL port 3306	4.17%	2
ET POLICY Suspicious inbound to PostgreSQL port 5432	4.17%	2
ET SNMP Samsung Printer SNMP Hardcode RW Community String	2.08%	1
ET INFO Session Traversal Utilities for NAT (STUN Binding Requ...	2.08%	1
ET SCAN Potential VNC Scan 5800-5820	2.08%	1
ET SCAN Potential VNC Scan 5900-5920	2.08%	1

Figure 3: Snorby top 15 signatures.



```
root@SCO:/etc/nsm/rules# cat local.rules
alert tcp any any -> $HOME_NET 22 (msg:"ThompsonB SSH connection attempt"; sid:1
000002; rev:1;)
root@SCO:/etc/nsm/rules# 
```

Figure 4: Contents of `/etc/nsm/rules/local.rules+ file.`



Listing Sessions (36 unique unclassified sessions)

□	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
□ ★	0	SCO-eth0:1	172.30.0.2	172.30.0.8	Snort Alert [1:1000002:1]	2:28 AM	2

IP Header Information

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.30.0.2	172.30.0.8	4	5	0	88	26692	0	0	128	6	14869

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (1/296)	Category	Sig Info	
1	1000002	1	0.34%	N/A	Query Signature Database	View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
49978	22	1464915566	4130459428	5	0	24	8210	4946	0

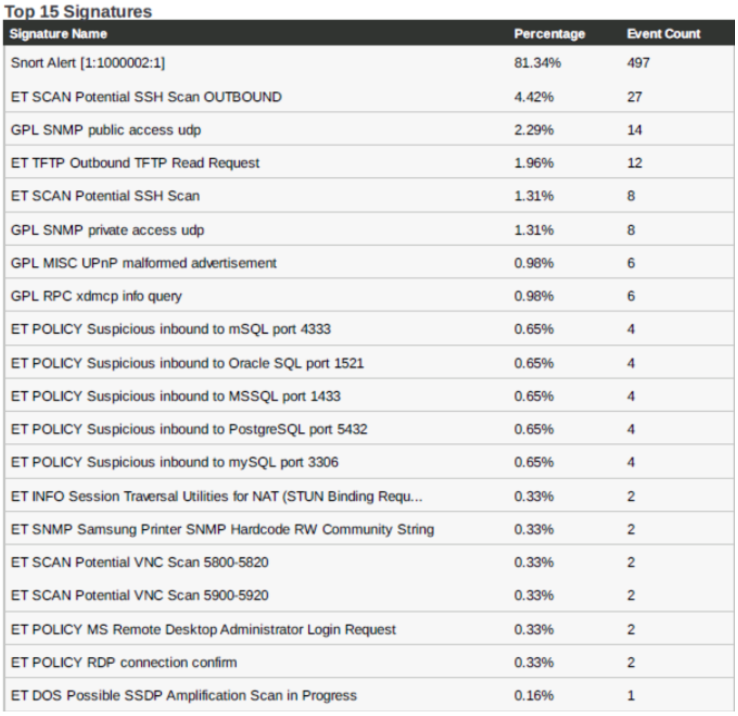
Payload

```
0000000: c9 a4 b1 48 22 27 77 64 58 5b c7 d9 f8   1a 1b e4 6f 27 5c 3f e7 18 33 8d 30 d2   ...H"'wdX[......o'\?..3.0.
000001A: cb 88 6a 63 40 3b 8b b8 0e 5d 3e bc d7   30 fc be 7b 88 cc 6c a3 20               ..jc@;...]>..0..{..l..
```

Notes

This event currently has zero notes - You can add a note by clicking the button below.

Figure 5: Information for custom Snort alert.



Top 15 Signatures

Signature Name	Percentage	Event Count
Snort Alert [1:1000002:1]	81.34%	497
ET SCAN Potential SSH Scan OUTBOUND	4.42%	27
GPL SNMP public access udp	2.29%	14
ET TFTP Outbound TFTP Read Request	1.96%	12
ET SCAN Potential SSH Scan	1.31%	8
GPL SNMP private access udp	1.31%	8
GPL MISC UPnP malformed advertisement	0.98%	6
GPL RPC xdmcp info query	0.98%	6
ET POLICY Suspicious inbound to mSQL port 4333	0.65%	4
ET POLICY Suspicious inbound to Oracle SQL port 1521	0.65%	4
ET POLICY Suspicious inbound to MSSQL port 1433	0.65%	4
ET POLICY Suspicious inbound to PostgreSQL port 5432	0.65%	4
ET POLICY Suspicious inbound to mySQL port 3306	0.65%	4
ET INFO Session Traversal Utilities for NAT (STUN Binding Requ...	0.33%	2
ET SNMP Samsung Printer SNMP Hardcode RW Community String	0.33%	2
ET SCAN Potential VNC Scan 5800-5820	0.33%	2
ET SCAN Potential VNC Scan 5900-5920	0.33%	2
ET POLICY MS Remote Desktop Administrator Login Request	0.33%	2
ET POLICY RDP connection confirm	0.33%	2
ET DOS Possible SSDP Amplification Scan in Progress	0.16%	1

Figure 6: Snorby top 15 signatures.