ICT2203 Project Report

Done by: Gu Boyuan[#1], Lim Wei Le[#2], Ng Ee Zen[#3] & Lee Ray Zan, Zane[#4]
2103210@sit.singaporetech.edu.sg[#1];2103205@sit.singaporetech.edu.sg[#2];2103204@sit.singaporetech.edu.sg[#3];
2103208@sit.singaporetech.edu.sg[#4];

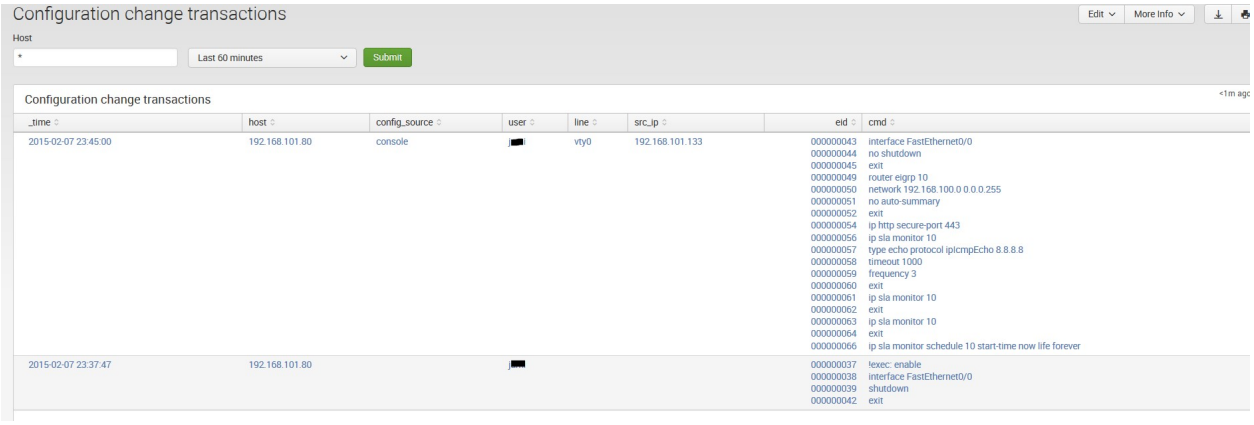
Additional Security Features

In addition to the network security concepts taught in this module, our team has also implemented additional security features such as a Security Information and Event Management (SIEM) system on our AAA server and an Application-Layer (L7) firewall on our DNS and web server.

Splunk (SIEM)

Splunk is used for monitoring and searching through big data. It indexes and correlates information in a container that makes it searchable, and makes it possible to generate alerts, reports and visualisations.

Splunk allows our monitoring team to remotely and concurrently view live log updates from all of our network devices, split into unique indexes per device for the convenience of log searching. This allows for quick incident response in the event of an attack, and ease of investigation with all our network logs consolidated in a simple-to-use yet extensive GUI application.



Configuration change transactions

Edit | More Info

Host: *

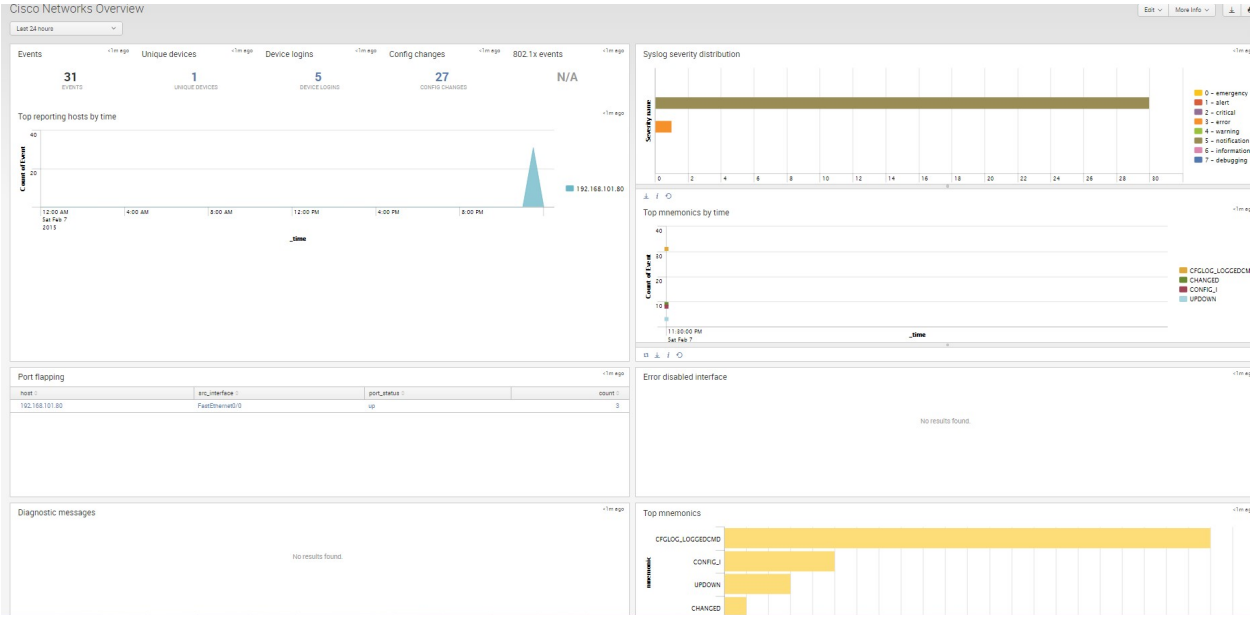
Last 60 minutes | Submit

Configuration change transactions

<1m ago

_time	host	config_source	user	line	src_ip	eid	cmd
2015-02-07 23:45:00	192.168.101.80	console	[redacted]	vty0	192.168.101.133	000000043	interface FastEthernet0/0
						000000044	no shutdown
						000000045	exit
						000000049	router eigrp 10
						000000050	network 192.168.100.0 0.0.0.255
						000000051	no auto-summary
						000000052	exit
						000000054	ip http secure-port 443
						000000056	ip sla monitor 10
						000000057	type echo protocol ipicmpEcho 8.8.8.8
						000000058	timeout 1000
						000000059	frequency 3
						000000060	exit
						000000061	ip sla monitor 10
						000000062	exit
						000000063	ip sla monitor 10
						000000064	exit
						000000066	ip sla monitor schedule 10 start-time now life forever
2015-02-07 23:37:47	192.168.101.80		[redacted]			000000037	!exec: enable
						000000038	interface FastEthernet0/0
						000000039	shutdown
						000000042	exit

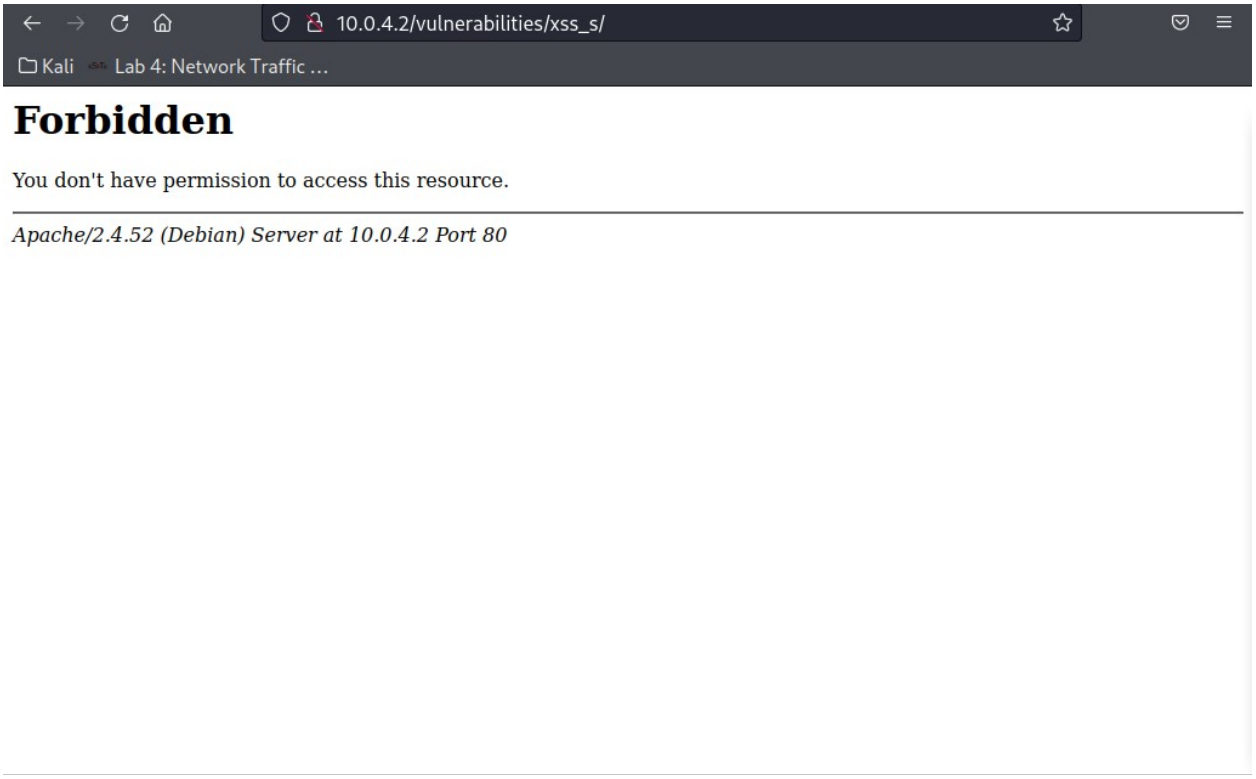
Besides syslog logging on our network devices, Splunk also gets live updates directly from TACACS.net. This allows for real-time logging of authentication attempts and auditing as it is being recorded on our AAA server. We are able to create lookup tables and custom dashboards to easily find the information we need when conducting an investigation, or just doing periodic network monitoring.


Cisco Networks Overview
Edit
More Info
Last 24 hours
Events
31
EVENTS
Unique devices
1
UNIQUE DEVICES
Device logins
5
DEVICE LOGINS
Config changes
27
CONFIG CHANGES
802.1x events
N/A
Top reporting hosts by time
Count of Event
192.168.101.80
_time
Syslog severity distribution
Severity name
0 - emergency
1 - alert
2 - critical
3 - error
4 - warning
5 - notification
6 - information
7 - debugging
Top mnemonics by time
Count of Event
CFGLOG_LOGGEDCM
CHANGED
CONFIG_I
UPDOWN
_time
Port flapping
host
src_interface
port_status
count
192.168.101.80
FastEthernet0/0
up
3
Error disabled interface
No results found.
Diagnostic messages
No results found.
Top mnemonics
mnemonic
CFGLOG_LOGGEDCMD
CONFIG_I
UPDOWN
CHANGED

Apache Modsecurity & IPTables (L7 Firewall)

A Layer 7 (L7) firewall is a type of firewall that operates on the OSI model's 7th layer. The seventh layer of the OSI model, often known as the application layer, allows for more advanced traffic-filtering rules.

The Apache Modsecurity module is a collection of HTTP firewall rules on Apache that can be used to block many common attacks such as XSS, SQL injection and much more. It utilises community rules which are frequently updated online to prevent the latest attacks against websites. This is an essential secondary layer of defence should our ASA firewall rules fail to block new zero-day attacks against our vulnerable DVWA server. Modsecurity will deny any potential attacks on our website by returning a 403 error code.



IPTables is a Linux application-layer firewall used to filter connections to the OS itself. Here, we added a simple rule to drop further packets when a single IP creates too many concurrent connections to our webserver on port 80. This is useful as a secondary defence against Denial of Service (DOS) attacks and it will work well even against hard-to-detect slow DOS attacks like slowloris should

attackers find a way to bypass our Cisco ASA firewall. We used a combination of IPTables and UFW to achieve DOS mitigation.

```
# Custom rule to limit concurrent HTTP connections
-A ufw-before-input -p tcp --syn --dport 80 -m connlimit --connlimit-above 10 -j DROP
-A ufw-before-input -p tcp --syn --dport 443 -m connlimit --connlimit-above 10 -j DROP
```

```
┌──(kali㉿ns1)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Bind9                      ALLOW       Anywhere
5222/tcp                   ALLOW       Anywhere
5223/tcp                   ALLOW       Anywhere
5269/tcp                   ALLOW       Anywhere
5280/tcp                   ALLOW       Anywhere
5281/tcp                   ALLOW       Anywhere
5298                       ALLOW       Anywhere
52/udp                     ALLOW       Anywhere
80/tcp                     LIMIT       Anywhere
```

A good network defence should span across every single layer of the OSI. While it is important to secure our network devices with strong firewall rules and port security, it is equally as crucial to ensure that our end devices or servers hosting public-facing websites are also well-protected.