

TEAM 6: SAXOPHONE GORILLA

INTRUSION REPORT (2:00PM)

INTRUSION ATTEMPT DETECTED: A range of malicious occurrences were detected on our log server, which possibly affected our web server around the time Mar 26 12:07:26. And beyond.

The Servers

After returning from the fire drill, I noticed a new host had been added to our log server. Our log server is internet-facing (in interest of saving time and working on securing our primary servers) and does not require any sort of administrative power to send logs to it. Simply put, anyone on the competition network can send logs to our server.

I pinged the address and noticed it was down. Looking at the logs generated by the new host, which was IP address 148.48.1.126, I saw a suspicious message:

```
2016-03-26T12:07:39.299-05:00 148.48.1.126 syslog GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
```

View: [Table](#) / [JSON](#) / [Raw](#)

Field	Action	Value
<input checked="" type="checkbox"/> @timestamp		2016-03-26T17:07:39.299Z
<input type="checkbox"/> @version		1
<input type="checkbox"/> _id		AVOz5UQ2UGRC1VKdIPHf
<input type="checkbox"/> _index		logstash-2016.03.26
<input type="checkbox"/> _type		syslog
<input type="checkbox"/> facility		0
<input type="checkbox"/> facility_label		kernel
<input checked="" type="checkbox"/> host		148.48.1.126
<input checked="" type="checkbox"/> message		GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
<input type="checkbox"/> priority		0
<input type="checkbox"/> severity		0
<input type="checkbox"/> severity_label		Emergency
<input type="checkbox"/> tags		_grokparsefailure_sysloginput
<input checked="" type="checkbox"/> type		syslog

After researching this message, I found the following on Nmap's official website:

 Nmap Development mailing list archives

[← By Date →](#) [← By Thread →](#)

Re: More Service Detection notes: HTTP, FTP, DNS, etc

From: doug () hcs.w.org
Date: Fri, 19 May 2006 17:36:03 -0700

On Fri, May 19, 2006 at 02:35:49PM -0700 or thereabouts, Fyodor wrote:
Actually, we may want to include some escaped characters as the way the 404 page returns them may give more details as to the service.

Maybe "GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0\r\n\r\n"

Cheers,
-F

The more I think about it, that looks like a really good probe! The stranger we can make a request the more diverse and identifiable the responses should be. That probe should elicit some interesting responses. It will be very interesting to see how different HTTP based systems will deal with the escaped characters in their 404 replies. Mixing ASCII cases in the escape sequence is a really neat idea (%2C vs. %2e).

Nmap is a security scanner used to discover hosts and services on a computer network for discovery and intelligence-gathering purposes. Immediately I knew that this was no error: red team was trying to think outside of the box in their intrusion attempts.

Shortly after this, my monitoring server alerted me of a failed password alert. I checked the logs:

Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59421 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59427 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59414 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59424 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59420 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59412 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59428 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59417 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59415 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59425 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59418 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59429 ssh2]
Mar 26 13:10:16	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59419 ssh2]
Mar 26 13:10:15	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59423 ssh2]
Mar 26 13:10:15	192.168.1.99	GitLab	message repeated 5 times: [Failed password for root from 148.48.1.126 port 59416 ssh2]
Mar 26 13:10:14	192.168.1.99	GitLab	message repeated 4 times: [Failed password for root from 148.48.1.126 port 59413 ssh2]
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59423 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59417 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59419 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59425 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59413 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59427 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59415 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59418 ssh2
Mar 26 13:10:05	192.168.1.99	GitLab	Failed password for root from 148.48.1.126 port 59416 ssh2

It's the same IP address! Now we are sure that 148.48.1.126 is a malicious user. Because the IP was only attempting to brute force root (and some instances of cdc), we decided NOT to block the IP; the root and cdc passwords were *strong* and would be hard to crack. If we did ban the IP, the user could simply obtain a new IP address and make us go through the work of detecting them again. We decided to let them stay and we have been watching their every move. ~~So far, they have done nothing additional.~~

We now see that the malicious user is trying to login to the web server over SSH which is STRICTLY FORBIDDEN to users. This is definitely red team.

timestamp	< host	< logsource	< message
Mar 26 13:50:57	192.168.1.77	webserver	Connection closed by 148.48.1.126 [preauth]
Mar 26 13:50:53	192.168.1.77	webserver	node=webserver type=USER_AUTH msg=audit(1459018253.215:6297): pid=5817 uid=0 auid=4294967295 ses=4294967295 acct="Helloitsme" exe="/usr/sbin/sshd" hostname=148.48.1.126
Mar 26 13:50:53	192.168.1.77	webserver	Failed password for Helloitsme from 148.48.1.126 port 61330 ssh2
Mar 26 13:50:51	192.168.1.77	webserver	node=webserver type=ANOM_LOGIN_LOCATION msg=audit(1459018251.259:6296): pid=5817 uid=0 auid=4294967295 : msg="op=PAM:pam_access acct="Helloitsme" exe="/usr/sbin/sshd" hostname=148.48.1.126
Mar 26 13:50:51	192.168.1.77	webserver	pam_access(sshd:auth): access denied for user 'Helloitsme' from 148.48.1.126
Mar 26 13:50:51	192.168.1.77	webserver	pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=148.48.1.126 user=Helloitsme

The Phone Calls




























I am also managing all phone calls for the team, and we received many phone calls from a range of people (or the same person with different accents) right after the failed root password alert. I asked them to pull up the green team documentation to verify a certain code in it, to prove that they were actually a green team user. They began to stutter and quickly put me on hold....then the line went dead. This happened on two other instances with similar results. We have not heard back from any “green team member” since (except for the legitimate ones who could locate their documentation).

In other news

No other servers besides GitLab and possibly the Log Server were at risk (except maybe being scanned by Nmap). This alert screen shows the failed passwords for GitLab, and also shows that our flags have remained untouched (ignore the config files alert, it should not be an alert).

Alert Name	Created By	Last Run	Status	Alert Output
BLUE FLAG ALERT	dlimanow	Sat, 26 Mar 2016 13:33:42 -0500	OK	OK: 0 matching entries found logs=0;1;1
Failed Password	dlimanow	Sat, 26 Mar 2016 13:34:02 -0500	CRITICAL	CRITICAL: 2 matching entries found logs=2;1;1
Important Config Files Changed	dlimanow	Sat, 26 Mar 2016 13:34:02 -0500	CRITICAL	CRITICAL: 5 matching entries found logs=5;1;1
RED FLAG ALERT	dlimanow	Sat, 26 Mar 2016 13:33:42 -0500	OK	OK: 0 matching entries found logs=0;1;1

The service scanner on IScore (and our monitoring server) is showing all services and hosts are alive, and no flags have been stolen or placed.

Host		Status	Duration	Attempt	Last Check	Status Information
GitLab	  	Up	5h 58m 10s	1/5	2016-03-26 13:43:14	OK - 192.168.1.99: rta 0.400ms, lost 0%
Key Escrow Debian	  	Up	14h 11m 24s	1/5	2016-03-26 13:43:20	OK - 192.168.1.18: rta 0.360ms, lost 0%
LDAP	  	Up	11h 18m 3s	1/5	2016-03-26 13:41:47	OK - 192.168.1.8: rta 2.237ms, lost 0%
localhost	  	Up	36d 0h 35m 39s	1/10	2016-03-26 13:45:57	OK - 127.0.0.1: rta 0.029ms, lost 0%
Nagios Log Server	  	Up	11h 24m 2s	1/1	2016-03-26 13:44:42	OK - 192.168.1.6: rta 0.156ms, lost 0%
Runner Debian	  	Up	11h 11m 35s	1/5	2016-03-26 13:43:02	OK - 192.168.1.22: rta 2.795ms, lost 0%
Runner Fedora	  	Up	11h 10m 57s	1/5	2016-03-26 13:43:47	OK - 192.168.1.23: rta 0.360ms, lost 0%
Shell	  	Up	14h 3m 21s	1/5	2016-03-26 13:41:31	OK - 192.168.1.10: rta 0.362ms, lost 0%
Web	  	Up	11h 18m 42s	1/5	2016-03-26 13:46:07	OK - 192.168.1.77: rta 0.397ms, lost 0%

Last Updated: 2016-03-26 13:46:25