TEAM 6: SAXOPHONE GORILLA INTRUSION REPORT (12:00PM)

No intrusions were detected on all of our servers as of Mar 26 11:39:34.

We know that no servers were compromised because

1) Nothing is being reported by IScore (all services up, flags not compromised)
2) Our log server/monitoring server combination is not reporting anything suspicious
    a) No alerts fired for the following:
        i) Failed passwords (more than three in a two minute time frame)
        ii) Flag directory/file write or read change
        iii) Common config file change
    b) We decided to alert for this things because that is most likely what Red Team would trigger if they were able to get on our network with the intention of malicious passwords. We want to watch failed passwords for brute-force attacks or the like. We want to audit the flag locations for any changes. Finally, any config file changes, such as for sudoers or time changes should tell us that a malicious user is probably present.

We have noticed that there was a failed password attempt on our GitLab server, so we are watching this IP/user closely because a failed password attempt could mean that Red Team is attempting to login to these users using predefined, default passwords or by some brute-force means.

```
Mar 26 09:45:19    192.168.1.99    GitLab    Failed password for Orin from 148.48.1.130 port 34422 ssh2
```

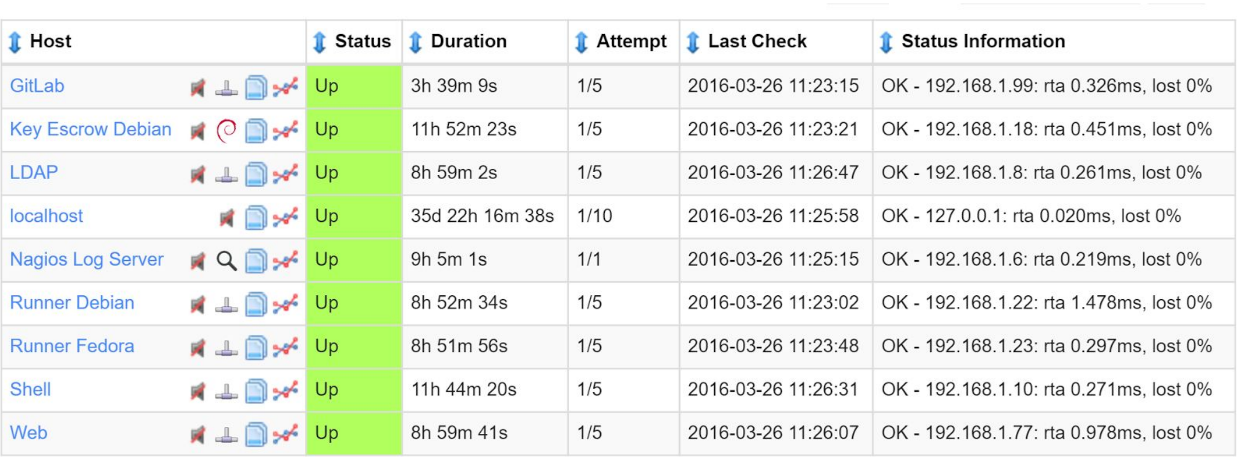
Log files showing no problems (accounts for *all* servers). I did not include the config change alert because it is firing due to changes in the shadow file (normal operation) on some servers.

BLUE FLAG ALERT	dlimanow	Sat, 26 Mar 2016 11:12:26 -0500	OK	OK: 0 matching entries found |logs=0;1;1	None	

Failed Password	dlimanow	Sat, 26 Mar 2016 11:13:47 -0500	OK	OK: 0 matching entries found |logs=0;1;1

RED FLAG ALERT	dlimanow	Sat, 26 Mar 2016 11:12:26 -0500	OK	OK: 0 matching entries found |logs=0;1;1	None

The following screenshot, from our monitoring server, shows all hosts are alive and healthy. This means that the Red Team has not done anything drastic to bring any of our services down.



Host	Status	Duration	Attempt	Last Check	Status Information
GitLab	Up	3h 39m 9s	1/5	2016-03-26 11:23:15	OK - 192.168.1.99: rta 0.326ms, lost 0%
Key Escrow Debian	Up	11h 52m 23s	1/5	2016-03-26 11:23:21	OK - 192.168.1.18: rta 0.451ms, lost 0%
LDAP	Up	8h 59m 2s	1/5	2016-03-26 11:26:47	OK - 192.168.1.8: rta 0.261ms, lost 0%
localhost	Up	35d 22h 16m 38s	1/10	2016-03-26 11:25:58	OK - 127.0.0.1: rta 0.020ms, lost 0%
Nagios Log Server	Up	9h 5m 1s	1/1	2016-03-26 11:25:15	OK - 192.168.1.6: rta 0.219ms, lost 0%
Runner Debian	Up	8h 52m 34s	1/5	2016-03-26 11:23:02	OK - 192.168.1.22: rta 1.478ms, lost 0%
Runner Fedora	Up	8h 51m 56s	1/5	2016-03-26 11:23:48	OK - 192.168.1.23: rta 0.297ms, lost 0%
Shell	Up	11h 44m 20s	1/5	2016-03-26 11:26:31	OK - 192.168.1.10: rta 0.271ms, lost 0%
Web	Up	8h 59m 41s	1/5	2016-03-26 11:26:07	OK - 192.168.1.77: rta 0.978ms, lost 0%

We are manually watching commands executed on all of our servers through Nagios LS. So far nothing drastic has been commanded on our terminals. We can filter for “comm” (command run) and look at the uid (user’s id). By running getent passwd *uid* we can determine which user ran which command. The log source is given as the server hostname for quick identification. This type of logging is implemented on all of our primary servers.

logsource	ShellServer
message	node=ShellServer type=SYSCALL

	uid=16037 gid=500 euid=16037 suid=16037 fsuid=16037 egid=500 sgid=500 fsgid=500 tty=pts5 ses=313 comm="uname"