CONFIDENTIAL

Intrusion Report for CDC

Iowa State University
TEAM 5

VERSION 12:00PM

Table of Contents

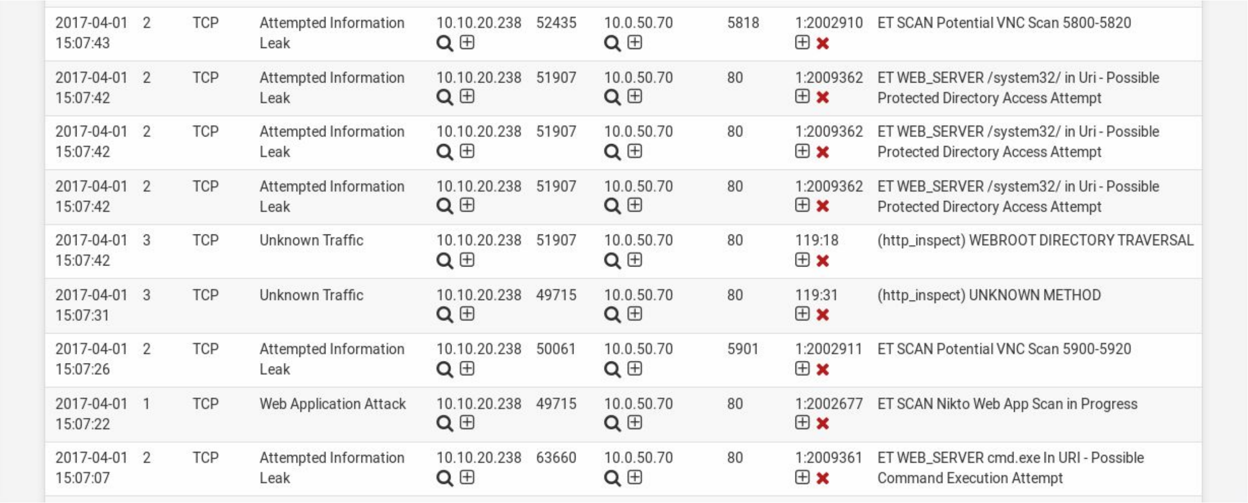
Executive Summary

The purpose of Intrusion Reports is to inform White Team of any detected intrusion attempts. Detailed in this document is descriptions of all attempted attacks/hacks/intrusions on any of our servers within our network. Screenshots and raw log data pertaining to any abnormalities will be complemented with explanations. Steps taken to mitigate attacks, if determined that an attack is imminent, occurring, or passed will be highlighted in this document.

Server Reporting

Firewall Server Report (Reporter: Stefan)

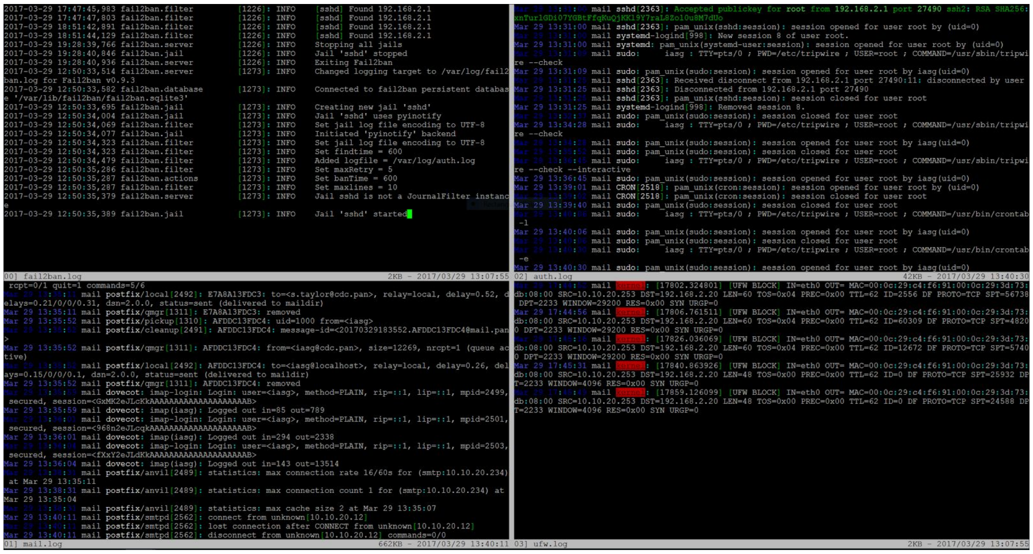
Time	Event	Description and evidence
	N/A	**Nothing to report** We did not see much activity in the firewall logs against the firewall server itself. We did see the red team attempt to access protected directories as well as scan for potential vulnerabilities on our servers.



2017-04-01 15:07:43	2	TCP	Attempted Information Leak	10.10.20.238	52435	10.0.50.70	5818	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2017-04-01 15:07:42	2	TCP	Attempted Information Leak	10.10.20.238	51907	10.0.50.70	80	1:2009362	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt
2017-04-01 15:07:42	2	TCP	Attempted Information Leak	10.10.20.238	51907	10.0.50.70	80	1:2009362	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt
2017-04-01 15:07:42	2	TCP	Attempted Information Leak	10.10.20.238	51907	10.0.50.70	80	1:2009362	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt
2017-04-01 15:07:42	3	TCP	Unknown Traffic	10.10.20.238	51907	10.0.50.70	80	119:18	(http_inspect) WEBROOT DIRECTORY TRAVERSAL
2017-04-01 15:07:31	3	TCP	Unknown Traffic	10.10.20.238	49715	10.0.50.70	80	119:31	(http_inspect) UNKNOWN METHOD
2017-04-01 15:07:26	2	TCP	Attempted Information Leak	10.10.20.238	50061	10.0.50.70	5901	1:2002911	ET SCAN Potential VNC Scan 5900-5920
2017-04-01 15:07:22	1	TCP	Web Application Attack	10.10.20.238	49715	10.0.50.70	80	1:2002677	ET SCAN Nikto Web App Scan in Progress
2017-04-01 15:07:07	2	TCP	Attempted Information Leak	10.10.20.238	63660	10.0.50.70	80	1:2009361	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt

Mail Server Report (Reporter: Stefan)

Time	Event	Description and evidence
	N/A	**Nothing to report**

		We have been monitoring /var/auth.log, /var/fail2ban.log, /var/mail.log/ and /var/ufw.log to look for suspicious activity, but have not found any recently. 

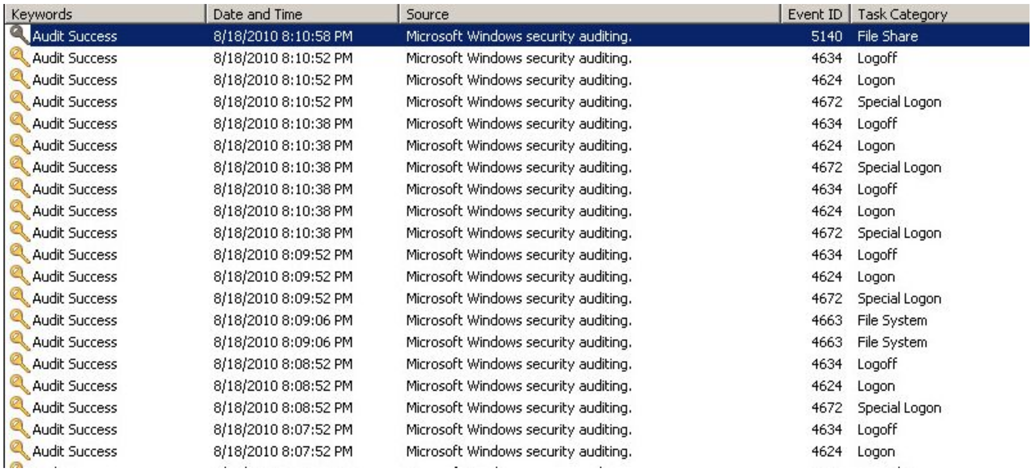
```
2017-03-29 17:47:45,983 fail2ban.filter         [1226]: INFO    [sshd] Found 192.168.2.1
2017-03-29 17:47:47,803 fail2ban.filter         [1226]: INFO    [sshd] Found 192.168.2.1
2017-03-29 18:51:42,891 fail2ban.filter         [1226]: INFO    [sshd] Found 192.168.2.1
2017-03-29 18:51:44,129 fail2ban.filter         [1226]: INFO    [sshd] Found 192.168.2.1
2017-03-29 19:28:39,766 fail2ban.server         [1226]: INFO    Stopping all jails
2017-03-29 19:28:40,846 fail2ban.jail           [1226]: INFO    Jail 'sshd' stopped
2017-03-29 19:28:40,936 fail2ban.server         [1226]: INFO    Exiting Fail2ban
2017-03-29 12:50:33,514 fail2ban.server         [1273]: INFO    Changed logging target to /var/log/fail2
ban.log for Fail2ban v0.9.3
2017-03-29 12:50:33,582 fail2ban.database       [1273]: INFO    Connected to fail2ban persistent databas
e '/var/lib/fail2ban/fail2ban.sqlite3'
2017-03-29 12:50:33,695 fail2ban.jail           [1273]: INFO    Creating new jail 'sshd'
2017-03-29 12:50:34,004 fail2ban.jail           [1273]: INFO    Jail 'sshd' uses pyinotify
2017-03-29 12:50:34,069 fail2ban.filter         [1273]: INFO    Set jail log file encoding to UTF-8
2017-03-29 12:50:34,077 fail2ban.jail           [1273]: INFO    Initiated 'pyinotify' backend
2017-03-29 12:50:34,323 fail2ban.filter         [1273]: INFO    Set jail log file encoding to UTF-8
2017-03-29 12:50:34,323 fail2ban.filter         [1273]: INFO    Set findtime = 600
2017-03-29 12:50:34,479 fail2ban.filter         [1273]: INFO    Added logfile = /var/log/auth.log
2017-03-29 12:50:35,286 fail2ban.filter         [1273]: INFO    Set maxRetry = 5
2017-03-29 12:50:35,287 fail2ban.actions        [1273]: INFO    Set banTime = 600
2017-03-29 12:50:35,287 fail2ban.filter         [1273]: INFO    Set maxlines = 10
2017-03-29 12:50:35,379 fail2ban.server         [1273]: INFO    Jail sshd is not a JournalFilter instanc
e
2017-03-29 12:50:35,389 fail2ban.jail           [1273]: INFO    Jail 'sshd' started
00] fail2ban.log                                                        2KB - 2017/03/29 13:07:55
```

```
 rcpt=0/1 quit=1 commands=5/6
Mar 29 13:35:11 mail postfix/local[2492]: E7A8A13FDC3: to=<s.taylor@cdc.pan>, relay=local, delay=0.52, d
elays=0.21/0/0/0.31, dsn=2.0.0, status=sent (delivered to maildir)
Mar 29 13:35:11 mail postfix/qmgr[1311]: E7A8A13FDC3: removed
Mar 29 13:35:52 mail postfix/pickup[1310]: AFDDC13FDC4: uid=1000 from=<iasg>
Mar 29 13:35:52 mail postfix/cleanup[2491]: AFDDC13FDC4: message-id=<20170329183552.AFDDC13FDC4@mail.pan
>
Mar 29 13:35:52 mail postfix/qmgr[1311]: AFDDC13FDC4: from=<iasg@cdc.pan>, size=12269, nrcpt=1 (queue ac
tive)
Mar 29 13:35:52 mail postfix/local[2492]: AFDDC13FDC4: to=<iasg@localhost>, relay=local, delay=0.26, del
ays=0.15/0/0/0.1, dsn=2.0.0, status=sent (delivered to maildir)
Mar 29 13:35:52 mail postfix/qmgr[1311]: AFDDC13FDC4: removed
Mar 29 13:35:59 mail dovecot: imap-login: Login: user=<iasg>, method=PLAIN, rip=::1, lip=::1, mpid=2499,
 secured, session=<GxMK2eJLcKkAAAAAAAAAAAAAAAAAAAAB>
Mar 29 13:35:59 mail dovecot: imap(iasg): Logged out in=85 out=789
Mar 29 13:36:01 mail dovecot: imap-login: Login: user=<iasg>, method=PLAIN, rip=::1, lip=::1, mpid=2501,
 secured, session=<968n2eJLcqkAAAAAAAAAAAAAAAAAAAAB>
Mar 29 13:36:01 mail dovecot: imap(iasg): Logged out in=294 out=2338
Mar 29 13:36:04 mail dovecot: imap-login: Login: user=<iasg>, method=PLAIN, rip=::1, lip=::1, mpid=2503,
 secured, session=<fXxY2eJLdKkAAAAAAAAAAAAAAAAAAAAB>
Mar 29 13:36:04 mail dovecot: imap(iasg): Logged out in=143 out=13514
Mar 29 13:38:31 mail postfix/anvil[2489]: statistics: max connection rate 16/60s for (smtp:10.10.20.234)
 at Mar 29 13:35:11
Mar 29 13:38:31 mail postfix/anvil[2489]: statistics: max connection count 1 for (smtp:10.10.20.234) at
Mar 29 13:35:04
Mar 29 13:38:31 mail postfix/anvil[2489]: statistics: max cache size 2 at Mar 29 13:35:07
Mar 29 13:40:11 mail postfix/smtpd[2562]: connect from unknown[10.10.20.12]
Mar 29 13:40:11 mail postfix/smtpd[2562]: lost connection after CONNECT from unknown[10.10.20.12]
Mar 29 13:40:11 mail postfix/smtpd[2562]: disconnect from unknown[10.10.20.12] commands=0/0
01] mail.log                                                      662KB - 2017/03/29 13:40:11
```

```
Mar 29 13:31:00 mail sshd[2363]: Accepted publickey for root from 192.168.2.1 port 27490 ssh2: RSA SHA256:
xnTurlGDi07YGBtFfqKuQjKKl9Y7raL8Zol0u8M7dUo
Mar 29 13:31:00 mail sshd[2363]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 29 13:31:00 mail systemd-logind[998]: New session 8 of user root.
Mar 29 13:31:00 mail systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Mar 29 13:31:09 mail sudo:     iasg : TTY=pts/0 ; PWD=/etc/tripwire ; USER=root ; COMMAND=/usr/sbin/tripwi
re --check
Mar 29 13:31:09 mail sudo: pam_unix(sudo:session): session opened for user root by iasg(uid=0)
Mar 29 13:31:25 mail sshd[2363]: Received disconnect from 192.168.2.1 port 27490:11: disconnected by user
Mar 29 13:31:25 mail sshd[2363]: Disconnected from 192.168.2.1 port 27490
Mar 29 13:31:25 mail sshd[2363]: pam_unix(sshd:session): session closed for user root
Mar 29 13:31:25 mail systemd-logind[998]: Removed session 8.
Mar 29 13:32:37 mail sudo: pam_unix(sudo:session): session closed for user root
Mar 29 13:34:28 mail sudo:     iasg : TTY=pts/0 ; PWD=/etc/tripwire ; USER=root ; COMMAND=/usr/sbin/tripwi
re --check
Mar 29 13:34:28 mail sudo: pam_unix(sudo:session): session opened for user root by iasg(uid=0)
Mar 29 13:35:52 mail sudo: pam_unix(sudo:session): session closed for user root
Mar 29 13:36:45 mail sudo:     iasg : TTY=pts/0 ; PWD=/etc/tripwire ; USER=root ; COMMAND=/usr/sbin/tripwi
re --check --interactive
Mar 29 13:36:45 mail sudo: pam_unix(sudo:session): session opened for user root by iasg(uid=0)
Mar 29 13:39:01 mail CRON[2518]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 29 13:39:02 mail CRON[2518]: pam_unix(cron:session): session closed for user root
Mar 29 13:39:40 mail sudo: pam_unix(sudo:session): session closed for user root
Mar 29 13:40:06 mail sudo:     iasg : TTY=pts/0 ; PWD=/etc/tripwire ; USER=root ; COMMAND=/usr/bin/crontab
 -l
Mar 29 13:40:06 mail sudo: pam_unix(sudo:session): session opened for user root by iasg(uid=0)
Mar 29 13:40:06 mail sudo: pam_unix(sudo:session): session closed for user root
Mar 29 13:40:30 mail sudo:     iasg : TTY=pts/0 ; PWD=/etc/tripwire ; USER=root ; COMMAND=/usr/bin/crontab
 -e
Mar 29 13:40:30 mail sudo: pam_unix(sudo:session): session opened for user root by iasg(uid=0)
02] auth.log                                                            42KB - 2017/03/29 13:40:30
```

```
Mar 29 17:44:52 mail kernel: [17802.324801] [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:c4:f6:91:00:0c:29:3d:73:
db:08:00 SRC=10.10.20.253 DST=192.168.2.20 LEN=60 TOS=0x04 PREC=0x00 TTL=62 ID=2556 DF PROTO=TCP SPT=56738
 DPT=2233 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 29 17:44:56 mail kernel: [17806.761511] [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:c4:f6:91:00:0c:29:3d:73:
db:08:00 SRC=10.10.20.253 DST=192.168.2.20 LEN=60 TOS=0x04 PREC=0x00 TTL=62 ID=60309 DF PROTO=TCP SPT=4820
0 DPT=2233 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 29 17:45:16 mail kernel: [17826.036069] [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:c4:f6:91:00:0c:29:3d:73:
db:08:00 SRC=10.10.20.253 DST=192.168.2.20 LEN=60 TOS=0x04 PREC=0x00 TTL=62 ID=12672 DF PROTO=TCP SPT=5740
0 DPT=2233 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 29 17:45:31 mail kernel: [17840.863926] [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:c4:f6:91:00:0c:29:3d:73:
db:08:00 SRC=10.10.20.253 DST=192.168.2.20 LEN=48 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=TCP SPT=25932 DP
T=2233 WINDOW=4096 RES=0x00 SYN URGP=0
Mar 29 17:45:49 mail kernel: [17859.126099] [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:c4:f6:91:00:0c:29:3d:73:
db:08:00 SRC=10.10.20.253 DST=192.168.2.20 LEN=48 TOS=0x00 PREC=0x00 TTL=62 ID=0 DF PROTO=TCP SPT=24588 DP
T=2233 WINDOW=4096 RES=0x00 SYN URGP=0
03] ufw.log                                                             2KB - 2017/03/29 13:07:55
```

AD Server Report (Reporter: Megan)

Time	**Event**	**Description and evidence**
	Nothing to Report	

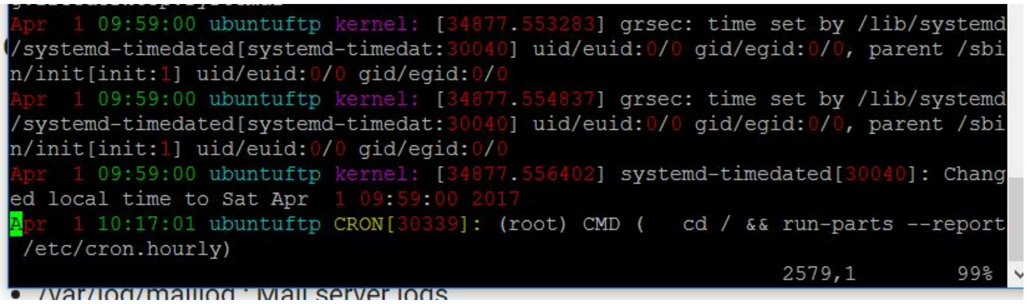
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/18/2010 8:10:58 PM	Microsoft Windows security auditing.	5140	File Share
Audit Success	8/18/2010 8:10:52 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:10:52 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/18/2010 8:10:52 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/18/2010 8:10:38 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/18/2010 8:09:52 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:09:52 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/18/2010 8:09:52 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/18/2010 8:09:06 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	8/18/2010 8:09:06 PM	Microsoft Windows security auditing.	4663	File System
Audit Success	8/18/2010 8:08:52 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:08:52 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	8/18/2010 8:08:52 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	8/18/2010 8:07:52 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	8/18/2010 8:07:52 PM	Microsoft Windows security auditing.	4624	Logon

File Server Report (Reporter: Daniel)

Time	**Event**	**Description and evidence**

<table>
<tr>
<td><strong>10:05 (GMT)</strong></td>
<td><strong>Syslog file changes</strong></td>
<td>

Syslog is reporting OK things, such as the time being synced. We see no evidence of nefarious behavior on this server.



```
Apr  1 09:59:00 ubuntuftp kernel: [34877.553283] grsec: time set by /lib/systemd
/systemd-timedated[systemd-timedat:30040] uid/euid:0/0 gid/egid:0/0, parent /sbi
n/init[init:1] uid/euid:0/0 gid/egid:0/0
Apr  1 09:59:00 ubuntuftp kernel: [34877.554837] grsec: time set by /lib/systemd
/systemd-timedated[systemd-timedat:30040] uid/euid:0/0 gid/egid:0/0, parent /sbi
n/init[init:1] uid/euid:0/0 gid/egid:0/0
Apr  1 09:59:00 ubuntuftp kernel: [34877.556402] systemd-timedated[30040]: Chang
ed local time to Sat Apr  1 09:59:00 2017
Apr  1 10:17:01 ubuntuftp CRON[30339]: (root) CMD (   cd / && run-parts --report
 /etc/cron.hourly)
                                                           2579,1        99%
```

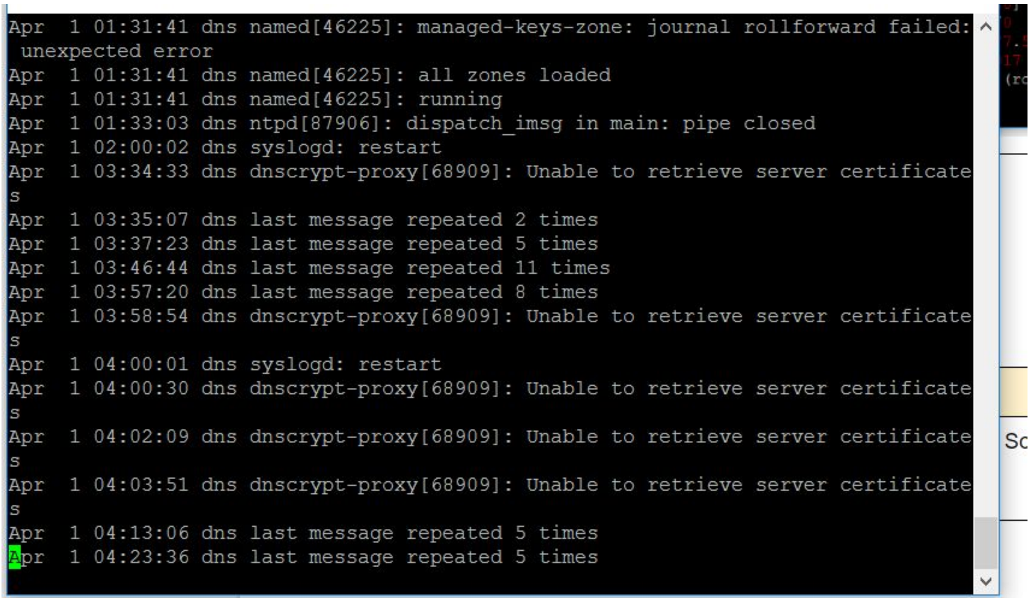
- /var/log/maillog : Mail server logs

</td>
</tr>
</table>

DNS/NTP Server Report (Reporter: Daniel)

<table>
<tr>
<th>Time</th>
<th>Event</th>
<th>Description and evidence</th>
</tr>
<tr>
<td>11:23(GMT)</td>
<td>Checked the system logs</td>
<td>

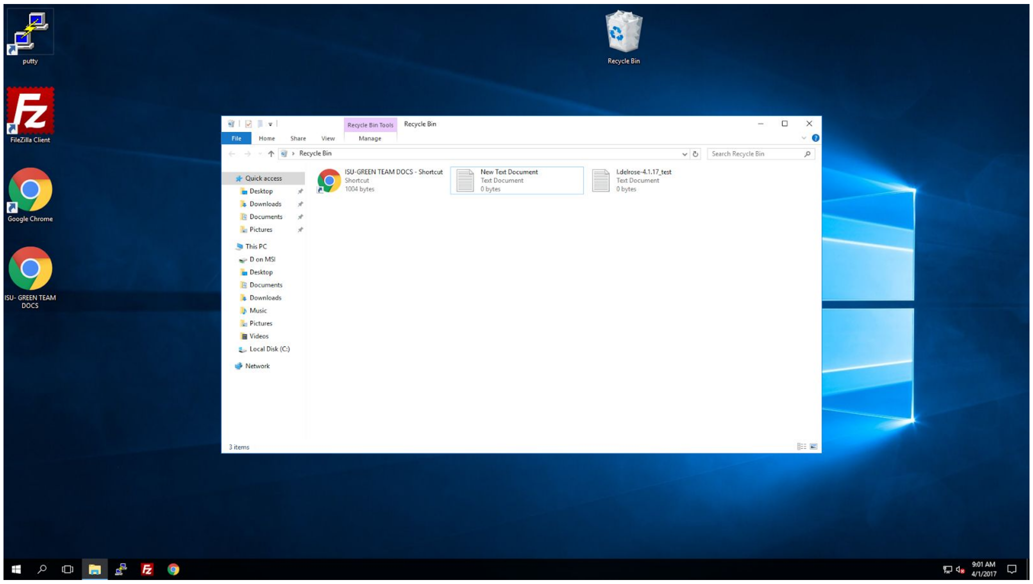
Only thing we could find in logs were DNS errors. We do not believe this has to do with an intrusion, but one of our engineers will look into this to ensure there are no vulnerabilities involved.



```
Apr  1 01:31:41 dns named[46225]: managed-keys-zone: journal rollforward failed:
 unexpected error
Apr  1 01:31:41 dns named[46225]: all zones loaded
Apr  1 01:31:41 dns named[46225]: running
Apr  1 01:33:03 dns ntpd[87906]: dispatch_imsg in main: pipe closed
Apr  1 02:00:02 dns syslogd: restart
Apr  1 03:34:33 dns dnscrypt-proxy[68909]: Unable to retrieve server certificate
s
Apr  1 03:35:07 dns last message repeated 2 times
Apr  1 03:37:23 dns last message repeated 5 times
Apr  1 03:46:44 dns last message repeated 11 times
Apr  1 03:57:20 dns last message repeated 8 times
Apr  1 03:58:54 dns dnscrypt-proxy[68909]: Unable to retrieve server certificate
s
Apr  1 04:00:01 dns syslogd: restart
Apr  1 04:00:30 dns dnscrypt-proxy[68909]: Unable to retrieve server certificate
s
Apr  1 04:02:09 dns dnscrypt-proxy[68909]: Unable to retrieve server certificate
s
Apr  1 04:03:51 dns dnscrypt-proxy[68909]: Unable to retrieve server certificate
s
Apr  1 04:13:06 dns last message repeated 5 times
Apr  1 04:23:36 dns last message repeated 5 times
```

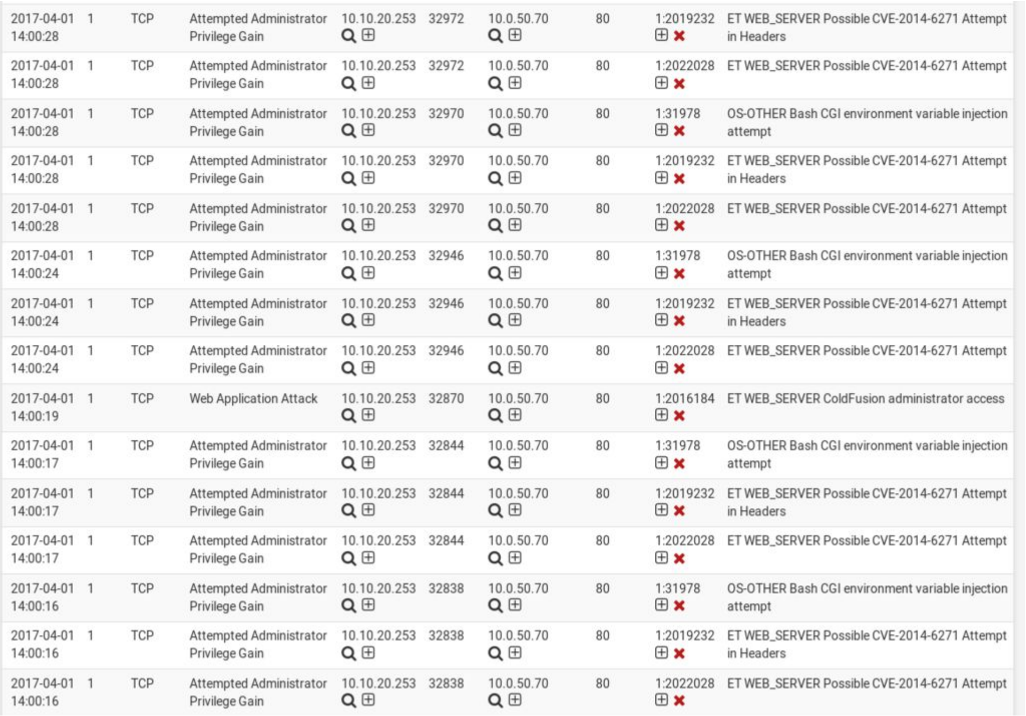
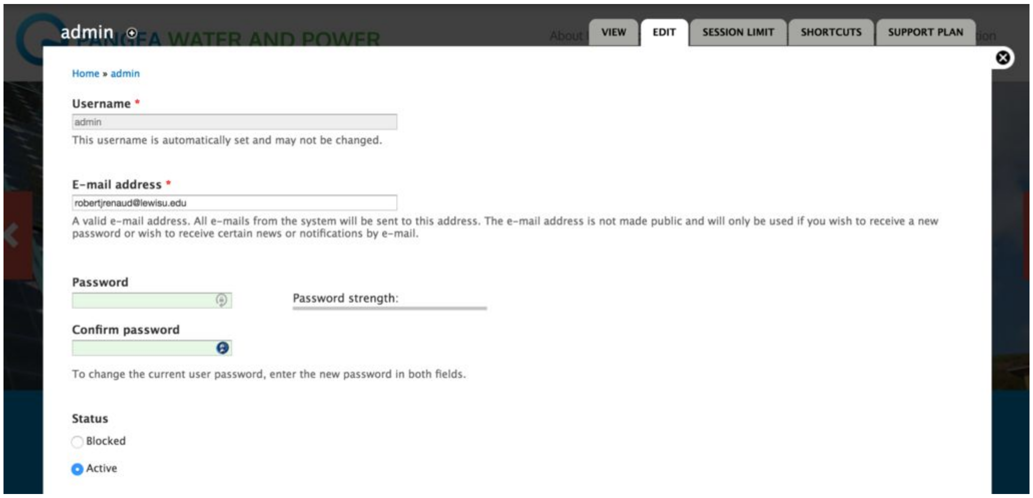
</td>
</tr>
</table>

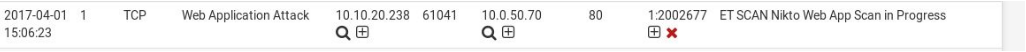
RDP Server Report (Reporter: Logan)

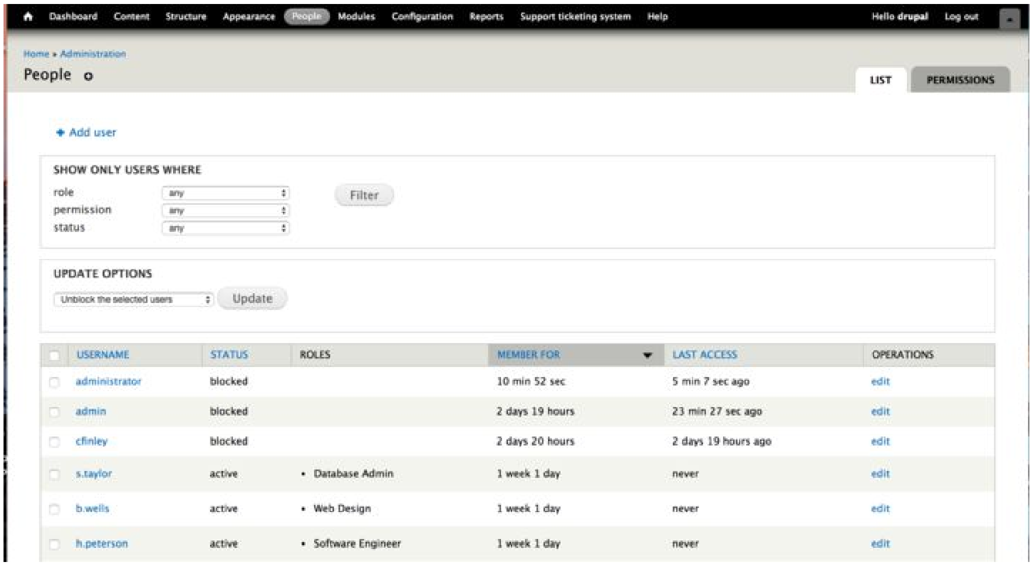
Time	Event	Description and evidence
11:01 GMT	Suspicious files found	Two files containing no data but named in a manner to arouse suspicion, were located in the recycle bin. 

WWW Server Report (Reporter: Megan)

Time	Event	Description and evidence

<table>
<tr>
<td>08:55 AM (CTL)</td>
<td>The username is admin, but is not an administrative account.</td>
<td>

<table>
<tr><td>2017-04-01 14:00:28</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32972</td><td>10.0.50.70</td><td>80</td><td>1:2019232</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</td></tr>
<tr><td>2017-04-01 14:00:28</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32972</td><td>10.0.50.70</td><td>80</td><td>1:2022028</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt</td></tr>
<tr><td>2017-04-01 14:00:28</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32970</td><td>10.0.50.70</td><td>80</td><td>1:31978</td><td>OS-OTHER Bash CGI environment variable injection attempt</td></tr>
<tr><td>2017-04-01 14:00:28</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32970</td><td>10.0.50.70</td><td>80</td><td>1:2019232</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</td></tr>
<tr><td>2017-04-01 14:00:28</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32970</td><td>10.0.50.70</td><td>80</td><td>1:2022028</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt</td></tr>
<tr><td>2017-04-01 14:00:24</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32946</td><td>10.0.50.70</td><td>80</td><td>1:31978</td><td>OS-OTHER Bash CGI environment variable injection attempt</td></tr>
<tr><td>2017-04-01 14:00:24</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32946</td><td>10.0.50.70</td><td>80</td><td>1:2019232</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</td></tr>
<tr><td>2017-04-01 14:00:24</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32946</td><td>10.0.50.70</td><td>80</td><td>1:2022028</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt</td></tr>
<tr><td>2017-04-01 14:00:19</td><td>1</td><td>TCP</td><td>Web Application Attack</td><td>10.10.20.253</td><td>32870</td><td>10.0.50.70</td><td>80</td><td>1:2016184</td><td>ET WEB_SERVER ColdFusion administrator access</td></tr>
<tr><td>2017-04-01 14:00:17</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32844</td><td>10.0.50.70</td><td>80</td><td>1:31978</td><td>OS-OTHER Bash CGI environment variable injection attempt</td></tr>
<tr><td>2017-04-01 14:00:17</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32844</td><td>10.0.50.70</td><td>80</td><td>1:2019232</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</td></tr>
<tr><td>2017-04-01 14:00:17</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32844</td><td>10.0.50.70</td><td>80</td><td>1:2022028</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt</td></tr>
<tr><td>2017-04-01 14:00:16</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32838</td><td>10.0.50.70</td><td>80</td><td>1:31978</td><td>OS-OTHER Bash CGI environment variable injection attempt</td></tr>
<tr><td>2017-04-01 14:00:16</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32838</td><td>10.0.50.70</td><td>80</td><td>1:2019232</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</td></tr>
<tr><td>2017-04-01 14:00:16</td><td>1</td><td>TCP</td><td>Attempted Administrator Privilege Gain</td><td>10.10.20.253</td><td>32838</td><td>10.0.50.70</td><td>80</td><td>1:2022028</td><td>ET WEB_SERVER Possible CVE-2014-6271 Attempt</td></tr>
</table>


Home » admin
Username *
admin
This username is automatically set and may not be changed.
E-mail address *
robertjrenaud@lewisu.edu
A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by e-mail.
Password
Password strength:
Confirm password
To change the current user password, enter the new password in both fields.
Status
○ Blocked
● Active
</td>
</tr>
<tr>
<td></td>
<td>Them trying to hit our Web server using a nikto scan</td>
<td>

<table>
<tr><td>2017-04-01 15:06:23</td><td>1</td><td>TCP</td><td>Web Application Attack</td><td>10.10.20.238</td><td>61041</td><td>10.0.50.70</td><td>80</td><td>1:2002677</td><td>ET SCAN Nikto Web App Scan in Progress</td></tr>
</table>
</td>
</tr>
</table>

09:30	Red added another malicious user "administrator" (user was a Drupal web user, without any permissions except posting comments). Mitigation: disabled new user registration and user account	

SHOW ONLY USERS WHERE

role: any
permission: any
status: any

UPDATE OPTIONS

Unblock the selected users

□	USERNAME	STATUS	ROLES	MEMBER FOR	LAST ACCESS	OPERATIONS
□	administrator	blocked		10 min 52 sec	5 min 7 sec ago	edit
□	admin	blocked		2 days 19 hours	23 min 27 sec ago	edit
□	cfinley	blocked		2 days 20 hours	2 days 19 hours ago	edit
□	s.taylor	active	• Database Admin	1 week 1 day	never	edit
□	b.wells	active	• Web Design	1 week 1 day	never	edit
□	h.peterson	active	• Software Engineer	1 week 1 day	never	edit

Social Engineering/Intelligence Report

Several people have asked us questions regarding our servers and a few have been taking pictures of us. We do not know if these people are red team or not, so we are being extremely cautious with them. Our team leader asked a “reporter” to walk into the hallway with him if he wanted to interview him, rather than having strangers loiter near our screens which could show potentially sensitive data.