CONFIDENTIAL

Intrusion Report for CDC

Iowa State University
TEAM 5

VERSION 4:00PM

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.

Last 10 Minute Leak!

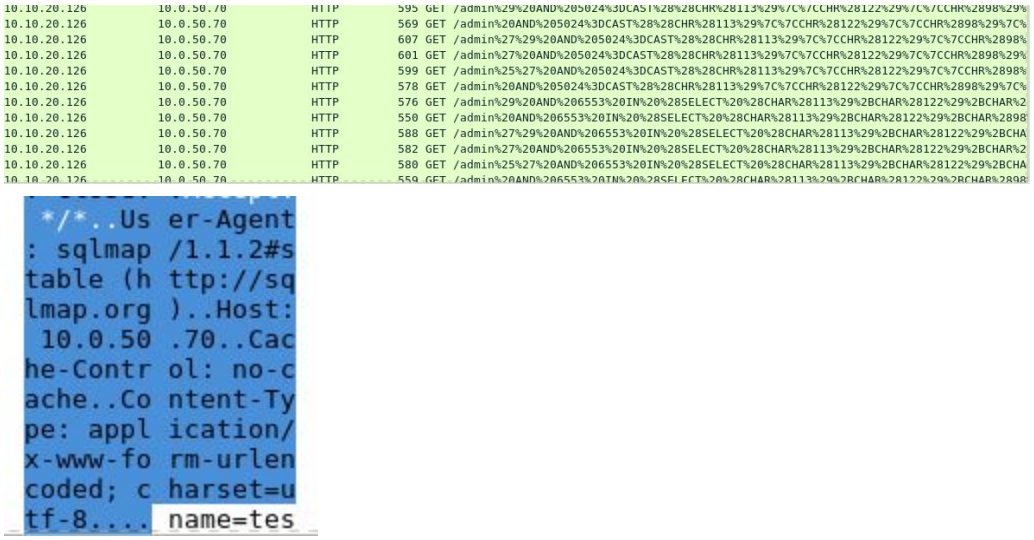
A laptop with all of our credentials was lost. Red traffic may have attempted to access us, but all of our services are jailed. You must use a private key to logon as a root account for any of our boxes, so there is no way that red team could gain root unless they were to steal our locally-held key.

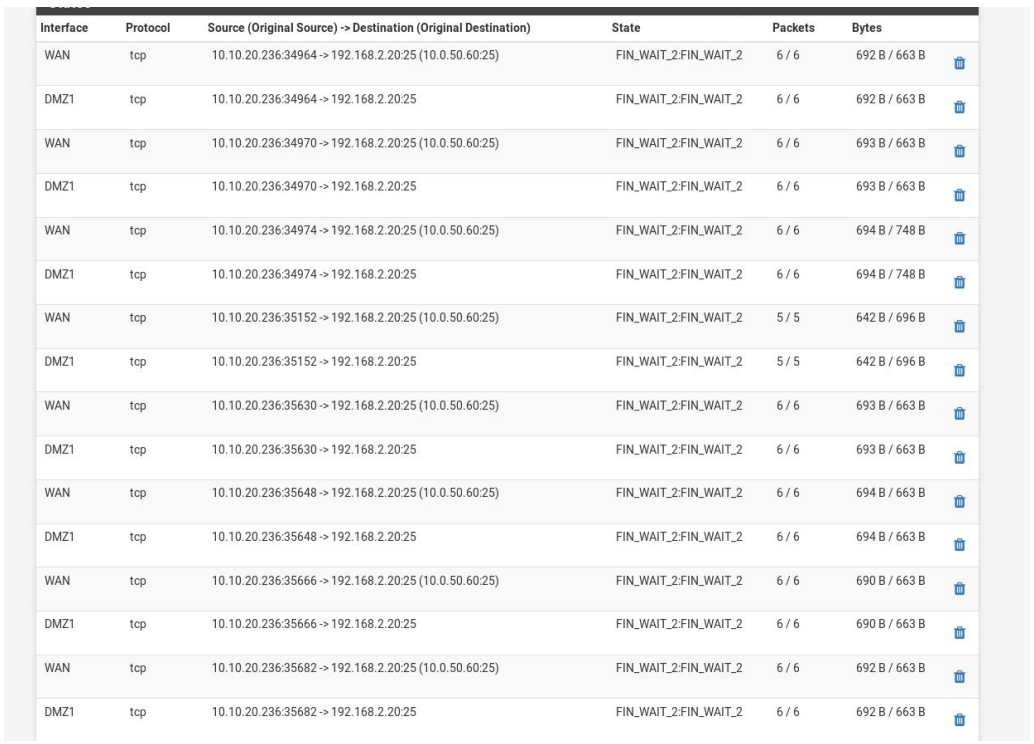
Server Reporting

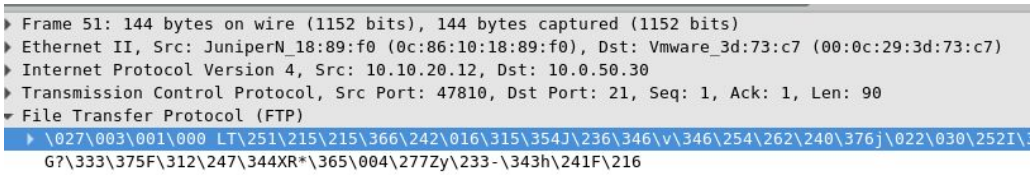
Firewall Server Report (Reporter: Stefan)

Time	Event	Description and evidence
15:00	Attempt to brute-force Mail server	2017-04-01 15:00:55 3 TCP Misc activity 10.10.20.229 57882 10.0.50.30 993 1:2002995 ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack 2017-04-01 15:00:53 3 TCP Misc activity 10.10.20.229 57101 10.0.50.40 995 1:2002993 ET SCAN Rapid POP3S Connections - Possible Brute Force Attack
Time was off on server	NMAP Script attacking Mail server	[Full request URI: http://10.0.50.60/] [HTTP request 1/1] File Data: 88 bytes HTML Form URL Encoded: application/x-www-form-urlencoded Form item: "<methodCall> <methodName>system.listMethods</methodName> <params> 00 00 0c 29 3d 73 c7 0c 86 10 18 89 f0 08 00 45 00 ..)=s... ......E. 10 01 5a 1c c4 40 00 7f 06 96 dd 0a 0a 00 b7 0a 00 .Z..@... ..... 20 32 3c 0f 52 00 50 06 f1 9c cb 70 b3 84 b1 50 18 2<.R.P.. ..p...P. 30 01 00 94 95 00 00 50 4f 53 54 20 2f 20 48 54 54 .....PO ST / HTT 40 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e P/1.1..U ser-Agen 50 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (60 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4e 6d 61 70 compatib le; Nmap 70 20 53 63 72 69 70 74 69 6e 67 20 45 6e 67 69 6e Scripti ng Engin 80 65 3b 20 68 74 74 70 73 3a 2f 2f 6e 6d 61 70 2e e; https ://nmap. 90 6f 72 67 2f 62 6f 6f 6b 2f 6e 73 65 2e 68 74 6d org/book /nse.htm a0 6c 29 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 l)..Conn ection: b0 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 close..C ontent-T

<table>
<tr>
<td>Time was off on server</td>
<td>SQL Injection attack with encoding URL params

SQLMap script being run on web server</td>
<td>


</td>
</tr>
<tr>
<td>15:40</td>
<td>Mail server Brute Force</td>
<td>


Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	tcp	10.10.20.236:34964 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	692 B / 663 B
DMZ1	tcp	10.10.20.236:34964 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	692 B / 663 B
WAN	tcp	10.10.20.236:34970 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	693 B / 663 B
DMZ1	tcp	10.10.20.236:34970 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	693 B / 663 B
WAN	tcp	10.10.20.236:34974 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	694 B / 748 B
DMZ1	tcp	10.10.20.236:34974 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	694 B / 748 B
WAN	tcp	10.10.20.236:35152 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	5 / 5	642 B / 696 B
DMZ1	tcp	10.10.20.236:35152 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	5 / 5	642 B / 696 B
WAN	tcp	10.10.20.236:35630 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	693 B / 663 B
DMZ1	tcp	10.10.20.236:35630 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	693 B / 663 B
WAN	tcp	10.10.20.236:35648 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	694 B / 663 B
DMZ1	tcp	10.10.20.236:35648 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	694 B / 663 B
WAN	tcp	10.10.20.236:35666 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	690 B / 663 B
DMZ1	tcp	10.10.20.236:35666 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	690 B / 663 B
WAN	tcp	10.10.20.236:35682 -> 192.168.2.20:25 (10.0.50.60:25)	FIN_WAIT_2:FIN_WAIT_2	6 / 6	692 B / 663 B
DMZ1	tcp	10.10.20.236:35682 -> 192.168.2.20:25	FIN_WAIT_2:FIN_WAIT_2	6 / 6	692 B / 663 B
</td>
</tr>
<tr>
<td>Time unknown on</td>
<td>Looks as if it is a shellcode attempt on FTP server</td>
<td>


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

Mail Server Report (Reporter: Stefan)

Time	Event	Description and evidence

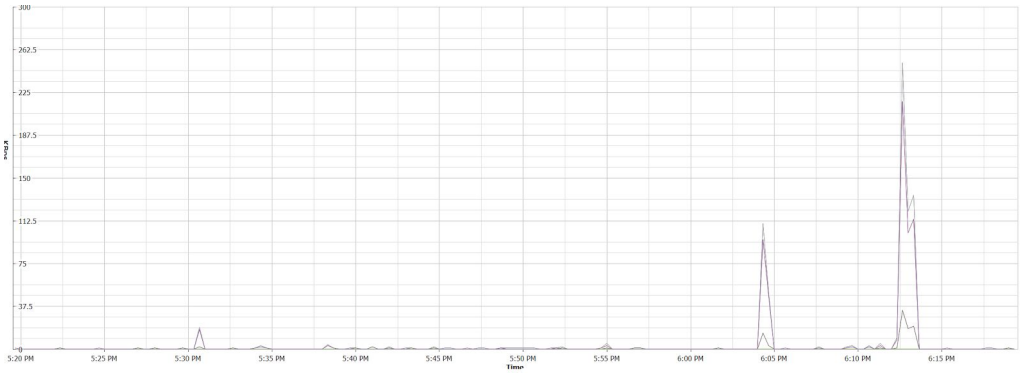
```
s.smith@mail:~$ cd mail/new/
s.smith@mail:~/mail/new$ ls
1490812508.Vfc01I13fdc1M533602.mail.cdc.pan
1490821688.Vfc01I13fdddM396237.mail.cdc.pan
1490821688.Vfc01I13fdfcM779568.mail.cdc.pan
1490821722.Vfc01I13fe01M392728.mail.cdc.pan
1490821722.Vfc01I13fe02M587412.mail.cdc.pan
1490825471.Vfc01I13fd3eM607100.mail.cdc.pan
s.smith@mail:~/mail/new$ cat 1490825471.Vfc01I13fd3eM607100.mail.cdc.pan
Return-Path: <s.smith@cdc.pan>
X-Original-To: s.smith@cdc.pan
Delivered-To: s.smith@cdc.pan
Received: from cdc.pan (unknown [10.10.20.236])
        by mail.pan (Postfix) with ESMTP id 89C1E13FD3C
        for <s.smith@cdc.pan>; Wed, 29 Mar 2017 17:11:11 -0500 (CDT)
Subject: Update required for pumps

Attention, there's an update you need to run to keep the pumps working efficient
ly. It's available at this address, just download it and run it and everything w
ill keep running smoothly. http://10.10.20.236/update.exe

Thanks,

Simon Smith, Intern
```

We noticed that the red team sent users a large number of malicious emails asking them to download an exe file. We were able to block this in our firewall.



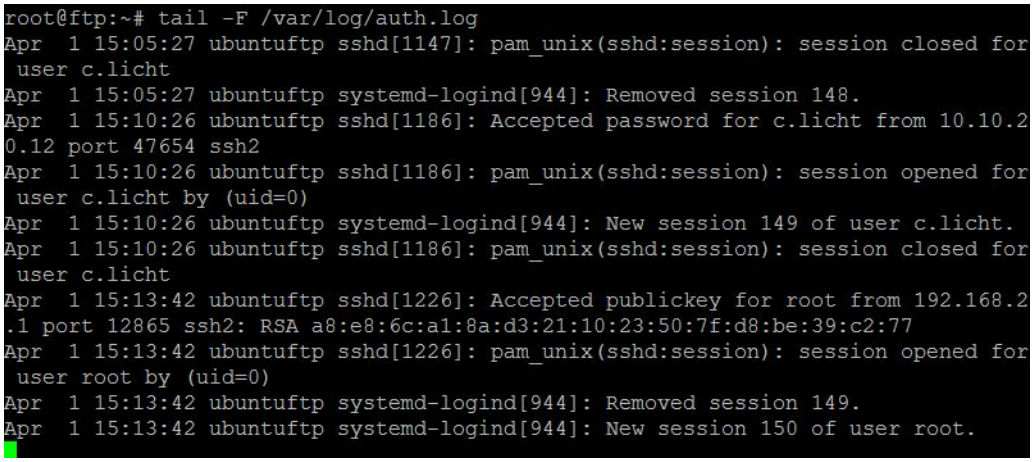
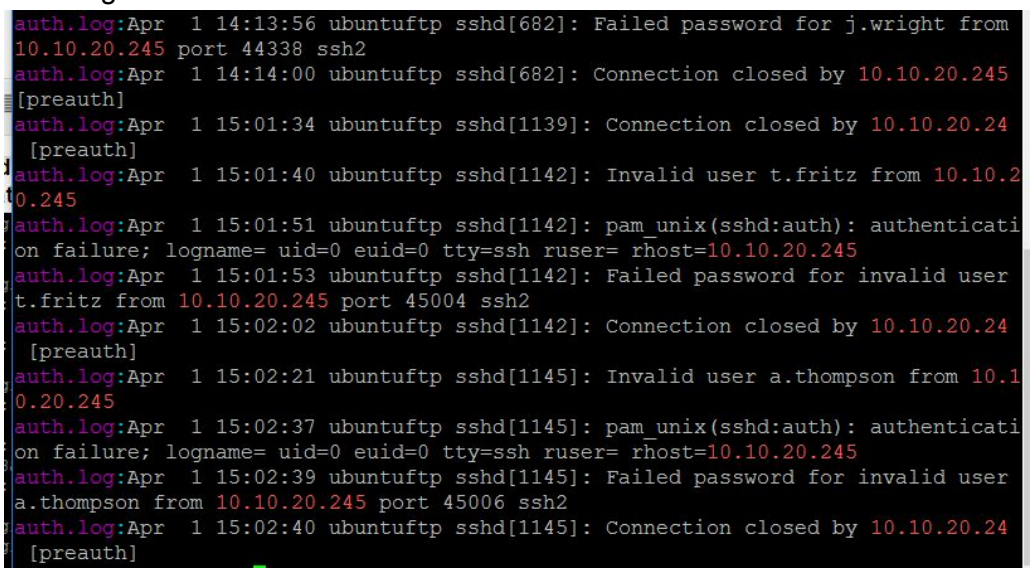
		5]: MAIL FROM:<s.smith@cdc.pan>\nRCPT TO:<p.emerson@cdc.pan>\ndata\nSubject: Update required for pumps\n\n Att Mar 29 17:53:55 mail postfix/smtpd[26699]: 52FF913FFAD: client=unknown[10.10.20.236] Mar 29 17:53:55 mail postfix/cleanup[26698]: 52FF913FFAD: message-id=<> Mar 29 17:53:55 mail postfix/qmgr[1311]: 52FF913FFAD: from=<s.smith@cdc.pan>, size=464, nrcpt=1 (queue act ive) Mar 29 17:53:55 mail postfix/local[26695]: 45D1113FFAC: to=<l.delrose@cdc.pan>, relay=local, delay=0.11, d elays=0.05/0/0/0.06, dsn=2.0.0, status=sent (delivered to maildir) Mar 29 17:53:55 mail postfix/smtpd[26699]: disconnect from unknown[10.10.20.236] ehlo=1 mail=1 rcpt=1 data =1 quit=1 commands=5 Mar 29 17:53:55 mail postfix/qmgr[1311]: 45D1113FFAC: removed Mar 29 17:53:55 mail postfix/smtpd[26699]: connect from unknown[10.10.20.236] Mar 29 17:53:55 mail postfix/smtpd[26699]: improper command pipelining after EHLO from unknown[10.10.20.23 6]: MAIL FROM:<s.smith@cdc.pan>\nRCPT TO:<p.luther@cdc.pan>\ndata\nSubject: Update required for pumps\n\nA tte Mar 29 17:53:55 mail postfix/smtpd[26699]: 6286413FFAE: client=unknown[10.10.20.236] Mar 29 17:53:55 mail postfix/cleanup[26698]: 6286413FFAE: message-id=<> Mar 29 17:53:55 mail postfix/local[26696]: 52FF913FFAD: to=<p.emerson@cdc.pan>, relay=local, delay=0.13, d elays=0.06/0/0/0.07, dsn=2.0.0, status=sent (delivered to maildir) Mar 29 17:53:55 mail postfix/qmgr[1311]: 52FF913FFAD: removed Mar 29 17:53:55 mail postfix/qmgr[1311]: 6286413FFAE: from=<s.smith@cdc.pan>, size=463, nrcpt=1 (queue act ive) Mar 29 17:53:55 mail postfix/smtpd[26699]: disconnect from unknown[10.10.20.236] ehlo=1 mail=1 rcpt=1 data =1 quit=1 commands=5 Mar 29 17:53:55 mail postfix/local[26695]: 6286413FFAE: to=<p.luther@cdc.pan>, relay=local, delay=0.11, de lays=0.08/0/0/0.03, dsn=2.0.0, status=sent (delivered to maildir) Mar 29 17:53:55 mail postfix/qmgr[1311]: 6286413FFAE: removed

AD Server Report (Reporter: Megan)

Time	Event	Description and evidence
15:49	Nothing to report	No irregular events were recorded in the active directory. Keywords | Date and Time | Source | Event ID | Task Category Audit Success | 8/18/2010 11:59:57 PM | Microsoft Windows security auditing. | 4634 | Logoff Audit Success | 8/18/2010 11:59:57 PM | Microsoft Windows security auditing. | 4624 | Logon Audit Success | 8/18/2010 11:59:57 PM | Microsoft Windows security auditing. | 4672 | Special Logon Audit Success | 8/18/2010 11:58:59 PM | Microsoft Windows security auditing. | 4663 | File System Audit Success | 8/18/2010 11:58:59 PM | Microsoft Windows security auditing. | 4663 | File System Audit Success | 8/18/2010 11:58:58 PM | Microsoft Windows security auditing. | 4634 | Logoff Audit Success | 8/18/2010 11:58:58 PM | Microsoft Windows security auditing. | 4624 | Logon Audit Success | 8/18/2010 11:58:58 PM | Microsoft Windows security auditing. | 4672 | Special Logon Audit Success | 8/18/2010 11:58:10 PM | Microsoft Windows security auditing. | 4624 | Logon Audit Success | 8/18/2010 11:58:10 PM | Microsoft Windows security auditing. | 4672 | Special Logon Audit Success | 8/18/2010 11:57:57 PM | Microsoft Windows security auditing. | 4634 | Logoff Audit Success | 8/18/2010 11:57:57 PM | Microsoft Windows security auditing. | 4624 | Logon

File Server Report (Reporter: Daniel)

Time	Event	Description and evidence
15:05 (GMT)	PAM generated logs from a new login source	We had a login over an odd SSH port: 47654. We have been using 22 and 22330 but not 47654. The user was c.licht. We will keep a close eye on this, but since there were no failed authentications with this user we believe the logins may be legitimate.

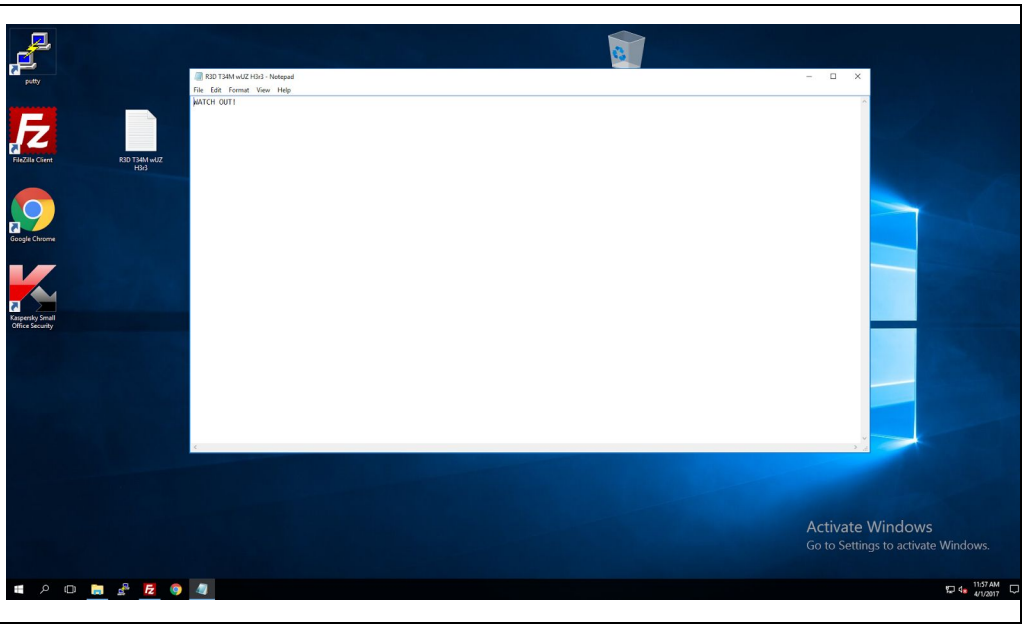
		
14:13 (GMT)	Login failures from different IP	I ran grep -ri “failure” in /var/log/ to find any generated logs that possibly correlated to a failed login. The command returned some failed login attempts from 10.10.20.245 which is an address that we do not normally use. Looking further into this, I grepped for the IP address in /var/logs and was returned with this image:  You can see that there are plenty of failed login attempts for multiple users. It is quite obvious that this IP address may have belonged to a red-teamer at one point.

DNS/NTP Server Report (Reporter: Daniel)

Time	Event	Description and evidence
3:50 (GMT)	Processes by root and system show normal activity thus far	Our DNS/NTP server had no failed login attempts since the last intrusion report. We have not seen a lot of activity on this server, other than through its' necessary processes. load averages: 0.08, 0.08, 0.08 dns.pangea 15:49:33 29 processes: 28 idle, 1 on processor up 14:19 CPU states: 0.0% user, 0.0% nice, 0.0% system, 0.0% interrupt, 100% idle Memory: Real: 47M/202M act/tot Free: 282M Cache: 97M Swap: 0K/81M PID USERNAME PRI NICE SIZE RES STATE WAIT TIME CPU COMMAND 68909 _dnscryp 2 0 776K 1512K sleep kqread 0:12 0.00% dnscrypt-pr 46225 _bind 18 0 26M 28M idle sigwait 0:12 0.00% named 46844 _pflogd 4 0 692K 456K sleep bpf 0:02 0.00% pflogd 1 root 10 0 444K 528K idle wait 0:01 0.00% init 47122 _ntp 2 -20 736K 1748K sleep poll 0:00 0.00% ntpd 82839 root 2 0 704K 1208K idle poll 0:00 0.00% cron 83879 _syslogd 2 0 1088K 1552K idle kqread 0:00 0.00% syslogd 46169 root 2 0 3608K 3408K sleep select 0:00 0.00% sshd 45904 root 10 0 1420K 2724K sleep wait 0:00 0.00% bash 12025 _smtpq 2 0 1576K 3760K idle kqread 0:00 0.00% smtpd 17329 root 2 0 940K 1460K idle select 0:00 0.00% sshd 73503 _smtpd 2 0 1492K 3756K idle kqread 0:00 0.00% smtpd 66988 _smtpd 2 0 1368K 3592K idle kqread 0:00 0.00% smtpd 41542 _smtpd 2 0 1572K 3816K idle kqread 0:00 0.00% smtpd 18101 _smtpd 2 0 1356K 3540K idle kqread 0:00 0.00% smtpd 77640 _smtpd 2 0 1444K 3644K idle kqread 0:00 0.00% smtpd 27909 root 28 0 772K 2132K onproc - 0:00 0.00% top 58787 root 2 0 1624K 2184K idle kqread 0:00 0.00% smtpd

RDP Server Report (Reporter: Logan)

Time	Event	Description and evidence
13:57pm	Checked the event viewer security audit tab in Windows for RDP	We found a text file indicating the presence of red team. However our logs indicated no remote network access aside from the current RDP session so we believe this was direct access by Red team when green team left a machine unattended.

Mitigation: At this time (2:08pm) we are monitoring the situation closely, as we believe it may have been an attempt by Red team to get us to change a password in a public setting. At 2:10 we noticed a user running notepad.exe, which is not typical of a green team user we have seen so far and could have been used by the alleged-malicious user to leave the text file. After shoulder surfing the green team user in person and passively observing them we found they were running notepad.exe and running green team checks. At this time we believe the activity may have been because of a “ambitious green team user”. At 2:25pm, we increased our security policy on the RDP box by restricting user access to a strict set of whitelisted programs required to perform green team checks. After adding whitelisting rules to RDP we observed no further malicious (or playful green team) activity.

At no point during the competition did any red team member successfully enter into the remote desktop environment remotely. In fact, the only non-standard contact we received was from network scanners which did not yield access. Overall, the use of an RDP server provided a secure environment for green team access.

WWW Server Report (Reporter: Megan)

Time	Event	Description and evidence
15:03	Web Server taken down for maintenance.	Our web server had to be taken down temporarily for maintenance, which only took three to five minutes. When we put the web server back up we couldn’t find any evidence of unusual or malicious activities.
15:37	Web Server	The service status showed that our web server was down when it actually

	HTTP said to be down	wasn't. After talking with the white team they agreed to give us back our points.

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.