The People’s Government of Pangea

Department of Information Technology

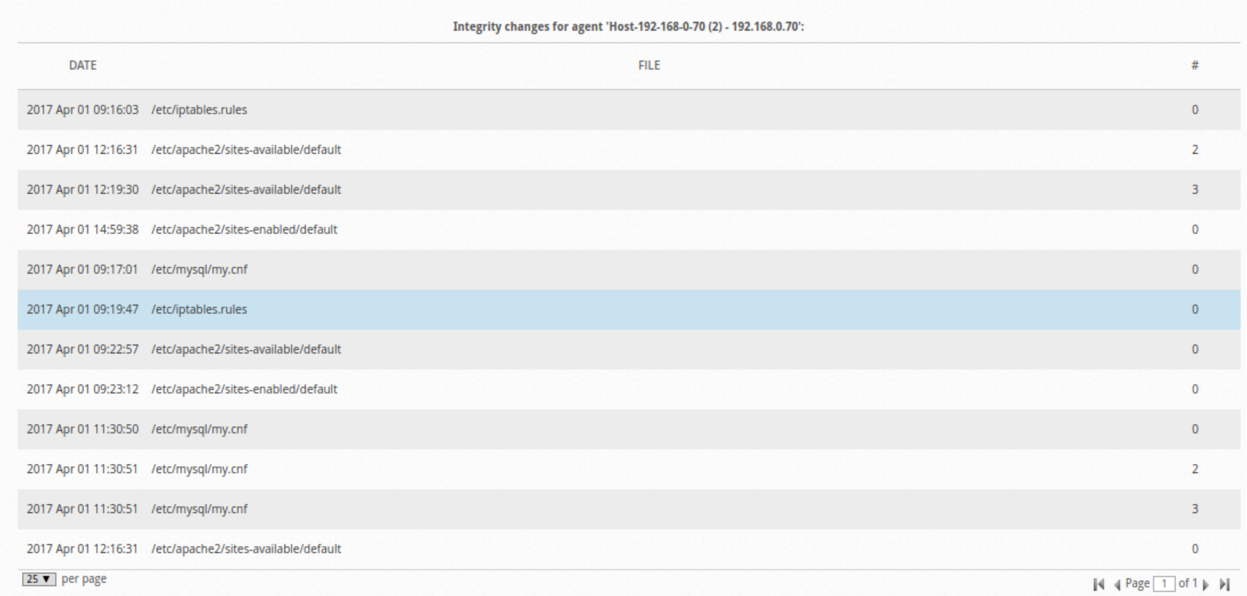
Cyber Operations Team 15 (Wright State University)

Intrusion Report

At 2:18pm, the Apache logs showed that the water system had been shut off by the t.fritz account. As one of our Green Team members recently came over to ask about the HMI accounts, we believe that she logged in and turned off the water to test the system. We simply turned the water back on and as of 2:32pm, the system has not been turned off again. She also drew our attention to the fact that the j.wright account did not have access to the HMI, and we learned that we had mistyped the password while we were resetting it – j.wright should have access again.

At 2:45pm, the Green Team tested the water system using the j.wright account, and the water system was briefly powered off.

We have been running OSSIM throughout the day, monitoring the web and AD servers, and we did not detect changes on either of those. We have services monitoring for file and registry changes on both, and the only changes to files correspond to changes we have made on the web server (enabling MySQL logging, adding iptables rules, and forcing files to download from Drupal):

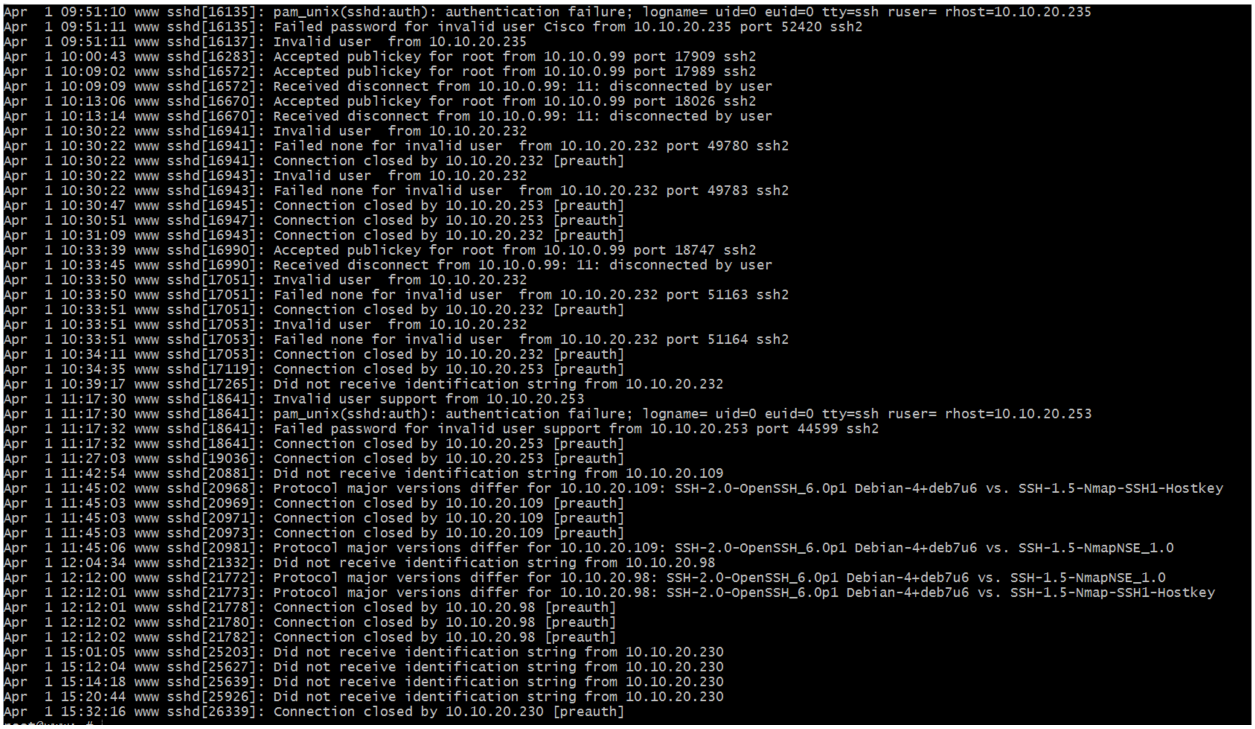


Integrity changes for agent 'Host-192-168-0-70 (2) - 192.168.0.70':

DATE	FILE	#
2017 Apr 01 09:16:03	/etc/iptables.rules	0
2017 Apr 01 12:16:31	/etc/apache2/sites-available/default	2
2017 Apr 01 12:19:30	/etc/apache2/sites-available/default	3
2017 Apr 01 14:59:38	/etc/apache2/sites-enabled/default	0
2017 Apr 01 09:17:01	/etc/mysql/my.cnf	0
2017 Apr 01 09:19:47	/etc/iptables.rules	0
2017 Apr 01 09:22:57	/etc/apache2/sites-available/default	0
2017 Apr 01 09:23:12	/etc/apache2/sites-enabled/default	0
2017 Apr 01 11:30:50	/etc/mysql/my.cnf	0
2017 Apr 01 11:30:51	/etc/mysql/my.cnf	2
2017 Apr 01 11:30:51	/etc/mysql/my.cnf	3
2017 Apr 01 12:16:31	/etc/apache2/sites-available/default	0

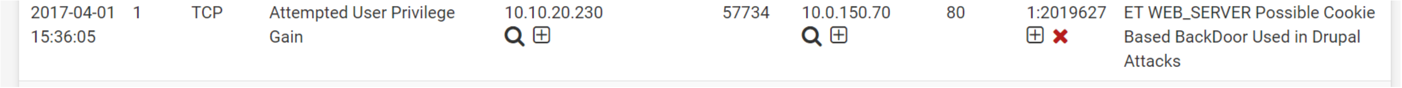
Starting at around 3:00pm, we were starting to get requests for SSH access from multiple IP addresses. To be safe, we went ahead and blocked the IP address 10.10.20.253 temporarily.

Looking at /var/log/auth.log, we could see that the connections got closed by the system because authentication failed for root. Knowing that we require RSA keys for authentication to root, we went ahead and re-allowed the connections, feeling safe that their bruteforce attempts would fail:

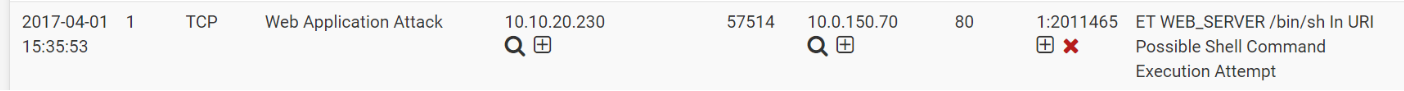


```
Apr  1 09:51:10 www sshd[16135]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.20.235
Apr  1 09:51:11 www sshd[16135]: Failed password for invalid user Cisco from 10.10.20.235 port 52420 ssh2
Apr  1 09:51:11 www sshd[16137]: Invalid user  from 10.10.20.235
Apr  1 10:00:43 www sshd[16283]: Accepted publickey for root from 10.10.0.99 port 17909 ssh2
Apr  1 10:09:02 www sshd[16572]: Accepted publickey for root from 10.10.0.99 port 17989 ssh2
Apr  1 10:09:09 www sshd[16572]: Received disconnect from 10.10.0.99: 11: disconnected by user
Apr  1 10:13:06 www sshd[16670]: Accepted publickey for root from 10.10.0.99 port 18026 ssh2
Apr  1 10:13:14 www sshd[16670]: Received disconnect from 10.10.0.99: 11: disconnected by user
Apr  1 10:30:22 www sshd[16941]: Invalid user  from 10.10.20.232
Apr  1 10:30:22 www sshd[16941]: Failed none for invalid user  from 10.10.20.232 port 49780 ssh2
Apr  1 10:30:22 www sshd[16941]: Connection closed by 10.10.20.232 [preauth]
Apr  1 10:30:22 www sshd[16943]: Invalid user  from 10.10.20.232
Apr  1 10:30:22 www sshd[16943]: Failed none for invalid user  from 10.10.20.232 port 49783 ssh2
Apr  1 10:30:47 www sshd[16945]: Connection closed by 10.10.20.253 [preauth]
Apr  1 10:30:51 www sshd[16947]: Connection closed by 10.10.20.253 [preauth]
Apr  1 10:31:09 www sshd[16943]: Connection closed by 10.10.20.232 [preauth]
Apr  1 10:33:39 www sshd[16990]: Accepted publickey for root from 10.10.0.99 port 18747 ssh2
Apr  1 10:33:45 www sshd[16990]: Received disconnect from 10.10.0.99: 11: disconnected by user
Apr  1 10:33:50 www sshd[17051]: Invalid user  from 10.10.20.232
Apr  1 10:33:50 www sshd[17051]: Failed none for invalid user  from 10.10.20.232 port 51163 ssh2
Apr  1 10:33:51 www sshd[17051]: Connection closed by 10.10.20.232 [preauth]
Apr  1 10:33:51 www sshd[17053]: Invalid user  from 10.10.20.232
Apr  1 10:33:51 www sshd[17053]: Failed none for invalid user  from 10.10.20.232 port 51164 ssh2
Apr  1 10:34:11 www sshd[17053]: Connection closed by 10.10.20.232 [preauth]
Apr  1 10:34:35 www sshd[17119]: Connection closed by 10.10.20.253 [preauth]
Apr  1 10:39:17 www sshd[17265]: Did not receive identification string from 10.10.20.232
Apr  1 11:17:30 www sshd[18641]: Invalid user support from 10.10.20.253
Apr  1 11:17:30 www sshd[18641]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.20.253
Apr  1 11:17:32 www sshd[18641]: Failed password for invalid user support from 10.10.20.253 port 44599 ssh2
Apr  1 11:17:32 www sshd[18641]: Connection closed by 10.10.20.253 [preauth]
Apr  1 11:27:03 www sshd[19036]: Connection closed by 10.10.20.253 [preauth]
Apr  1 11:42:54 www sshd[20881]: Did not receive identification string from 10.10.20.109
Apr  1 11:45:02 www sshd[20968]: Protocol major versions differ for 10.10.20.109: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6 vs. SSH-1.5-Nmap-SSH1-Hostkey
Apr  1 11:45:03 www sshd[20969]: Connection closed by 10.10.20.109 [preauth]
Apr  1 11:45:03 www sshd[20971]: Connection closed by 10.10.20.109 [preauth]
Apr  1 11:45:03 www sshd[20973]: Connection closed by 10.10.20.109 [preauth]
Apr  1 11:45:06 www sshd[20981]: Protocol major versions differ for 10.10.20.109: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6 vs. SSH-1.5-NmapNSE_1.0
Apr  1 12:04:34 www sshd[21332]: Did not receive identification string from 10.10.20.98
Apr  1 12:12:00 www sshd[21772]: Protocol major versions differ for 10.10.20.98: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6 vs. SSH-1.5-NmapNSE_1.0
Apr  1 12:12:01 www sshd[21773]: Protocol major versions differ for 10.10.20.98: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6 vs. SSH-1.5-Nmap-SSH1-Hostkey
Apr  1 12:12:01 www sshd[21778]: Connection closed by 10.10.20.98 [preauth]
Apr  1 12:12:02 www sshd[21780]: Connection closed by 10.10.20.98 [preauth]
Apr  1 12:12:02 www sshd[21782]: Connection closed by 10.10.20.98 [preauth]
Apr  1 15:01:05 www sshd[25203]: Did not receive identification string from 10.10.20.230
Apr  1 15:12:04 www sshd[25627]: Did not receive identification string from 10.10.20.230
Apr  1 15:14:18 www sshd[25639]: Did not receive identification string from 10.10.20.230
Apr  1 15:20:44 www sshd[25926]: Did not receive identification string from 10.10.20.230
Apr  1 15:32:16 www sshd[26339]: Connection closed by 10.10.20.230 [preauth]
```

We had 10.10.20.230 attempt to use a possible Drupal backdoor, and we noticed that there was an attempt to get a shell using a URL, but nothing seems to have come of it:



2017-04-01 15:36:05	1	TCP	Attempted User Privilege Gain	10.10.20.230 🔍 ⊞	57734	10.0.150.70 🔍 ⊞	80	1:2019627 ⊞ ✖	ET WEB_SERVER Possible Cookie Based BackDoor Used in Drupal Attacks



2017-04-01 15:35:53	1	TCP	Web Application Attack	10.10.20.230 🔍 ⊞	57514	10.0.150.70 🔍 ⊞	80	1:2011465 ⊞ ✖	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt

At the end, user credentials were leaked and we changed the passwords for the two users that had access, and our HMI was not compromised as of 3:56pm.