The People's G overnment of P angea

Department of Information Technology

Cyber Operations Team 15 (Wright State University)

Intrusion Report

Our HMI went out at 10:04 am. The time was incorrect, but the login was from h.peterson (following log excerpt is from /var/log/apache2/access.log:

```
10.10.20.215 - h.peterson [01/Apr/2017:15:03:11 +0000] "GET /water
HTTP/1.1" 200 2047 "https://10.0.150.50/?ajax_request=" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - h.peterson [01/Apr/2017:15:03:13 +0000] "GET
/water/woff HTTP/1.1" 200 1964 "https://10.0.150.50/water"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - h.peterson [01/Apr/2017:15:03:19 +0000] "GET /power
HTTP/1.1" 200 2047 "https://10.0.150.50/water/woff" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - h.peterson [01/Apr/2017:15:03:20 +0000] "GET
/power/poff HTTP/1.1" 200 1963 "https://10.0.150.50/power"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - h.peterson [01/Apr/2017:15:03:22 +0000] "GET
/killswitch HTTP/1.1" 200 1964 "https://10.0.150.50/power/poff"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - h.peterson [01/Apr/2017:15:03:25 +0000] "GET
/killswitch/on HTTP/1.1" 200 2093 "https://10.0.150.50/killswitch"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/57.0.2987.133 Safari/537.36"
10.10.20.215 - - [01/Apr/2017:15:03:28 +0000] "GET /status HTTP/1.1"
200 1936 "https://10.0.150.50/killswitch/on" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36"
```

(from /var/log/apache2/access_log)

Most of the attacks seem to be coming from the IP addresses 10.10.20.232, 10.10.20.235, and 10.10.20.253, so this could have easily been a legitimate access attempt from Holly Peterson herself. We will be monitoring for further attempts, however.

Our HMI went down again at 10:18. Checking the access logs, it appears that h.peterson is responsible for the failure. After two more attempts to turn off the HMI, we talked to Holly and confirmed that she was the one accessing the HMI, and luckily not an attacker that compromised her credentials. We will be reworking the authentication on the HMI and removing Holly's access.

We have modified the HMI so that only Jane Wright and Ted Fritz have access as pump technicians to the water switch. If anyone else needs access, they may request it through the help desk.

As of 10:50am, the web server continues to be attacked heavily, but there are no signs of compromise yet. Checking through the output of 'ps' for a list of shells only shows shells that can be verified to be running from our own SSH sessions:

```
[root@mail ~]# w
 10:54:24 up 51 min,  2 users,  load average: 0.16, 0.03, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    10.0.150.101     10:12   41.00s  0.13s  0.13s -bash
root     pts/1    10.0.150.102     10:12    0.00s  0.06s  0.00s w
[root@mail ~]# ps ax | grep sh
  357 ?        S      0:00 [kdmflush]
  359 ?        S      0:00 [kdmflush]
 1000 ?        S      0:00 [flush-253:0]
 1241 ?        Ss     0:00 /usr/sbin/sshd
 1459 ?        Ss     0:00 sshd: root@pts/0
 1462 pts/0    Ss+    0:00 -bash
 1482 ?        Ss     0:00 sshd: root@pts/1
 1485 pts/1    Ss     0:00 -bash
 1774 pts/1    S+     0:00 grep sh
[root@mail ~]#
```

Snort is regularly detecting exploits for CVE-2013-0156 and directory traversal on the website, and there was a set of attempts at a Ruby on Rails exploit (CVE-2013-0156). Starting at 11:16, there were several attempts at SQL injection attacks:

2017-04-01 11:16:08	1	TCP	Web Application Attack	10.10.20.235	53986	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:08	1	TCP	Web Application Attack	10.10.20.235	53984	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:08	1	TCP	Web Application Attack	10.10.20.235	53985	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:08	1	TCP	Web Application Attack	10.10.20.235	53983	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:07	1	TCP	Web Application Attack	10.10.20.235	53981	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:07	1	TCP	Web Application Attack	10.10.20.235	53979	10.0.150.70	80	1:2016935	ET WEB_SERVER SQL Injection Select Sleep Time Delay
2017-04-01 11:16:04	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	35321	10.0.150.70	80	1:2024121	ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)

We have been monitoring SQL queries and network connections on the web server. So far, we have not seen any SQL injection attempts make it through to the backend MySQL server.

Red team has been periodically creating new accounts on the website, and we have been deleting them. We found the configuration option in Drupal to disable account registration without administrator approval and have turned it on. They have since made three users, and they were all blocked by default:

Hank	blocked	33 min 20 sec	never	edit
user14	blocked	36 min 3 sec	never	edit
user13	blocked	36 min 51 sec	never	edit

At 11:48, Jane Wright turned off the water pump, but immediately turned it back on, so she was likely just testing her access.

We are also starting to see as of 11:45 network scan activity from 10.10.20.109:

2017-04-01 11:44:45	2	UDP	Attempted Information Leak	10.10.20.109	48190	10.0.150.70	39672	1:2018489	ET SCAN NMAP OS Detection Probe
2017-04-01 11:44:45	1	UDP	Executable Code was Detected	10.10.20.109	48190	10.0.150.70	39672	1:2101390	GPL SHELLCODE x86 inc ebx NOOP
2017-04-01 11:44:45	2	UDP	Attempted Information Leak	10.10.20.109	48190	10.0.150.70	39672	1:2018489	ET SCAN NMAP OS Detection Probe
2017-04-01 11:44:45	1	UDP	Executable Code was Detected	10.10.20.109	48190	10.0.150.70	39672	1:2101390	GPL SHELLCODE x86 inc ebx NOOP
2017-04-01 11:44:45	2	TCP	Attempted Information Leak	10.10.20.109	48130	10.0.150.70	22	1:2001219	ET SCAN Potential SSH Scan