

CONFIDENTIAL

Intrusion Report for CDC

Iowa State University

VERSION 2:00PM

# Table of Contents

|   |          |
|---|----------|
| <b>Executive Summary</b>                      | <b>3</b> |
| <b>Server Reporting</b>                       | <b>3</b> |
| Firewall Server Report (Reporter: Stefan)     | 3        |
| Mail Server Report (Reporter: Stefan)         | 3        |
| AD Server Report (Reporter: Megan)            | 4        |
| File Server Report (Reporter: Daniel)         | 4        |
| DNS/NTP Server Report (Reporter: Daniel)      | 5        |
| RDP Server Report (Reporter: Logan)           | 6        |
| WWW Server Report (Reporter: Megan)           | 7        |
| <b>Mitigations and Countermeasures</b>        | <b>7</b> |
| RDP Server Protections                        | 7        |
| Mail Server Protections                       | 7        |
| Green Team Host Machine Protections           | 7        |
| <b>Yahoo Leak Response</b>                    | <b>8</b> |
| <b>Social Engineering/Intelligence Report</b> | <b>8</b> |

## 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  |                        |                        |                        |                        |             |            |  |  |  |  |  |  |  |  |  |  |  |                                  |  |                                  |
|---|------------------------|---|------------------------|------------------------|------------------------|------------------------|-------------|------------|--|--|--|--|--|--|--|--|--|--|--|----------------------------------|--|----------------------------------|
| 12:07   | Web application attack | <b>We observed the red team attempt to use Nmap to discover vulnerabilities in our servers, but the attempts were blocked by our firewall.</b>  |                        |                        |                        |                        |             |            |  |  |  |  |  |  |  |  |  |  |  |                                  |  |                                  |
|   |                        | <table><tr><td>2017-04-01 12:07:47</td><td>1</td><td>TCP</td><td>Web Application Attack</td><td>10.10.20.98</td><td>36338</td><td>10.0.50.60</td><td>80</td><td>1:2009358</td><td>ET SCAN Nmap Scripting Engine User-Agent</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Detected (Nmap Scripting Engine)</td></tr></table> | 2017-04-01 12:07:47    | 1                      | TCP                    | Web Application Attack | 10.10.20.98 | 36338      | 10.0.50.60                               | 80                                       | 1:2009358                                | ET SCAN Nmap Scripting Engine User-Agent |  |  |  |  |  |  |  |                                  |  | Detected (Nmap Scripting Engine) |
|   |                        | 2017-04-01 12:07:47   | 1                      | TCP                    | Web Application Attack | 10.10.20.98            | 36338       | 10.0.50.60 | 80                                       | 1:2009358                                | ET SCAN Nmap Scripting Engine User-Agent |  |  |  |  |  |  |  |  |                                  |  |                                  |
|   |                        |   |                        |                        |                        |                        |             |            | Detected (Nmap Scripting Engine)         |  |  |  |  |  |  |  |  |  |  |                                  |  |                                  |
| <table><tr><td>2017-04-01 12:07:47</td><td>1</td><td>TCP</td><td>Web Application Attack</td><td>10.10.20.98</td><td>36332</td><td>10.0.50.60</td><td>80</td><td>1:2009358</td><td>ET SCAN Nmap Scripting Engine User-Agent</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Detected (Nmap Scripting Engine)</td></tr></table> | 2017-04-01 12:07:47    | 1   | TCP                    | Web Application Attack | 10.10.20.98            | 36332                  | 10.0.50.60  | 80         | 1:2009358                                | ET SCAN Nmap Scripting Engine User-Agent |  |  |  |  |  |  |  |  |  | Detected (Nmap Scripting Engine) |  |                                  |
| 2017-04-01 12:07:47   | 1                      | TCP   | Web Application Attack | 10.10.20.98            | 36332                  | 10.0.50.60             | 80          | 1:2009358  | ET SCAN Nmap Scripting Engine User-Agent |  |  |  |  |  |  |  |  |  |  |                                  |  |                                  |
|   |                        |   |                        |                        |                        |                        |             |            | Detected (Nmap Scripting Engine)         |  |  |  |  |  |  |  |  |  |  |                                  |  |                                  |

### Mail Server Report (Reporter: Stefan)

| Time | Event | Description and evidence   |
|------|-------|--|
|      |       | <p><b>Nothing to report</b></p> <p>We did not notice any malicious activity since the last intrusion report. To better identify any potential malicious actions, we installed Tripwire to notify us if any important system files are changed.</p> |

## AD Server Report (Reporter: Megan)

| Time           | Event   | Description and evidence   |
|----------------|---|--|
| <b>1:20 pm</b> | One of the user accounts was compromised via a password leak (by Yahoo! Services a.k.a. White team) | We temporarily disabled the account and changed the password. The account was re-enabled once the password was successfully updated. We look at the auth.log files and the compromised user was not used to log into any services. |

## File Server Report (Reporter: Daniel)

| Time               | Event                         | Description and evidence   |
|--------------------|-------------------------------|--|
| <b>12:01 (GMT)</b> | <b>C.licht user is "busy"</b> | <b>In auth.log, we spotted multiple successful attempts to login as user c.licht. This is likely green team, however we report it here because we plan on keeping a close watch on this user and all their activity.</b> |

|  |  |   |
|--|--|---|
|  |  | <pre> Apr 1 12:00:33 ubuntuftp systemd-logind[944]: Removed session 106. Apr 1 12:00:34 ubuntuftp systemd-logind[944]: New session 107 of user c.light. Apr 1 12:00:34 ubuntuftp sshd[31366]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:03:09 ubuntuftp sshd[29577]: Received disconnect from 192.168.2.1: 11: disconnected by user Apr 1 12:03:09 ubuntuftp sshd[29577]: pam_unix(sshd:session): session closed for user root Apr 1 12:03:09 ubuntuftp systemd-logind[944]: Removed session 107. Apr 1 12:03:10 ubuntuftp systemd-logind[944]: Removed session 73. Apr 1 12:05:36 ubuntuftp sshd[31407]: Accepted password for c.light from 10.10.20.12 port 51765 ssh2 Apr 1 12:05:36 ubuntuftp sshd[31407]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:05:36 ubuntuftp systemd-logind[944]: New session 108 of user c.light. Apr 1 12:05:36 ubuntuftp sshd[31407]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:10:37 ubuntuftp sshd[31498]: Accepted password for c.light from 10.10.20.12 port 38799 ssh2 Apr 1 12:10:37 ubuntuftp sshd[31498]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:10:37 ubuntuftp systemd-logind[944]: Removed session 108. Apr 1 12:10:38 ubuntuftp systemd-logind[944]: New session 109 of user c.light. Apr 1 12:10:38 ubuntuftp sshd[31498]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:15:34 ubuntuftp sshd[31543]: Accepted password for c.light from 10.10.20.12 port 57974 ssh2 Apr 1 12:15:34 ubuntuftp sshd[31543]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:15:34 ubuntuftp systemd-logind[944]: Removed session 109. Apr 1 12:15:35 ubuntuftp systemd-logind[944]: New session 110 of user c.light. Apr 1 12:15:35 ubuntuftp sshd[31580]: fatal: Write failed: Connection reset by peer Apr 1 12:15:35 ubuntuftp sshd[31543]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:15:35 ubuntuftp systemd-logind[944]: Removed session 110. Apr 1 12:17:01 ubuntuftp CRON[31583]: PAM unable to dlopen(pam_ldap.so): /lib/security/pam_ldap.so: cannot Apr 1 12:17:01 ubuntuftp CRON[31583]: PAM adding faulty module: pam_ldap.so Apr 1 12:17:01 ubuntuftp CRON[31583]: pam_unix(cron:session): session opened for user root by (uid=0) Apr 1 12:17:01 ubuntuftp CRON[31583]: pam_unix(cron:session): session closed for user root Apr 1 12:20:34 ubuntuftp sshd[31587]: Accepted password for c.light from 10.10.20.12 port 47853 ssh2 Apr 1 12:20:34 ubuntuftp sshd[31587]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:20:34 ubuntuftp systemd-logind[944]: New session 111 of user c.light. Apr 1 12:20:34 ubuntuftp sshd[31587]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:25:35 ubuntuftp sshd[31626]: Accepted password for c.light from 10.10.20.12 port 36885 ssh2 Apr 1 12:25:35 ubuntuftp sshd[31626]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:25:35 ubuntuftp systemd-logind[944]: Removed session 111. Apr 1 12:25:36 ubuntuftp systemd-logind[944]: New session 112 of user c.light. Apr 1 12:25:36 ubuntuftp sshd[31626]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:30:35 ubuntuftp sshd[31670]: Accepted password for c.light from 10.10.20.12 port 53023 ssh2 Apr 1 12:30:35 ubuntuftp sshd[31670]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:30:35 ubuntuftp systemd-logind[944]: Removed session 112. Apr 1 12:30:36 ubuntuftp systemd-logind[944]: New session 113 of user c.light. Apr 1 12:30:36 ubuntuftp sshd[31670]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:35:35 ubuntuftp sshd[31709]: Accepted password for c.light from 10.10.20.12 port 40165 ssh2 Apr 1 12:35:35 ubuntuftp sshd[31709]: pam_unix(sshd:session): session opened for user c.light by (uid=0) Apr 1 12:35:35 ubuntuftp systemd-logind[944]: Removed session 113. Apr 1 12:35:36 ubuntuftp systemd-logind[944]: New session 114 of user c.light. Apr 1 12:35:36 ubuntuftp sshd[31709]: pam_unix(sshd:session): session closed for user c.light Apr 1 12:36:31 ubuntuftp sshd[31749]: Accepted publickey for root from 192.168.2.1 port 48887 ssh2: RSA e Apr 1 12:36:31 ubuntuftp sshd[31749]: pam_unix(sshd:session): session opened for user root by (uid=0) Apr 1 12:36:31 ubuntuftp systemd-logind[944]: Removed session 114. </pre> |
|--|--|---|

## DNS/NTP Server Report (Reporter: Daniel)

| Time           | Event                           | Description and evidence   |
|----------------|---------------------------------|--|
| 12:45<br>(GMT) | DNS/NTP<br>showing<br>cert logs | The DNS/NTP server was unable to retrieve certificates for a while. We believe this is intrusion-report-worthy because we want all of our clients to be safe with encrypted traffic. |

|  |  |   |
|--|--|---|
|  |  | <pre> Apr 1 06:41:11 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 06:45:17 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 06:45:32 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 06:49:41 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 06:49:56 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 06:54:08 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 06:54:23 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 06:58:38 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 06:58:53 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:03:11 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:03:26 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:07:47 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:08:02 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:12:26 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:12:41 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:17:08 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:17:23 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:21:53 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:22:08 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:26:41 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:26:56 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:31:32 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:31:48 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:36:27 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:36:42 dns dnscrypt-proxy[68909]: Unable to retrieve server certificates Apr 1 07:41:24 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 07:41:24 dns dnscrypt-proxy[68909]: Server certificate #808464433 received Apr 1 07:41:24 dns dnscrypt-proxy[68909]: This certificate is valid Apr 1 07:41:24 dns dnscrypt-proxy[68909]: Chosen certificate #808464433 is valid from Apr 1 07:41:24 dns dnscrypt-proxy[68909]: Server key fingerprint is CB51:0B61:7A1F:FCEB Apr 1 08:42:09 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 08:42:09 dns dnscrypt-proxy[68909]: Server certificate #808464433 received Apr 1 08:42:09 dns dnscrypt-proxy[68909]: This certificate is valid Apr 1 08:42:09 dns dnscrypt-proxy[68909]: Chosen certificate #808464433 is valid from Apr 1 08:42:09 dns dnscrypt-proxy[68909]: Server key fingerprint is CB51:0B61:7A1F:FCEB Apr 1 09:43:28 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 09:43:28 dns dnscrypt-proxy[68909]: Server certificate #808464433 received Apr 1 09:43:28 dns dnscrypt-proxy[68909]: This certificate is valid Apr 1 09:43:28 dns dnscrypt-proxy[68909]: Chosen certificate #808464433 is valid from Apr 1 09:43:28 dns dnscrypt-proxy[68909]: Server key fingerprint is CB51:0B61:7A1F:FCEB Apr 1 10:43:54 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 10:43:54 dns dnscrypt-proxy[68909]: Server certificate #808464433 received Apr 1 10:43:54 dns dnscrypt-proxy[68909]: This certificate is valid Apr 1 10:43:54 dns dnscrypt-proxy[68909]: Chosen certificate #808464433 is valid from Apr 1 10:43:54 dns dnscrypt-proxy[68909]: Server key fingerprint is CB51:0B61:7A1F:FCEB Apr 1 11:44:29 dns dnscrypt-proxy[68909]: Refetching server certificates Apr 1 11:44:29 dns dnscrypt-proxy[68909]: Server certificate #808464433 received Apr 1 11:44:29 dns dnscrypt-proxy[68909]: This certificate is valid Apr 1 11:44:29 dns dnscrypt-proxy[68909]: Chosen certificate #808464433 is valid from </pre> |
|--|--|---|










## RDP Server Report (Reporter: Logan)

| Time | Event                   | Description and evidence  |
|------|-------------------------|---|
|      | Security Migrations for | As an added security measure we installed Kaspersky antivirus on the Remote Desktop service. See the Migrations section below for more details. |



|  |                 |  |
|--|-----------------|--|
|  | anti-keylogging |  |
|--|-----------------|--|

## WWW Server Report (Reporter: Megan)

| Time  | Event  | Description and evidence   |                 |                     |                      |            |             |            |   |         |  |                |                    |                      |   |         |  |                 |                    |                      |   |         |  |                 |                     |                      |
|---|--|--|-----------------|---------------------|----------------------|------------|-------------|------------|---|---------|--|----------------|--------------------|----------------------|---|---------|--|-----------------|--------------------|----------------------|---|---------|--|-----------------|---------------------|----------------------|
| 12:55   | Malicious activity has halted on the Drupal web site. We have not found evidence of malicious activity in the Docker image or web host. We believe the previous (noon intrusion report) mitigation of disabling malicious users and was successful because there has been no malicious activity since deleting the newly added user account. | <table><tr><th>USERNAME</th><th>STATUS</th><th>ROLES</th><th>MEMBER FOR</th><th>LAST ACCESS</th><th>OPERATIONS</th></tr><tr><td> administrator</td><td>blocked</td><td></td><td>2 hours 28 min</td><td>2 hours 22 min ago</td><td><a href="#">edit</a></td></tr><tr><td> admin</td><td>blocked</td><td></td><td>2 days 21 hours</td><td>2 hours 41 min ago</td><td><a href="#">edit</a></td></tr><tr><td> chisley</td><td>blocked</td><td></td><td>2 days 22 hours</td><td>2 days 21 hours ago</td><td><a href="#">edit</a></td></tr></table> | USERNAME        | STATUS              | ROLES                | MEMBER FOR | LAST ACCESS | OPERATIONS |  administrator | blocked |  | 2 hours 28 min | 2 hours 22 min ago | <a href="#">edit</a> |  admin | blocked |  | 2 days 21 hours | 2 hours 41 min ago | <a href="#">edit</a> |  chisley | blocked |  | 2 days 22 hours | 2 days 21 hours ago | <a href="#">edit</a> |
| USERNAME  | STATUS   | ROLES  | MEMBER FOR      | LAST ACCESS         | OPERATIONS           |            |             |            |   |         |  |                |                    |                      |   |         |  |                 |                    |                      |   |         |  |                 |                     |                      |
|  administrator | blocked  |  | 2 hours 28 min  | 2 hours 22 min ago  | <a href="#">edit</a> |            |             |            |   |         |  |                |                    |                      |   |         |  |                 |                    |                      |   |         |  |                 |                     |                      |
|  admin         | blocked  |  | 2 days 21 hours | 2 hours 41 min ago  | <a href="#">edit</a> |            |             |            |   |         |  |                |                    |                      |   |         |  |                 |                    |                      |   |         |  |                 |                     |                      |
|  chisley       | blocked  |  | 2 days 22 hours | 2 days 21 hours ago | <a href="#">edit</a> |            |             |            |   |         |  |                |                    |                      |   |         |  |                 |                    |                      |   |         |  |                 |                     |                      |

## Mitigations and Countermeasures

### RDP Server Protections

As an added security measure we installed Kaspersky antivirus on the Remote Desktop service.

### Mail Server Protections

As an added measure to ensure the integrity of user mail, we installed TripWire and began monitoring file system changes. We have not detected any malicious activity, but we will continue to be vigilant.

### Green Team Host Machine Protections

We've received reports by federal investigators that there has been a rise in keylogger based malware on Green team host machines. We evaluated the threat and deemed it to be a significant threat. While our Green team documents are bootstrap instructions to get the Green team user to log into an Remote Desktop environment which is a secure environment over an encrypted tunnel, a physical keylogger or keylogging malware installed on the host system could still be used to intercept passwords and other sensitive data. We attempted to mitigate this threat through the following actions.

- We inspected the host machines for physical attachments and software based malware. We observed no unexpected processes and found that all processes were digitally signed with valid certificates.
- On our Remote Desktop services we installed antivirus software that should catch typical variants of common malware including keyloggers.
- We briefed Green team members on social engineering attacks and implemented new security policies that require Green team members to prompt visitors for current Iowa State University student IDs before interacting with any unknown personnel.

## Yahoo Leak Response

We were given a public leak list of accounts from the Yahoo! Breach. After finding some of our users' live credentials on the leak document, we sprang to action by temporarily disabling the accounts. Our sandboxes and jails within our servers contained the attacks, however our servers sustained minor outages.

After gaining back control of our servers, we notified green team by updating the green team documentation. We changed the passwords of compromised users soon after disabling them. Within ten minutes, the user accounts were back up with new, secure passwords and green team was notified. We feel proud of the quick and legitimate administrative actions we took to regain access to our servers and stop the hackers in this instance. All of our services are back to green now on IScorE. We are closely monitoring the situation for any further leaks or breaches.

## 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. We've also seen known Red team members approach us and other teams with likely false information. However, as described in Green Team Host Machine Protections we have implemented new social security policies that ask Green team members to identify and valid photo IDs of Blue team members.