CONFIDENTIAL

Intrusion Report for CDC

Iowa State University

VERSION 10:00AM

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.

Server Reporting

Firewall Server Report

Time	Event	Description and evidence

Mail Server Report

Time	Event	Description and evidence

AD Server Report

Time	Event	Description and evidence

File Server Report

Time	Event	Description and evidence

DNS/NTP Server Report

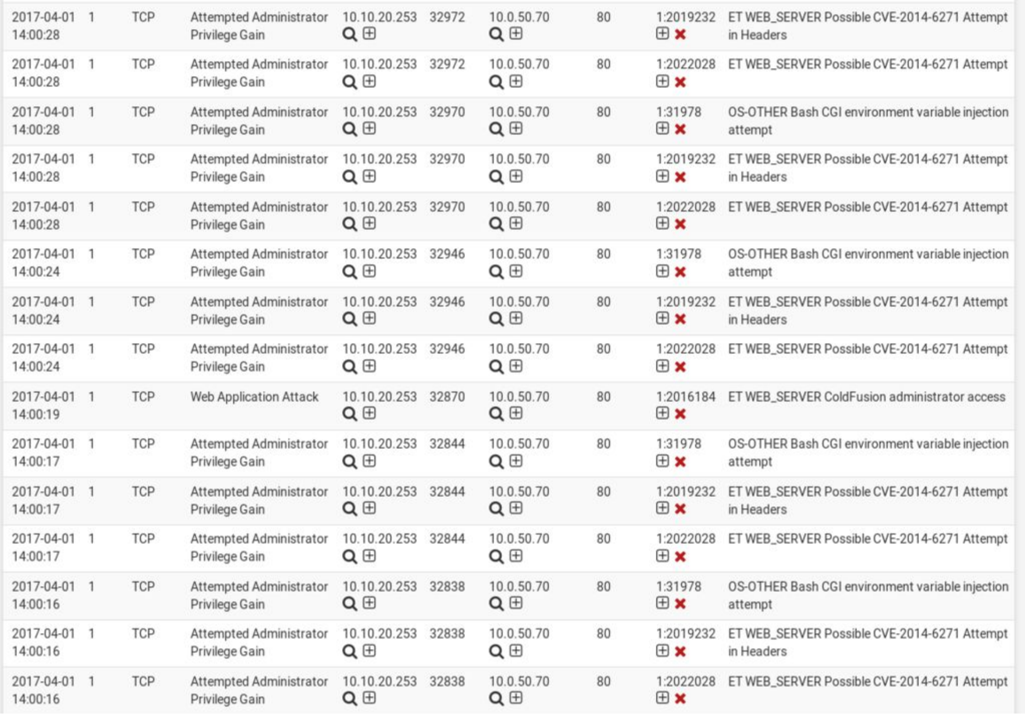
Time	Event	Description and evidence
18:58 (GMT)	DNS Check on Event Log	Security logs returned a positive audit. Some new events are included that arose after the latest report was due.

RDP Server Report

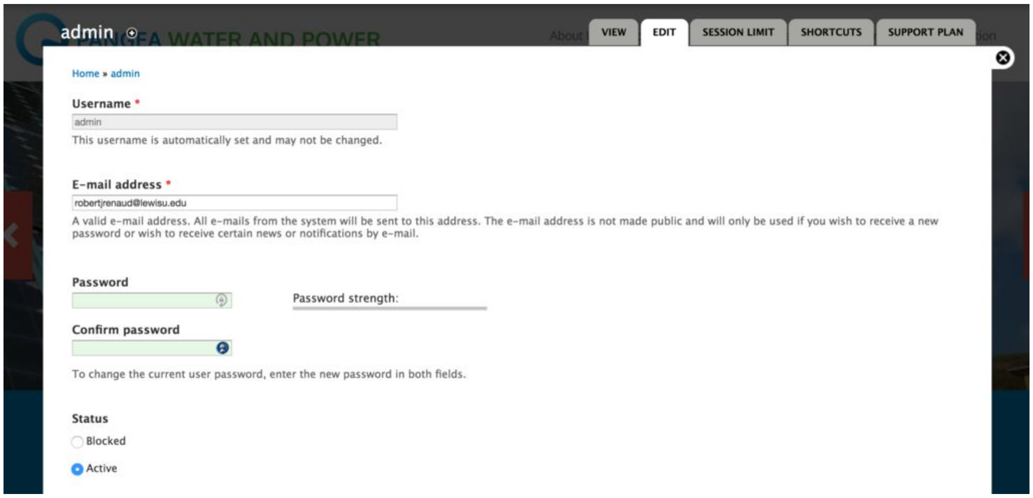
Time	Event	Description and evidence
09:52 (GMT)	Checked the event viewer security audit tab in Windows for RDP	RDP audits all passed. The RDP server is in good shape and untouched to the best of our knowledge.

WWW Server Report

Time	Event	Description and evidence



2017-04-01 14:00:28	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32972	10.0.50.70	80	1:2019232	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
2017-04-01 14:00:28	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32972	10.0.50.70	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2017-04-01 14:00:28	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32970	10.0.50.70	80	1:31978	OS-OTHER Bash CGI environment variable injection attempt
2017-04-01 14:00:28	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32970	10.0.50.70	80	1:2019232	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
2017-04-01 14:00:28	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32970	10.0.50.70	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2017-04-01 14:00:24	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32946	10.0.50.70	80	1:31978	OS-OTHER Bash CGI environment variable injection attempt
2017-04-01 14:00:24	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32946	10.0.50.70	80	1:2019232	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
2017-04-01 14:00:24	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32946	10.0.50.70	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2017-04-01 14:00:19	1	TCP	Web Application Attack	10.10.20.253	32870	10.0.50.70	80	1:2016184	ET WEB_SERVER ColdFusion administrator access
2017-04-01 14:00:17	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32844	10.0.50.70	80	1:31978	OS-OTHER Bash CGI environment variable injection attempt
2017-04-01 14:00:17	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32844	10.0.50.70	80	1:2019232	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
2017-04-01 14:00:17	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32844	10.0.50.70	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt
2017-04-01 14:00:16	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32838	10.0.50.70	80	1:31978	OS-OTHER Bash CGI environment variable injection attempt
2017-04-01 14:00:16	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32838	10.0.50.70	80	1:2019232	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers
2017-04-01 14:00:16	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253	32838	10.0.50.70	80	1:2022028	ET WEB_SERVER Possible CVE-2014-6271 Attempt



Home » admin

Username *

admin

This username is automatically set and may not be changed.

E-mail address *

robertjrenaud@lewisu.edu

A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by e-mail.

Password

Password strength:

Confirm password

To change the current user password, enter the new password in both fields.

Status

○ Blocked

● Active

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.