

November 3, 2014

Dr. David Daniel, President,
Ms. Lisa Choate, External Chair of the Audit and Compliance Committee:

We have completed an audit of the vulnerability scanning process as part of our fiscal year 2014 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objectives of the audit were to ensure that the vulnerability scanning process is aligned with best practices and to ensure that vulnerabilities are being addressed in a timely manner.

Overall, we found that the vulnerability scanning process appears to be generally aligned with best practices; however, vulnerabilities are not being addressed in a timely manner by the asset owners. The attached report details recommendations that will further enhance the vulnerability scanning process and improve timeliness of remediation efforts that are the responsibility of the asset owners.

Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.



Institutional Chief Audit Executive

UT Dallas Responsible Parties:

Mr. Nate Howe, Chief Information Security Officer

Members of the UT Dallas Audit and Compliance Committee:

External Members:

Mr. Bill Keffler

Mr. Ed Montgomery

Ms. Cynthia Trochu

Dr. Hobson Wildenthal, Executive Vice President and Provost

Dr. Calvin Jamison, Vice President for Administration

Mr. Terry Pankratz, Vice President for Budget and Finance

Dr. Andrew Blanchard, Vice President for Information Resources and Chief Information Officer, Dean of Undergraduate Studies

Dr. Bruce Gnade, Vice President for Research

Dr. Darrelene Rachavong, Vice President for Student Affairs

Mr. Timothy Shaw, University Attorney

The University of Texas System:

Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs

Alan Marks, Attorney

Mr. J. Michael Peppers, CIA, CRMA, CPA, FACHE, Chief Audit Executive

Ms. Moshmee Kalamkar, CPA, CIA, Audit Manager

State of Texas Agencies:

Legislative Budget Board

Governor's Office

State Auditor's Office

Sunset Advisory Commission

Executive Summary

Vulnerability Scanning Process, Report No. 1504

Audit Objective and Scope: To ensure that the vulnerability scanning process is aligned with best practices and to ensure that vulnerabilities are being addressed in a timely manner.	
Audit Results: The audit resulted in one recommendation considered as priority, or significant, to University operations and two other recommendations to enhance the vulnerability scanning process and improve timeliness of remediation efforts that are the responsibility of the asset owners.	
<i>Priority Recommendation</i>	<i>Estimated Implementation Date</i>
(1) Reduce Number of Outstanding Vulnerabilities	February 28, 2015
<i>Other Reportable Recommendations</i>	<i>Estimated Implementation Date</i>
(2) Enhance Vulnerability Scanning Process	May 31, 2015
(3) Enhance Controls Around Metasploit	November 30, 2014
Conclusion: The vulnerability scanning process appears to be generally aligned with best practices; however, vulnerabilities are not being addressed in a timely manner by the asset owners.	
Responsible Vice President: Mr. Terry Pankratz, Vice President for Budget and Finance	Responsible Party: Mr. Nate Howe, Chief Information Security Officer
Staff Assigned to Audit: Ali Subhani, CIA, CISA, GSNA, IT Audit Manager; Colby Taylor, IT Staff Auditor	

Table of Contents

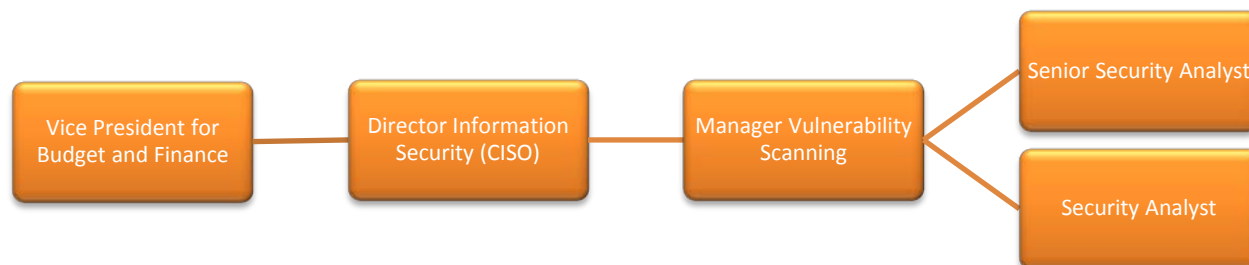
Background	4
Audit Objective	6
Scope and Methodology.....	6
Audit Results and Management's Responses.....	6
Audit Recommendations	7
<i>Priority Recommendations</i>	
(1) Reduce Number of Outstanding Vulnerabilities.....	7
<i>Other Reportable Recommendations</i>	
(2) Enhance Vulnerability Scanning Process	9
(3) Enhance Controls Around Metasploit.....	12
Conclusion	14

Background

According to TAC §202.70 (4),¹ “Risks to information resources shall be managed.” Unpatched operating systems, out of date applications, and vendor supplied default passwords all contribute to increased risks within the information technology (IT) infrastructure. However, these risks can be managed if there are processes in place to detect vulnerabilities, assess their potential impact, and deploy corrective measures.

Vulnerability management includes processes and technologies that an organization utilizes to identify, assess, and remediate vulnerabilities that exist in IT infrastructures. The [Information Security Office \(ISO\)](#), within the Office of Budget and Finance (OBF), is responsible for administering the vulnerability management processes at the University. The ISO’s responsibility is limited to managing the processes to identify, assess and communicate vulnerabilities within the IT infrastructure. The responsibility for carrying out steps to remediate vulnerabilities that are discovered rests with the asset owner(s).

ORGANIZATION CHART



The ISO’s vulnerability management process can be divided into two different activities:

- Web Application Activities – are only focused on scanning web applications that are accessible from outside the university network.
- IT Infrastructure Activities – are focused on scanning assets that are accessible from both the internal (private assets) and external (public assets) university network.

The following tools are utilized by the ISO in the vulnerability scanning process:

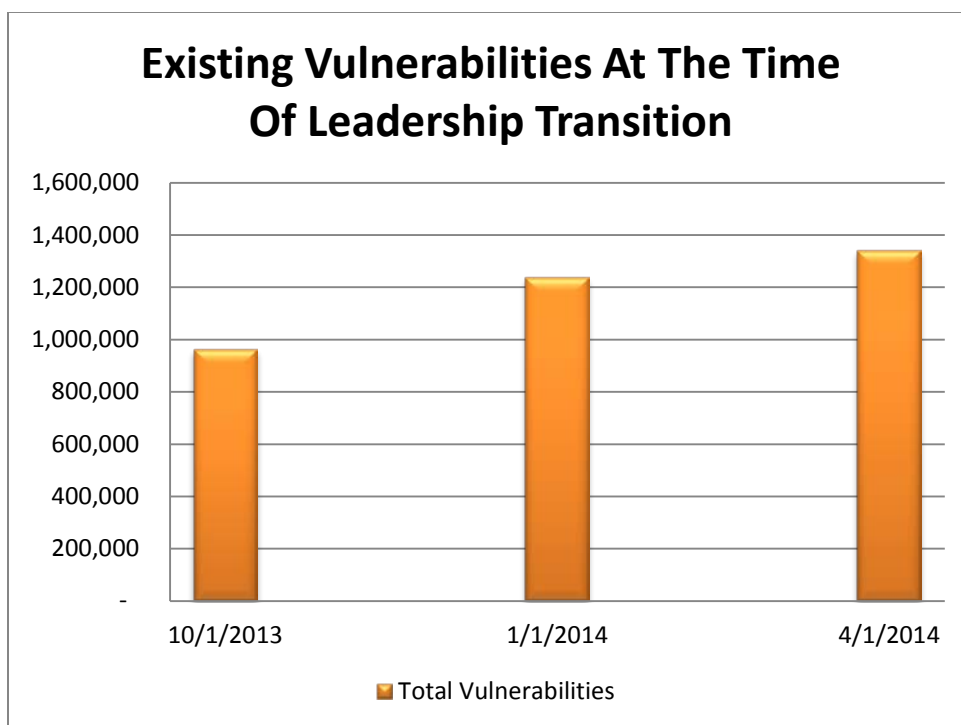
- Cenxic - utilized for identifying vulnerabilities in web applications.
- Metasploit - utilized for exploiting vulnerabilities that may exist within the infrastructure.
- Nexpose - utilized for identifying vulnerabilities in servers, workstations and databases.

¹

[http://info.sos.state.tx.us/pls/pub/readtac\\$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70](http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)

- Secunia - utilized for automating patching of software, thus reducing the administrative burden on technical staff.

During fiscal year 2014, a change in leadership was made within the ISO, and a new director for the department was hired in March 2014. Prior to the change in leadership, opportunities existed to improve the vulnerability scanning process and the number of vulnerabilities continued to consistently increase since October 2013. The following chart depicts vulnerabilities that were noted in the vulnerability scans that were conducted prior to the start of the audit:



As evidenced, by the chart above, the new Director has inherited a problem that has continued to get worse over time. The Director has strengthened vulnerability management by formalizing the process and reassigning responsibilities so that two additional staff members can assist with vulnerability management activities. As a result of the strengthened process, there has already been a decrease in the number of vulnerabilities in select departments on campus. Best practices that were observed within the audit are detailed below.

Audit Objective

To ensure that the vulnerability scanning process is aligned with best practices and to ensure that vulnerabilities are being addressed in a timely manner.

Scope and Methodology

The scope of this audit was Fiscal Year 2014 to date, and our fieldwork concluded on August 29, 2014. To satisfy our objectives, we performed the following:

- Interviewed personnel to gain an understanding of the vulnerability management processes.
- Reviewed tools that are utilized in the vulnerability management process.
- Evaluated the quality of scan templates that were being utilized to identify vulnerabilities.
- Evaluated the percentage of assets that were being included in the scans.
- Identified assets that were excluded from vulnerability management scans.
- Validated that the scan engines that were utilized by the scanning tools were up to date.
- Validated that there were adequate controls around a security tool that can exploit vulnerabilities.

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Overall, we found that the vulnerability management process can be further enhanced. Our audit work indicated that the following controls and best practices currently exist:

- The ISO has made the necessary investments to purchase software tools to identify vulnerabilities.
- Two new staff members have been assigned to help assist with vulnerability management activities full-time. Additional personnel will help strengthen the vulnerability management activities.
- Scanning engines that are being utilized in the software tools were up-to-date. This helps ensure that the ISO has the capability to detect new vulnerabilities as they are published by the security community.

- Scan templates that are being utilized were configured to perform detailed checks of all known vulnerabilities. This helps ensure that widely known vulnerabilities will be identified if present in the university IT infrastructure.
- The ISO has increased face-to-face interactions with technical staff to better understand their needs related to vulnerability management. The interactions have been well received by technical staff as they have had a forum to address their concerns.
- The ISO staff has recently had success in reducing the number of vulnerabilities by rolling out Secunia in a few select departments. Secunia allows for automated patching of third party software, which reduces the administrative burden on technical staff as they would have to manually install patches.
- Of the 15,105 assets identified during discovery scans performed by Nexpose on the internal network, vulnerability assessments were currently being performed on 13,183 assets.
- Access privileges within Nexpose were appropriately restricted as individuals were restricted to view and carry out scanning activities on sites that they were responsible for.

Although the above controls exist, opportunities to enhance the vulnerability scanning process are noted below.

Priority Recommendations

A priority recommendation is defined as one that may be material to operations, financial reporting, or legal compliance. This would include an internal control weakness that does not reduce the risk of irregularities, illegal acts, errors, inefficiencies, waste, ineffectiveness, or conflicts of interest to a reasonable low level. We noted **one priority recommendation** resulting from this audit.

(1) Reduce Number of Outstanding Vulnerabilities

According to TAC §202.70 (4)², “*Risks to information resources shall be managed.*” During a review of vulnerabilities that were present within the environment, it was noted that there are a large number of vulnerabilities that currently exist, and the vulnerabilities are not being remediated by asset owners consistently once they have been communicated by ISO personnel. The following metrics were noted during the audit:

2

[http://info.sos.state.tx.us/pls/pub/readtac\\$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70](http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)

*	PRIVATE ASSETS	PUBLIC ASSETS
Total Assets	17,701	1,286
Total Vulnerabilities	1,127,756	4,927
Average Number of Vulnerabilities Per Asset	63	3.8
Percentage of Critical Vulnerabilities	70%	

* Metrics based on vulnerability scan results from August 2014

The significant majority of vulnerabilities exist because system administrators are neglecting their responsibility to install software patches in a timely manner once they are published by the vendor. Additionally, business leadership may be unaware of the number of vulnerabilities that exist. Currently, the vulnerabilities are only communicated to technical staff with responsibility for managing IT assets.

Recommendation: Management should consider:

- Implementing a quarterly reporting process where the CISO informs senior leadership (vice presidents and deans) of vulnerabilities that exist within assets under their responsibility.
- Establishing a target date for reducing the number of vulnerabilities that exist.
- Implementing procedures to hold System Administrators accountable for not carrying out their responsibility to patch systems in a timely manner.

Management's Response: *To promote remediation of vulnerabilities in a timely manner, the Information Security Office will develop improved reporting and metrics which will be shared with system owners, their supervisors, vice presidents and deans. System owners will be asked to document the timeframe in which remediation can be expected and the Information Security Office will track the timely completion of those commitments. We expect these additional tracking processes to be in place by February 30, 2015.*

Estimated Date of Implementation: *February 28, 2015*

Person Responsible for Implementation: *Nate Howe, CISO*

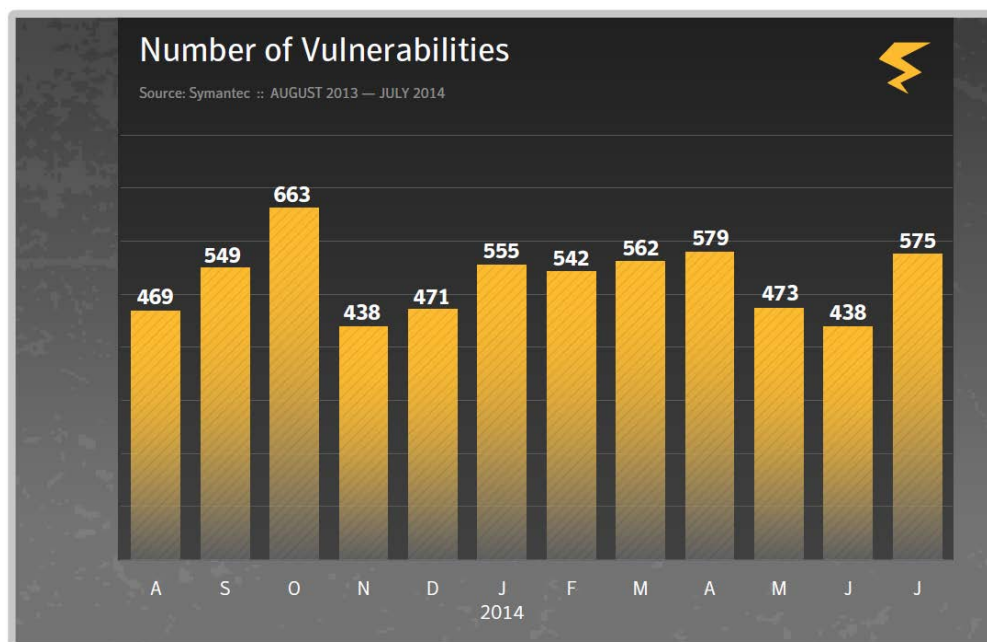
Other Reportable Audit Recommendations

The following recommendations should also be considered to improve the vulnerability scanning process.

(2) **Enhance Vulnerability Scanning Process**

According to TAC 202.75 ³, “(4) *Risks to information resources shall be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.*” During review of the vulnerability management process the following opportunities to manage risk by further enhancing the scanning process were noted:

- The ISO currently performs scanning of IT assets once every quarter. This includes assets that are accessible from outside the university network which are at increased risk of malicious activity due their accessibility from the outside world. New vulnerabilities are developed regularly, and quarterly scans may not be adequate for assets that are within the publicly accessible space. The following chart depicts the number of new vulnerabilities that have been discovered by security personnel on a monthly basis in the past fiscal year.



³

[http://info.sos.state.tx.us/pls/pub/readtac\\$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70](http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=70)

⁴ http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_07-2014.en-us.pdf

- A complete inventory of web applications that are present on the network currently does not exist. As a result, vulnerabilities that may be present within high-risk web applications have not been completely identified. This is mainly due to the ISO historically not having adequate staff resources devoted to scanning activities. Additionally, the ISO faces heavy resistance from technical staff when attempting to scan web applications due to the disruptive nature of the scans. The ISO scans can, however, be adequately planned to be performed outside of regular business hours to minimize the impact on users. Any vulnerability that would be exploited by a malicious user would not offer this benefit.
- There are currently no policy guidelines that mandate the timeframe within which asset owners must remediate the vulnerabilities that have been identified by ISO or the consequence for untimely remediation of the vulnerability by the asset owner. As a result, the timeliness of remediation by the asset owners could be generally improved as depicted by the following table:

VULNERABILITY AGE*	PRIVATE ASSETS	PUBLIC ASSETS
More Than 90 Days	1,106,981	4,844
61 To 90 Days	12,491	60
31 to 60 Days	8,274	23

* Metrics based on vulnerability scan results from August 2014

- Infoblox Grid is utilized by the Office of Information Resources (OIR) to centralize management control across network subnets, zones and sites. It offers the best inventory of IP addresses that are actually being utilized. Currently, no reconciliation is done between Infoblox and the discovery scans that are performed within Nexpose or Cenzic to identify assets that were not identified during discovery scans. As a result, there is a risk that assets that were powered off or inaccessible due to lack of network connectivity when the discovery scans were performed would not have received a vulnerability assessment. According to conversations with the Vulnerability Scanning Manager, reconciliation between Infoblox and Nexpose offers little value as the Networking and Telecommunication Services (NTS) department does not currently include comments that would help identify the physical location where the IP address is actually being utilized on campus. Without such data it is difficult for the ISO to locate the asset for further investigation even if reconciliation was being performed.

- When vulnerability scans are conducted, the ISO has the option of running an authenticated or an unauthenticated scan. Authenticated scans use credentials to do deep scanning whereas unauthenticated scans are limited to identifying vulnerabilities that can be remotely exploited without any credentials. Scanning processes that are being carried out on non-Windows operating systems are being performed with unauthenticated scans. This is due to lack of a central privileged user account in the non-Windows operating system environment. As a result, there is a risk that scanning activities are currently not identifying all vulnerabilities that exist on assets that are not running Windows operating systems.

Recommendation (a): Management should consider:

- Increasing the frequency of scans that are being performed on assets that reside within the public IP space (accessible from outside UTD network).
- Formalizing a policy that requires asset owner to remediate vulnerabilities within a timely manner.
- Performing reconciliation between the Nexpose discovery scans and Infoblox Lease History to identify assets that require further research for vulnerability management.
- Running credentialed scans on the non-Windows operating system environments.
- Further expanding scanning activities that are focused on internal and external web application assets. Empowering the ISO to carryout scanning of web applications.

Management's Response: *To enhance the vulnerability scanning processes, the Information Security office will make the following changes by April 30, 2015*

- a. Evaluate the frequency of scanning and document the rationale. More frequent scanning is desirable but must be balanced with other resource commitments, such as focusing on remediation support.*
- b. Standard remediation timeframes will be defined, based upon the various risk levels, and system owners will be asked to justify cases where timelines cannot be met.*
- c. Once NTS has enhanced data that is retained within InfoBlox, ISO will evaluate the feasibility of developing a reconciliation process between InfoBlox and Nexpose.*
- d. Request credentials to non-Windows systems to increase the level of detail obtained in scans, for specific high-risk systems. Because credentials to each non-Windows system must be requested on a case by case basis, rather than using a single account for all systems, this can be time consuming and will be balanced with the criticality of the asset being assessed.*
- e. Develop an inventory of web applications and assign risk ratings, with higher-risk sites being Internet accessible and/or accessing confidential information from a backend database.*

Estimated Date of Implementation: *April 30, 2015*

Person Responsible for Implementation: *Nate Howe, CISO*

Recommendation (b): NTS should develop a process so that comments indicating the physical location and relevant departmental information are included for the networks that are created within Infoblox.

Management's Response: *Agree. IR AIS/NTS is currently working to remove the 10.110 networks from infoblox and expects to have this completed within the next 6-12 months. Currently all new networks that are inserted are labeled by their function but not their location (building/floor). IR AIS/NTS will start the internal conversation & process to establish a procedure to capture that information and then develop a project to start updating the existing networks within infoblox.*

Estimated Date of Implementation: *May 31, 2015*

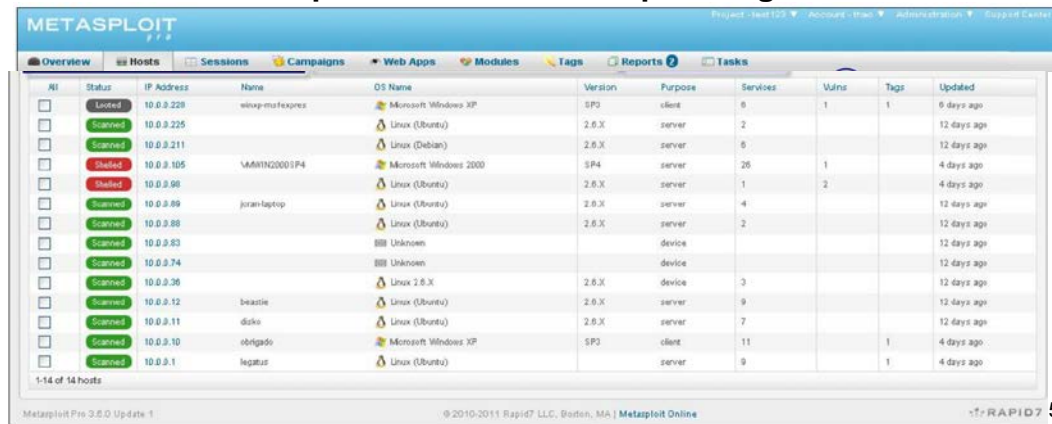
Person Responsible for Implementation: *David Nguyen, Associate Vice President Information Resources*

(3) **Enhance Controls Around Metasploit**

Metasploit is a security tool that allows security professionals to easily exploit vulnerabilities that have been discovered during vulnerability management processes. Such capability is required for instances where the security team is having difficulty convincing the asset owner that there is truly a need for remediating vulnerabilities. The Metasploit tool is accessible by three individuals within the ISO team. It was noted that:

- Currently, there is no departmental process that mandates formal authorization to be gained prior to utilizing Metasploit. As a result, there is risk that capabilities within Metasploit could potentially be abused, since individuals within the ISO would already be aware of the vulnerabilities that exist within the environment. During review of the logs that were available, it was observed that Metasploit has not been utilized against a production system to date.
- Logs generated by Metasploit can be deleted from the operating system by three individuals that are part of the vulnerability scanning team within the ISO team. As a result, there is a risk that logs that would track potential abuse of the capabilities offered by Metasploit can be destroyed.
- Currently, Metasploit logs are not sent to a logging server that ISO utilizes for consolidating logs from critical infrastructure. Additionally, Metasploit logs are currently not monitored by someone outside the vulnerability scanning team on a periodic basis. As a result, there is risk that any potential abuse of the capabilities offered by Metasploit would not be detected.

Sample Screenshot Metasploit Log



Host	Status	IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Tags	Updated
<input type="checkbox"/>	Loaded	10.0.0.228	winsp-mstexec	Microsoft Windows XP	SP3	client	8	1	1	6 days ago
<input type="checkbox"/>	Scanned	10.0.0.225		Linux (Ubuntu)	2.6.3	server	2			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.211		Linux (Debian)	2.6.3	server	6			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.105	VMWIN20001P4	Microsoft Windows 2000	SP4	server	26	1		4 days ago
<input type="checkbox"/>	Scanned	10.0.0.98		Linux (Ubuntu)	2.6.3	server	1	2		4 days ago
<input type="checkbox"/>	Scanned	10.0.0.89	jordan-laptop	Linux (Ubuntu)	2.6.3	server	4			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.88		Linux (Ubuntu)	2.6.3	server	2			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.83		BBB Unknown		device				12 days ago
<input type="checkbox"/>	Scanned	10.0.0.74		BBB Unknown		device				12 days ago
<input type="checkbox"/>	Scanned	10.0.0.36		Linux 2.6.3	2.6.3	device	3			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.12	beastie	Linux (Ubuntu)	2.6.3	server	9			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.11	disk	Linux (Ubuntu)	2.6.3	server	7			12 days ago
<input type="checkbox"/>	Scanned	10.0.0.10	obrigado	Microsoft Windows XP	SP3	client	11		1	4 days ago
<input type="checkbox"/>	Scanned	10.0.0.1	legatus	Linux (Ubuntu)		server	9		1	4 days ago

According to TAC 202.75⁶ "(A) Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or effect the release of confidential information. (B) Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules."

Recommendation: Management should consider:

- Sending Metasploit logs to a centralized logging server.
- Formalizing a process to authorize use of the Metasploit application.

Management's Response: *To ensure safety of the Metasploit tool, the Information Security Office will make the following changes by November 30, 2014.*

- Documented procedures will indicate that the Metasploit tool is only intended to be used against production systems when owners request additional evidence of vulnerability. An email approval from the CISO will be obtained before the tool is used to exploit a production system. The email will include a description of the vulnerabilities to be exploited and the justification explaining why the test will advance the objective of vulnerability reduction.*
- We believe it is feasible to send logs to a separate collection server, thus a reconfiguration will be attempted and reviewed for stability.*

Estimated Date of Implementation: *November 30, 2014*

Person Responsible for Implementation: *Nate Howe, CISO*

⁵ [http://academy.delmar.edu/Courses/ITSC1358/eBooks/Metasploit_ProGettingStarted\(book\).pdf](http://academy.delmar.edu/Courses/ITSC1358/eBooks/Metasploit_ProGettingStarted(book).pdf)

⁶ [http://info.sos.state.tx.us/pls/pub/readtac\\$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75](http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75)

Conclusion

Based on the audit work performed, we conclude that the vulnerability scanning process appears to be generally aligned with best practices; however, vulnerabilities are not being addressed in a timely manner by the asset owners.

We appreciate the courtesy and cooperation received from the management and staff of the ISO during this audit.