Vulnerability Assessment - 2016

NDUS – North Dakota University System – Dec. 2016

Document ID: NDUS.docx

December 21, 2016

Submitted to:

Prepared by:

Table of Contents

List of Exhibits

1. Executive Summary

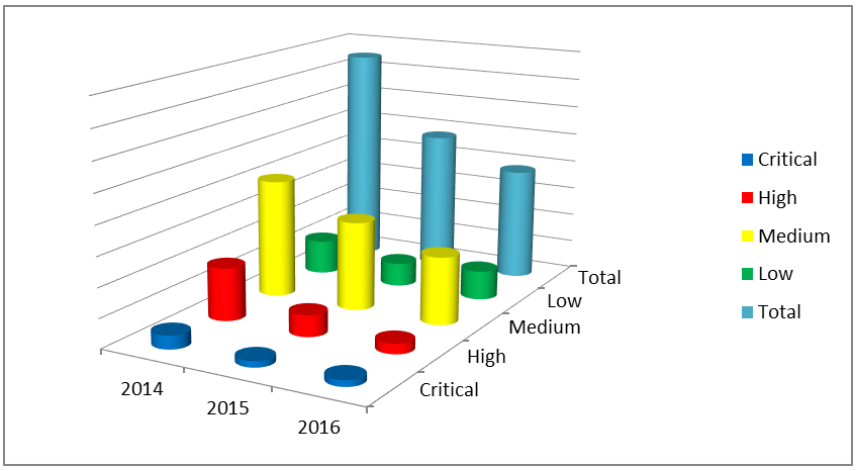
Information technology (IT) security practices are critically important for the North Dakota University System and its institutions to protect large amounts of sensitive and confidential information that are stored on their computer systems, including information for more than 45,000 students and 11,000 faculty and staff . Universities are attractive targets for computer hackers because they traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computer labs and high-capacity internet access that allows for the exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. University IT security problems are occurring more often through weaknesses in network and web-based computer programs and (applications) as well as via social engineering techniques.

On behalf of the North Dakota State Auditor and the North Dakota University System, from September 12 to October 20, 2016, Team Kimball (the team) carried out external and internal vulnerability assessments of the networks associated with the North Dakota University System (NDUS). These networks consisted of the following campuses as well as NDUS networks in the listed locations: Bismarck State College (BSC), Dakota College at Bottineau (DCB), Dickinson State University (DSU), Lake Region State College (LRSC), Mayville State University (MASU), Minot State University (MISU), North Dakota State College of Science (NDSCS), North Dakota State University (NDSU), NDUS Offices (Fargo, Bismarck, Grand Forks), University of North Dakota (UND), Valley City State University (VCSU), Williston State College (WSC).

External assessments were conducted with no privileges in order to mimic anyone surfing the Internet. In some cases as part of the external assessment, Team Kimball was provided with access to bypass external security controls. External network access as well as externally facing web applications were evaluated for each of the campuses. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases, as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation. The scans were configured to check for vulnerabilities on any host that was controlled by the campus. Key findings will be presented in detail within this report, 8 of the findings were found as part of the assessment in 2015 and one new finding was added associated with SSL certificates.

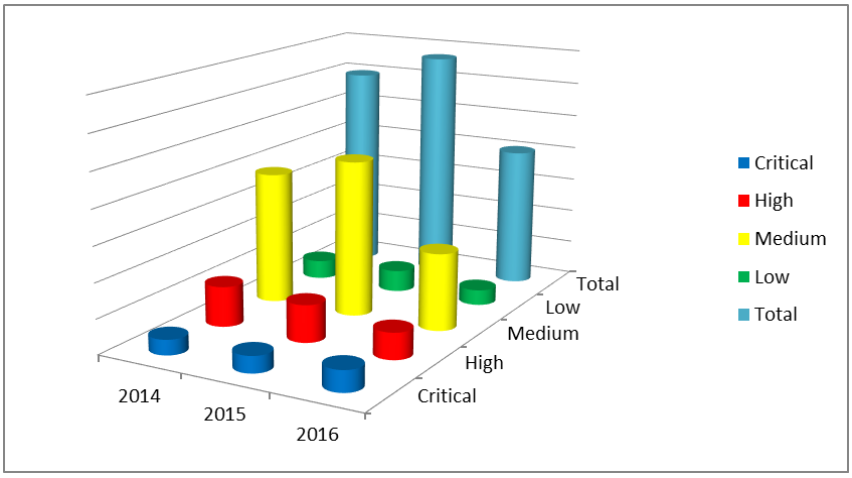
External Assessment findings show that the IT security of the NDUS systems has improved over the past year with the number of overall external vulnerabilities decreasing by more than 19% versus the 2015 assessment. Critical vulnerabilities in total count were unchanged and the High vulnerabilities were down by 53%. The Kimball team investigated the data further to determine the year over year vulnerabilities that were resolved and what percentage of vulnerabilities were new. This was performed for Critical and High vulnerabilities only. For Critical vulnerabilities from 2015 to 2016 50% were resolved. 68% of the critical vulnerabilities represented new vulnerabilities. For High vulnerabilities from 2015 to 2016 54% were resolved. 34% of the high vulnerabilities represented new vulnerabilities. Overall 46% of vulnerabilities were new. 53% were resolved from 2015 to 2016.

Figure 1. External Vulnerability Assessment Findings 2014 / 2015 / 2016



The Internal Assessment findings show that the internal IT security of the NDUS systems improved with total vulnerabilities down by 40% over 2015 numbers. However, there was an increase of 26% associated with Critical vulnerabilities and a decrease in High vulnerabilities by 29%. With respect to Critical vulnerabilities from 2015 to 2016 75% were resolved. 76% of the critical vulnerabilities reported represented new vulnerabilities. For High vulnerabilities from 2015 to 2016 70% were resolved. 65% of the high vulnerabilities represented new vulnerabilities. Overall for internal vulnerabilities 69% of vulnerabilities were new. 72% were resolved from 2015 to 2016.

Figure 2. Internal Vulnerability Assessment Findings 2014 / 2015 / 2016



These findings show that each of the campuses are focused on improvements in the overall security of the NDUS network but additional work is needed internal to the campus systems to keep pace with the significant progress that is being made on the external facing networks.

In addition to the vulnerability assessments, a phishing exercise was conducted to assess the level of awareness for each of the campuses and the NDUS office. This assessment was run from Nov 1 – Nov 8. Team Kimball provided immediate feedback via an educational page for those that fell for the phishing attempt.

Team Kimball also provided a policy and procedure review of the current NDUS policies with respect to established standards within the NIST (National Institute of Science and Technology) Cybersecurity Framework. These findings will provide the NDUS with guidance and prioritization on where they should spend time and resources to close existing gaps with respect to policies and procedures based on industry standards.

Appendix A of this document contains a response from the NDUS to the findings of the assessments.

2. Introduction and Background

Information technology (IT) security practices are critically important for the North Dakota University System and its institutions to protect large amounts of sensitive and confidential information that are stored on their computer systems, including information for more than 47,000 students and 11,000 faculty and staff. Universities are attractive targets for computer hackers because they traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computer labs and high-capacity internet access that allows for the exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. University IT security problems are occurring more often through weaknesses in network and web-based computer programs and applications as well as via social engineering techniques

IT security violations have occurred both in North Dakota and other states. The Privacy Rights Clearinghouse[1] database includes 768 breaches involving educational institutions that were made public in 2005–2016, involving more than 14 million breached records. The number of breaches includes breaches attributed to higher education institutions as well as trade schools, K–12 schools and school districts, and education-related nonprofit organizations. In 2015, breaches of Pennsylvania State University and the University of Virginia were blamed on Chinese hackers. At the University of Connecticut, student Social Security numbers and credit card data were taken. Washington State University and Johns Hopkins University were also the target of attacks.

IT security is essential to help campuses comply with federal laws and regulations designed to protect sensitive information such as educational records, personally identifiable information, and financial aid records.

On behalf of the North Dakota State Auditor and the North Dakota University System, from September 12 to October 20, 2016, Team Kimball (the team) carried out external and internal

[1] See Privacy Rights Clearinghouse, https://www.privacyrights.org/.

vulnerability assessments of the networks associated with the North Dakota University System (NDUS). These networks consisted of the following campuses as well as NDUS networks in the listed locations: Bismarck State College (BSC), Dakota College at Bottineau (DCB), Dickinson State University (DSU), Lake Region State College (LRSC), Mayville State University (MASU), Minot State University (MISU), North Dakota State College of Science (NDSCS), North Dakota State University (NDSU), NDUS Offices (Fargo, Bismarck, Grand Forks), University of North Dakota (UND), Valley City State University (VCSU), Williston State College (WSC).

External assessments were conducted with no privileges in order to mimic anyone surfing the Internet. In some cases as part of the external assessment, Team Kimball was provided with access to bypass external security controls. External network access as well as externally facing web applications were evaluated for each of the campuses. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation. The scans were configured to check for vulnerabilities on any host that was controlled by the campus.

3. Scope

Testing was performed on all networked devices within the ranges specified by each campus. External and Internal ranges were assessed. The scans checked for known vulnerabilities and weaknesses in the network and attached hosts and appliances. All selected web applications were audited using Burp Suite Professional vulnerability scanner. All detected vulnerabilities and weaknesses were documented, and guidelines for remediation were provided.

The testing team conducted the Vulnerability Assessment (VA) in accordance with the VA portion of the Pentest Execution Standard (PTES)[2]. The web application vulnerability assessment was conducted in accordance with the Open Web Application Security Project (OWASP) Top 10[3] model for web application security where appropriate. For each Campus, the team compared 2015 results with 2016 results for an overall assessment of improvement in security level associated with the campus.

The external assessment found only one campus in the EXTREME range associated with the PTES evaluation. This campus showed great improvement over last year but needs to continue to close out specific findings to bring their overall risk down. The internal assessment found 6 of the campuses in the EXTREME PTES range with several of these showing increases in overall numbers of vulnerabilities from 2015 to 2016. Figures 1 and 2 show that the total number of vulnerabilities both external and internal to the NDUS network are trending down over the 3-year period of the assessment. However, internal Critical level vulnerabilities have increased in each of the years assessed. These should specifically be evaluated and action taken to address these specific issues.

4. Methodology

The team performed an external and internal vulnerability assessment to determine which hosts were visible from outside of the NDUS and each of the institutions' networks. The team followed the standard penetration test methodology for the security assessment as shown in Exhibit 1. The light blue boxes were completed as part of the vulnerability assessment and the dark blue as part of the penetration testing.

The team utilized the following tools to assess the network and networked devices:

- NESSUS (commercial version)
- BURP Suite Professional Vulnerability Scanner
- NMAP Network Scanner
- Nipper
- Nikto

[2] Vulnerability Analysis, PTES, accessed on September 27th, 2015, http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Vulnerability_Analysis
[3] OWASP Top Ten Web, accessed on September 27th, 2015, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

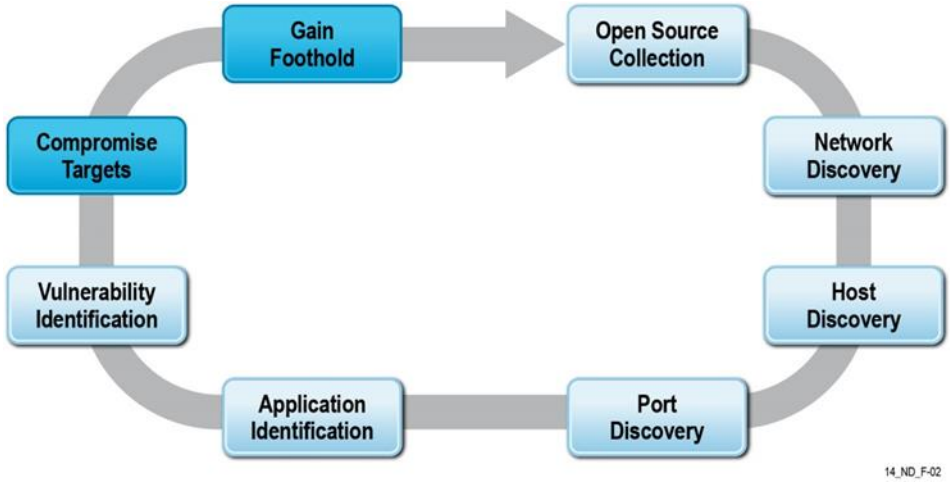


Figure 3. Team Kimball's Network Penetration Testing Methodology

5. Network Assessment Findings

The following findings represent a summarized version of the vulnerability assessments that were presented to each of the NDUS campuses and to NDUS. Detailed assessment results as well as remediation guidance for each of the findings have been provided to the campuses and many of them had resolved a significant portion of the critical findings prior to the team leaving the site. This section contains findings for both the external and internal network assessment. For the external assessment, the assessment team was connected to the internet with no special access. In some cases, as part of the external assessment, Team Kimball was provided with access to bypass external security controls. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases, as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation.

5.1. Finding 1: Missing Software Patch or Required Upgrade

It is imperative that software patches and software upgrades are applied in a timely manner, particularly those that are linked to application security. At the same time, it is important that the IT teams have sufficient time to evaluate the patches and upgrades to determine if their specific mix of applications will potentially have issues with the upgrade. This also allows the IT staff to ensure that their customer base does not have an adverse reaction to the patch.

Patch management is an important IT security practice designed to proactively prevent the exploitation of vulnerabilities on system devices. The expected result is to reduce the time and money spent dealing with vulnerabilities and their exploitation. Taking a proactive approach to patch management can reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after vulnerability has been exploited.

This item was again the largest finding in the assessment and contributed to the largest reported numbers of vulnerabilities. It is imperative that each of the campuses have a program in place to identify required patches and then to implement them in a timely manner. They must also have a system in place to prioritize those that may not be critical but are well known vulnerabilities that need to be addressed.

Recommendations for Finding 1: Missing Patches or Upgrades

1. Ensure that all campuses are running Nessus or equivalent tools for vulnerability assessment. This will allow them to determine what patches are required and be in a better position to provide prioritization associated with patching.
2. All campuses must apply all applicable hardware, software, and applications patches in a reasonable timeframe based on the severity of the issue. NDUS and the campuses should define the severity of the issue based on their current policies and procedures and risk associated with the software.

   Typical Patch Timelines:

   - Critical – 1 week
   - High – 45 days
   - Medium/Low – up to 1 year

3. Ensure a patch management program is in place that is tracking systems that are affected and timeline to resolution.
4. NDUS and campuses should evaluate commercially available patch management products to expedite patching and updates. Some commercially available products include:

   Commercially Available Patch Management Products:

   - ManageEngine Desktop Central (Win/Mac/3rd)
   - Symantec IT Management Suite (Win/Mac/Linux/3rd)
   - Dell Kace (Win/Mac/Linux/3rd)
   - GFI LanGuard (Win/Mac/Linux/3rd)
   - Microsoft SCCM

5.2. Finding 2: Unsupported Operating Systems

The assessment team found unsupported operating systems at nine of the eleven locations assessed as well as at the NDUS office. The operating systems were primarily Windows based with a few instances of unsupported UNIX, Linux, ESXi, and Cisco(IOS) systems found as well. The proliferation of unsupported and end-of-life products is an issue for many organizations and increases the effort required to minimize risk. As applications and operating systems reach their end-of-life (EOL), vendors stop offering support. Therefore, security and stability decrease, allowing attackers to exploit found vulnerabilities that will never receive a patch or security update. Patches, updates and security fixes will no longer be available, so identifying systems running EOL operating systems and applications is an important part of assessing and minimizing organizational risk

End of Support for XP SP2

The Service Pack support for the 32-bit edition of Windows XP™ SP2 was retired on July 13, 2010 and the 64-bit edition of XP SP2 was retired on April 8, 2014. Microsoft Windows Server 2003 support ended July 14th, 2015.

Consumers, business users, and software developers using Windows 2003™ and Windows XP™ SP2 (x86) will no longer receive updates for security fixes and non-security hotfixes.

The Risks in Using Unsupported Operating Systems

There are risks in using Windows 2003™ and XP SP2 (x86) because consumers will no longer receive product support, bug fixes, and patch releases. Any known and unknown vulnerabilities affecting the unsupported operating systems create a risk of exploitation or data breaches from attackers on the vulnerable OS.

Other risks from using Windows XP™ SP2 (x86) and Windows 2003™ occur whenever malware creators release malicious codes targeting unsupported and unpatched operating systems. Over time, the software developers and security software vendors offering protection for an unsupported OS will also stop providing detection signatures and product support. With that in mind, any malware targeting old OS puts an organization at risk of data loss or a security breach. The worst scenario is when critical and sensitive data is stolen by malware attackers.

In Flexera Software (Secunia) Vulnerability Review 2016, on average, over a five year period, the share of non-Microsoft vulnerabilities has hovered around 78%, peaking at 88.5% in 2012. This high-level percentage plateau is significant and makes it evident why end users and organizations cannot manage security by focusing on patching their Microsoft applications and operating systems alone. If they do that, they are only protecting their computers and IT infrastructures from 21% – a fifth – of the total risk posed by vulnerabilities.[4]

Recommendations for Finding 2: Unsupported Systems

1. Where possible move from unsupported versions of operating systems to supported versions.
2. For systems where this is not possible or where the cost is too high, consider defense in depth strategies to mitigate risk to these systems:
    a. Shutdown ports and applications not required
    b. Limit access to the machine
    c. Segregate the machine where possible
3. If the following operating systems are deployed or continue to be required within the NDUS network, an accurate inventory of these systems should be maintained, a waiver should be provided, and a defense in depth strategy outlined for protection of the machine and its associated network components.[5]

    - Mac OS X 10.5 (Leopard) and below
    - Microsoft Windows XP Professional and below

[4] Flexera Software (Secunia) Vulnerability Review 2016: http://resources.flexerasoftware.com/web/pdf/Research-SVM-Vulnerability-Review-2016.pdf
[5] http://blogs.microsoft.com/on-the-issues/2013/10/29/new-cybersecurity-report-details-risk-of-running-unsupported-software/

- Microsoft Server 2003 and below
- Solaris 9 / SunOS 5.9 and below
- AIX 6.1 and below
- Debian 7.0.x (EOL Apr 2016) and below
- FreeBSD 10.2 and below
- Red Hat Enterprise Linux 3.x and below
- SUSE Linux Enterprise 11 and below
- Ubuntu 12.04 (EOL April 2017) and below
- CentOS 5 (EOL 31 Mar 2017) and below

5.3. Finding 3: Easily Guessed or Default Credentials

Passwords are instrumental in the protection of data, systems, and networks. For example, passwords are used to authenticate users of operating systems and applications such as email, labor reporting, and remote access. In addition, passwords are often used in less visible ways; for example, a biometric device may generate a password based on a fingerprint scan, and that password is then used for authentication.

Organizations should be aware of the drawbacks of using password-based authentication. There are many types of threats against passwords, and most of these threats can only be partially mitigated. Also, users are burdened with memorizing and managing an ever-increasing number of passwords. However, although the existing mechanisms for enterprise password management can somewhat alleviate this burden, they each have significant usability disadvantages and can also cause more serious security incidents because they permit access to many systems through a single authenticator. Therefore, organizations should make long-term plans for replacing or supplementing password-based authentication with stronger forms of authentication for resources with higher security needs.

During our assessment, every campus was found to have systems with easily guessed or default credentials. These systems are goldmines for hackers as this provides easy access to the campuses internal network and may allow a hacker to move around (pivot) and gain additional footholds within the organization at will. In addition, if they are able to gain access to administrator level accounts the attackers will have full access to the system and any files or network access associated with the account.

Recommendations for Finding 3: Easily Guessed or Default Credentials

1. Create a password policy that specifies NDUS password management related requirements
2. Protect passwords from attacks that capture passwords (use HTTPS for web password submission or use multifactor authentication)
3. Configure password mechanisms to reduce the likelihood of successful password guessing and cracking

4. Determine requirements for password expiration based on balancing security and usability
5. Ensure systems are not deployed with default or out of the box user/password settings

5.4. Finding 4: Systems with well-known vulnerabilities

All eleven campuses and the NDUS office contained systems with well-known vulnerabilities. Each of these vulnerabilities have been in the news and patches have been available for some time. In addition, Nessus and other vulnerability assessment tools have supported identification of each of these vulnerabilities. These are called out because each of these vulnerabilities is known to be exploitable and open source exploits are widely available on the Internet.

Recommendations for Finding 4: Systems with well-known vulnerabilities

1. Ensure that all campuses are running Nessus or equivalent tools for vulnerability assessment. This will allow them to determine what patches are required and be in a better position to provide prioritization associated with patching.
2. All campuses must apply all applicable hardware, software, and application patches in a reasonable timeframe based on the severity of the issue. NDUS and the campuses should define the severity of the issue based on their current policies and procedures and risk associated with the software.

5.5. Finding 5: Cleartext Password

Passwords submitted over an unencrypted connection are vulnerable to capture by an attacker who is suitably positioned on the network. This includes any malicious party located on the user's own network, within their Internet Service Provider (ISP), within the ISP used by the application, and within the application's hosting infrastructure. Even if switched networks are employed at some of these locations, techniques exist to circumvent this defense and monitor the traffic passing through switches.

The application should use secure socket level or transport-level (SSL or TLS) encryption to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas of the application should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

Recommendations for Finding 5: Cleartext Password

1. Replace HTTP web services with HTTPS version in instances where data must be protected.
2. Replace unsecured services, such as telnet and rlogin, with a secure shell (SSH) service. If you must operate unsecured command line services, it is recommended that you operate them within a secured tunnel like SSL/TLS or VPN.

3. Training for user awareness.

5.6. Finding 6: SSL Certificate Issues

The http clear-text protocol is normally secured via an SSL or TLS tunnel, resulting in https traffic. In addition to providing encryption of data in transit, https allows the identification of servers (and, optionally, of clients) by means of digital certificates.

Historically, there have been limitations set in place by the U.S. government to allow cryptosystems to be exported only for key sizes of, at most, 40 bits, a key length which could be broken and would allow the decryption of communications. Since then, cryptographic export regulations have been relaxed (though some constraints still hold); however, it is important to check the SSL configuration being used to avoid putting in place cryptographic support which could be easily defeated. SSL-based services should not offer the possibility to choose weak ciphers.

Recommendations for Finding 6: Unsupported Web Server

1. Purchase or generate a proper certificate for this service.
2. If SSL is necessary, use strong hashing/encryption algorithms

5.7. Finding 7: Unsupported Web Server

During the assessment, it was determined that five of the eleven campuses assessed had unsupported web servers operating in their networks – this was up from 3 findings in 2015. These represent a security issue based on the risk associated with discovered vulnerabilities that cannot be patched or remedied by the web server supplier. Since these applications are directly connectable via the Internet, it is easy for an attacker to find these targets and exploit them.

Recommendations for Finding 7: Unsupported Web Server

1. Evaluate the need for the web server. If it is no longer being used shut it down.
2. Upgrade the server to a supported release.

If the server is no longer supported, look for a web server that is supported and will meet the requirements associated with your applications.

6. Web Application Assessment Findings

The website for each of the campuses and NDUS was assessed. The assessment team evaluated the web sites using Burp Suite Professional Vulnerability Scanner. This tool audits the web site for any potential attack vectors by issuing a number of requests and processing the results it receives from the server.

6.1. Finding 8: Cross-Site Scripting

During the web application assessment, three of the eleven campus websites had cross-site scripting related issues.

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. The attacker can create an innocuous looking web site which causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality which it contains, and the other applications which belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain which can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and therefore may be considered high risk. Similarly, if the organization which owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application, and exploiting users' trust in the organization in order to capture credentials for other applications which it owns. In many kinds of applications, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Recommendations for Finding 8: Cross-site Scripting

1. Input should be validated as strictly as possible on arrival, given the kind of content which it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
2. User input should be hypertext markup language (HTML)-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

6.2. Finding 9: Structured Query Language (SQL) Injection

SQL injection vulnerabilities arise when user-controllable data is incorporated into SQL database queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

Recommendations for Finding 9: SQL Injection

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. The affected campuses should review the documentation for the database and application platforms to determine the appropriate application program interfaces (APIs) which can be used to perform parameterized queries. It is strongly recommended that the affected campuses parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

Organizations should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective.

One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string in which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.

Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

7. Phishing Assessment Findings

A phishing exercise was conducted to assess the level of awareness for each of the campuses and the NDUS office. This assessment was run from Nov 1 – Nov 8. Team Kimball provided an educational page for those that fell for the phishing attempt to provide additional information associated with phishing and what to look for in the future.

As part of the assessment, Team Kimball sent over 9000 phishing attempts to members of the NDUS and campuses faculty and staff looking for those that would click thru on the social engineered link and then attempted to solicit user level credentials. The findings for the assessment found that 3.4% of those tested clicked on the link. In addition, of those that clicked on the link almost 40% continued and submitted credentials representing about 1.3% of those assessed.

To compare this with industry average data the Verizon DBIR report[6] for 2014 and 2015 show historical numbers of 23% click rate and 11% credential submission for 2014 and 30% click rate and 13% submission for 2015. Duo Insight reported[7] 31% click rates on phishing emails and 17% entered credentials and the University of Delaware[8] in conjunction with the Department of Homeland Security has conducted phishing over the past two years with 25% clicking link in 2015 and 18% clicking link and 12% submitting credentials in 2016.

Based on these numbers the 3.4% click rate for the NDUS staff is very good. For those that did click the link and proceeded to provide credentials a 40% submission rate is also below industry average of ~50%. However, identifying those folks at risk and providing training is important to continue to reduce risk.

It is important to note that as a part of this assessment, NDUS and the campuses provided additional access to the team to ensure that all emails were delivered. For each campus and the NDUS office – email filtering would have stopped a significant portion of the phishing attempts from ever reaching the intended recipient. This does simulate real world in that in some cases emails did get thru and there is no insurance that filtering would protect the end user.

Immediate training was provided to each user that clicked thru and submitted credentials in the form of a web page describing how phishing works and what they can do to better protect themselves.

1. Recommendations for Phishing Assessment Findings: User awareness training. While click thru and submission rates were very good as part of this assessment, 121 sets of credentials were still submitted showing a continued need for training.
2. Quarterly phishing - to validate the training and ensure credential submission rate remains below industry norms. Ensure training is provided immediately as part of the phishing exercise.
3. Verify spam filters are enabled to recognize and prevent emails from suspicious sources from ever reaching the inbox of employees.
4. Consider the use of Two factor authentication to prevent hackers who have compromised a user's credentials from ever gaining access.
5. Consider browser add-ons and extensions that can be enabled on browsers that prevent users from clicking on malicious links based on reputation.

[6] Verizon's 2016 Data Breach Investigations Report (DBIR) - www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

[7] Duo Security - https://www.teneo.net/us/blog/users-still-falling-phishing/

[8] University of Delaware phishing results 2016 - http://www1.udel.edu/udaily/2016/feb/phishing-test-021516.html

8. Policy and Procedure Assessment Findings

Team Kimball reviewed all information security documentation provided by North Dakota University System currently available with respect to the NIST Cybersecurity Framework. The review included all IT technical, operational, and management policies related to network and IT security.

NDUS is currently in the process of updating their information security policy framework. Documentation used by Team Kimball to perform the information security documentation assessment includes the following "Future Policy Framework" policies and standards that are currently available:

- *1202.1 Acceptable Use Policy*
- *1202.3 Data Privacy Policy*
- *1203.1 Network Security Standard*
- *1203.2 Server Security Standard*
- *1203.3 Physical Security Standard*
- *1203.7/1901.2.1 Data Classification and Information Security Standard*
  - *Classification of Common Data Elements*

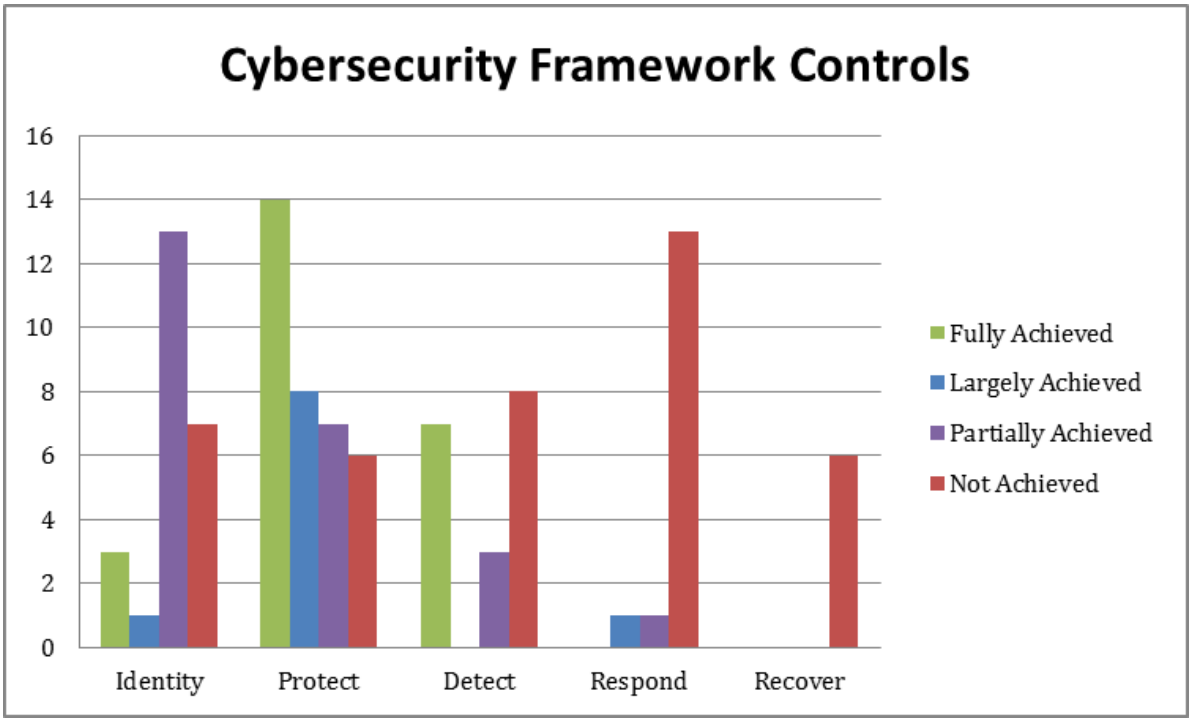
Planned "Future Policy Framework" information security documents not yet available for review include:

- *1203.4 Desktop Security Standard (December 2016)*
- *1203.5 Incident Response Standard (February 2017)*
- *1203.6 Disaster Recovery Standard (April 2017)*
- *1203.x Authentication Standard*
- *1203.x Data Disposal Standard*
- *1203.x Data Encryption Standard*
- *1203.x Mobile Device Standard*
- *1203.x Password Security Standard*

8.1. Security Control Evaluation

Documenting the implementation of security controls provides an understanding of the security posture for the system. The information below includes the number of relevant NIST Cybersecurity Framework controls that are grouped by the control families to which each relate. Based on the scope, the total controls per family are shown as fully achieved (FA), Largely Achieved (LA), Partially Achieved (PA), and Not Achieved (N), in accordance with how fully each is addressed in the current NDUS policy documentation.

Figure 4: Security Documentation Report Card – NIST CSF



The NDUS documentation can improve in the partially and not achieved areas by including policies and controls in the areas of:

Identify Core Function

- Definition of roles and responsibilities
- Risk Strategy including asset inventory and analysis
- Incident Response*
- Continuity Planning

Protect Core Function

- Authorization* & Password Security*
- Training and Awareness
- Roles & Responsibilities
- Incident Response*
- Continuity Planning

Detect & Respond Core Functions

- Incident Response*
- Continuity Planning

Recover Core Functions

- Incident Response*
- Risk Strategy

*indicates a NDUS policy document that is in the planning or developmental stage and not yet ready for review.

8.2. Recommendations / Follow-on Action Items

Team Kimball has identified specific recommendations to be considered in support of the development of NDUS's information security documentation. The recommendations are listed below.

1. Create an NDUS Policies and Procedure repository

   A clear central location should exist for Policies and Procedures. Users should be able to navigate easily to security information and be linked to governing policies of organizations outside of NDUS.

2. Evaluate the need for and create additional policies

   Team Kimball recommends including expanded policies on:

   - **Roles and Responsibilities**
   - **Compliance**
   - **Training and Awareness**
   - **Cryptography**
   - **Software**

3. Expand on NDUS provided security documents

   NDUS would benefit in a thorough review and further customization of the policy requirements. As a top priority, Team Kimball recommends:

   - **Information Security Policy** that defines NDUS information security planning and implementation including IS objectives, goals, documentation, controls, and policies on continuity management, asset identification, risk management, training, reporting, and reviews of effectiveness.
   - **Risk Assessment/Management Plan** that includes defined likelihood, business impact, and criticality of compromise to every organizational information asset
   - **Business Continuity Plan**
   - **Anti-Malware Plan**

4. Evaluate the need for and create specific policies and procedures to expound on targeted areas of information security

   There is a continual need for updated and additional NDUS specific documentation that supports the overarching existing Policies. Specific targeted areas can be identified through risk assessments or security events.

9. Conclusion

Team Kimball identified vulnerabilities in the NDUS network and within the NDUS campuses' networks. Vulnerabilities were compared to 2014 and 2015 results and showed an improvement in both external and internal security posture of the NDUS as a whole. Individual reports were provided to each of the campuses as well as to the NDUS office. These reports provided detailed explanations associated with each of the vulnerabilities found as well as recommended remediation guidance.

This report identified the common vulnerabilities that were presented in each of the campus reports for the NDUS as a whole. It identifies that there are 9 key finding areas that need to be addressed and has provided recommendation guidance for addressing each of the findings. More specific and detailed guidance has been provided to each individual campus as part of their individual assessment and should be worked into their individual campus action plans for remediation.

Team Kimball reviewed the information security documentation provided by the NDUS and analyzed that documentation for effectiveness. Overall, there are many existing NDUS policies that provide a good foundation for governing an information security management system. The policies that exist provide the overarching structure for more detailed information in operational and technical procedures or controls in the areas of access, network design, least privilege, physical security, logging, data transfer, and vulnerability scanning. Incident Response, Authorization, Password Security, and Disaster Recovery are all planned policy standards and will satisfy many of the under achieved recommended policy requirements.

Focus should continually be put into providing more detailed information on important security areas as they are discovered. These specific areas of additional focus will be identified from several methods including risk assessments, findings from audits or third party evaluations, or those that arise as issues from incident management. Continual attention should be paid to developing existing policies and supporting procedures to deficient areas to mitigate risk and avoid possible future security events.

10. Points of Contact for this Report

Program Manager – Team Kimball

Scott Strom, PMP
Operations Manager
L.R. Kimball, a CDI Company
Email: Scott.Strom@cdicorp.com
Phone: (814) 472-7700

Principal Architect - Enterprise Security & Protection

Erik Wallace, CISSP
Director – Product Management
Comtech Telecommunications Corp.
Email: Erik.Wallace@comtechtel.com
Phone: 410-280-1184

Security Analysts - Enterprise Security & Protection

Jason Yorty, Sr. Security Researcher|Pentester, CISSP, GXPN, GWAPT, GPEN, GCIH
Ryan Miller, Senior Vulnerability Analyst
Phillip Kidd, CNO Trainer/ Instructor
David Cash, CNO Trainer/ Instructor
John Levy, Vulnerability Analyst
Ginny White, Principal Engineer Cyber Policy

11. Appendix A: NDUS Response

Finding 1: Missing Software Patch or Required Upgrade

- NDUS has a Nessus vulnerability scanning system that scans NDUS public-facing IP addresses for vulnerabilities. This has resulted in a significant decrease in vulnerabilities associated with external-facing systems within the past few years. NDUS and campuses will be replacing or upgrading this vulnerability scanning system within the next biennium. The replacement will have the potential to expand scanning capabilities to internal networks and systems. NDUS Core Technology Services (CTS) currently has plans to deploy a more robust enterprise vulnerability scanning system for its internal data center systems within the next six months.
- The Information Security Council (ISC), made up of CTS and campus security representatives created network, server, and endpoint security standards that define controls for addressing vulnerabilities and patching in a timely manner.
- CTS and some campuses do have patch management products in place such as Dell Kace and Microsoft SCCM and WSUS, but patching capabilities will need to be expanded as part of an overall patch management program.
- NDUS is in the process of deploying endpoint protection software to CTS and campus computer systems with patch management capabilities that could be utilized.

Finding 2: Unsupported Operating Systems

- Many of the unsupported operating systems identified have either been migrated to supported versions or where that is not possible, defense in depth strategies have been applied to mitigate risk.
- NDUS and campuses will need to expand the vulnerability management capabilities to continue to detect and mitigate unsupported operating systems in a timely manner.

Finding 3: Easily Guessed or Default Credentials

- NDUS and campuses have been and continue to develop security controls to mitigate the risk of stolen, weak and default credentials.
- A multifactor authentication (MFA) system was deployed and is currently protecting many systems and applications across NDUS and campuses, including many remote access and public-facing systems. This MFA system will continue to expand to additional systems and applications.
- A 90-day password change requirement was implemented for credentials managed by the NDUS Identity Management system. A new Identity Management system currently being deployed will assist in reducing risks associated with identity and password management.
- A Password Standard is on the development roadmap for the ISC. This standard will specify controls and requirements for password management.

- Vulnerability management capabilities will need to be expanded to internal campus and CTS networks to detect and remediate systems configured with default credentials.

Finding 4: Systems with well-known vulnerabilities

- As part of this assessment, Team Kimball was given access to several internal networks that an external attacker would not have access to. Many of the systems identified with well-known vulnerabilities were on these internal networks. While it is important to address vulnerabilities on internal protected networks, these vulnerabilities are a lower risk than those on external-facing systems.
- There is an ongoing effort within NDUS and campuses to move external facing devices to internal networks, or implement additional security protections, where possible. These efforts limit the risk of an external attacker exploiting systems with well-known vulnerabilities.
- NDUS standards have been developed to set requirements for the timeframe well-known vulnerabilities should be remediated and patches installed.
- NDUS and campuses will need to develop plans to expand the vulnerability scanning system to internal networks. To validate that standards are being met, mechanisms will need to be implemented to collect metrics such as vulnerability aging (to determine how long a system has been vulnerable without remediation).

Findings 5: Cleartext Password

- NDUS and campuses need to utilize HTTPS in place of HTTP when data in transit needs to be protected, such as in cases of password submission and private or restricted data.
- NDUS is in the process of deploying a secure file transfer system and system-wide VPN that can help reduce the risk of unsecured data transfers and unsecured remote access services such as telnet and rlogin.

Finding 6: SSL Certificate Issues

- NDUS has procured an SSL certificate service for campuses to use. The clear majority of the campuses external facing web servers and systems utilize valid, secure SSL certificates. Campuses need to request and apply valid SSL certificates for any external facing systems where strong encryption, authentication, and/or identification is needed.
- Many of the SSL certificate issues identified in this assessment were on internal-facing systems not accessible to the public or general staff and students, where the risk is lower.

Finding 7: Unsupported Web Server

- Many of the unsupported web servers identified on NDUS campuses are non-production web servers set up by faculty and staff outside of the IT department. Where these are

unnecessary, campuses should shut them down. In cases where they are needed, campuses must try to migrate these to secure production web servers in a data center running a supported web server release.

- Some of the unsupported web servers were on embedded hardware such as printers. In this case, campuses should consider disabling the web server or preventing access to the device.
- Vulnerability management capabilities will need to be expanded to internal campus and CTS networks to detect and remediate systems running an unsupported web server.

Findings 8 & 9: Cross-Site Scripting and SQL Injection

- NDUS and campuses need to explore capabilities for securely developing and testing web applications. NDUS and campuses need to explore training opportunities for web developers to increase knowledge of web application vulnerabilities and methods to prevent and detect them. Additional technology, such as Web Application Firewalls, and secure development platforms will be investigated as possible risk mitigation techniques.