Appendix A

Air Force Institute of Technology

Penetration Test of Simulated Election

Test Report

Sarah West
Travis Royer
Sarah Lasiuk
Phillip Jenkins
Casey Holgado
John Greenwell

Faculty Advisor: Maj Todd R. Andel, PhD

August 10, 2011

[redacted]

Table of Contents

[redacted]

Executive Summary

This document summarizes the results of a penetration test done by six Air Force ROTC students interning at the Air Force Institute of Technology (AFIT). We conducted this test to help assist the Federal Voting Assistance Program (FVAP). One of FVAP's primary goals is to ensure that overseas active duty uniformed service members and their families may participate in their right to vote overseas through absentee ballots. One of FVAP's goals is to develop a method of voting entirely online, using personal computers. FVAP initiated an effort to test these systems through conducting multiple penetration tests on three different vendors' online voting systems; these vendors are (*to protect the privacy of the vendors, they will be named only as*) Vendor-1, Vendor-2, and Vendor-3. A simulated election was run for a 72 hour-period between August 2-4, 2011. Our goal was to identify and explore any vulnerabilities present within the system and to exploit as many of these vulnerabilities as possible, under certain rules of engagement. With this goal, we attacked the vendors' systems using a variety of methods, logged all of our actions and the results, and prepared them in Appendix A of this report.

The most notable vulnerability was an open Secure Shell (SSH) login prompt on one vendor's servers. Though identified, we were not able to crack it. A host of vulnerabilities were found and tampered with on the laptops simulating the voter machines, including our infiltration with personal administrator accounts. We did not personally succeed in remotely compromising voter confidentiality. We discovered a wide range of information on the servers from NMap and Nessus scans, but none of which were dangerous to security. In the end, we tried many attack vectors, but were not particularly successful. We provided recommendations regarding improvements which can be made to security; but, having not made any prominent breaches in security, we conclude these voting systems to be quite well defended.

1. Assets of Value

The value of penetration testing lies in providing detailed security assessment on real life applications. We tested these voting systems to provide information regarding any potential vulnerabilities that could be present. This test was to establish a risk mitigation framework for any such vulnerabilities identified. In providing our assessments of these risks, we enable the vendors to correct any problems and eliminate vulnerabilities in their software. The process of penetration testing helps to maintain and improve the confidentiality, availability, and integrity of these systems and to determine the effectiveness of their individual security architecture.

2. Vulnerabilities

The most salient vulnerability that we identified was an open Secure Shell (SSH) login that was available on the Vendor-1 voting server. This is a prominent vulnerability because it was an open line to remotely log in to and gain control over the voting server. Anyone on the Internet could potentially connect to this open service.

Physical vulnerabilities abound; any personal voting machine may be tampered with. Each vendor provided a laptop for the simulated voting process. Due to the fact that the voting is not conducted on a well monitored kiosk station, the vendors cannot control the security of the machine on which a voter accesses their voting application via browser. All bets are off when it comes to the voter's machine; both remote threats and physical threats are present. There are no guarantees whatsoever that the voter's machine is free of malware such as rootkits or malicious

viruses. The primary vulnerability that exists in the case of an infected voter machine is that hackers may view the user's input and thereby compromise their confidentiality.

The voting servers hosted by the vendors were unlike the personal voting machines. Some vulnerabilities were identified with scanning software NMap and Nessus. We proved it possible to identify information about the vendor servers. Namely, we were able to scan the servers and identify certificate information, service detection, device type, Hypertext Transfer Protocol information, operating system, and trace route information. These results were not 100% certain, but possessed reasonable reliability. You may refer to Appendix A for each of the vendor's software vulnerabilities found through performing Nessus scans on each of the vendors voting servers.

3. Threats

The open SSH login vulnerability on the Vendor-1 voting server can be easily accessed by anyone connecting to the IP address ([redacted]) via PuTTY or other remote login software. A username and password is required, but with enough time an attacker can get around this by brute force. Programs such as Hydra may be used to continually brute force attack the username and password until a successful login is established. Social engineering is also a powerful means of obtaining usernames and passwords relatively easy if employees are untrained in operational security. We did not determine the username or password in our penetration test, and therefore were not able to remotely log in to the Vendor-1 server.

[redacted]

The largest threat that we exploited was the physical security of the machines on which the voters cast their votes. From the first hour of the penetration test we were able to have hands on access to the voting machines with no resistance. We were able to place our own administrator accounts on the machines as well as gather data as the voting systems Internet Protocol (IP) configurations and settings. We were personally able to look over the shoulders of voters and view who they had voted for, thereby compromising the confidentiality of their vote.

Like fore-mentioned as a vulnerability, the fact that the systems allow for remote voting via any Internet-accessible device. Such devices could have various types of malware loaded on it prior to voting, either knowingly or unknowingly, and the possibility of remote keylogging or manipulation of a compromised computer is present. Remote threats open the door to ignorance on the part of the voter. Alone in a windowless room, they may be completely unaware that their vote was observed, or that the attacker cut their connection at the last moment and denied them availability. We were not successful in exploiting any remote threats in any way.

The vulnerability shown by the information we were able to gather is a only an indirect threat. Threats such as this can be valuable to a hacker by informing him what exploits he should utilize. For example, knowing that the server is likely running a Linux kernel narrows the exploits that he will try. Likewise, the knowledge of particular certificates could make a hacker privy to software that may be exploitable. He may also use some of this information in a social engineering attack, i.e. by pretending to be a hardware technician.

4. Impacts/Consequences

An open SSH line would allow a malicious individual command line control over the server. Here, he could explore, change, delete, intercept, download files, upload viruses, and more. He is limited by little more than the rights of the account to which he is logged on (which can be further compromised), his imagination, and his personal skill set once he gains this kind of access. Such exploitation would be a massive compromise of the system's integrity.

If one vote can never be fully secure from being modified, the system does not possess perfect integrity. There are multiple ways integrity of these systems could be potentially compromised. The fact that the voting machine is unsecured could create a devastating impact on the confidentiality of a person's vote for the election. An attacker could load a piece of malware onto a voter's machine that would record how they voted and return the information to the attacker. This could be done remotely on a compromised machine by viewing through a Virtual Network Connection (VNC) window. A second impact using VNC would be that the attacker could take control of the voter's system after the voter logs in. Doing this would allow the attacker to use the voter's session to vote for whoever the attacker wants to win the election.

The impact of the leveraged information collected through scans is proportional to the impact of the exploit. This is wide and varied. By itself, the knowledge that a server is running certain software has little to no impact at all. It all depends on how the information is coupled with exploitation techniques such as hacking attempts and social engineering.

5. Risk Level

We categorize the open SSH server as a *medium* risk. A remote login to the server is a powerful exploitation opportunity for a malicious individual. However, brute forcing a password alone is a task which takes a considerable amount of time, let alone being unaware of both the username and the password. Yet social engineering vectors exist and the SSH command shell is a sumptuous feast for a hacker.

We categorize the threat of remote or physical voting machine exploitation as a *medium* risk. A possible impact of this threat is that an attacker could place malware onto the voter's machine that would compromise the confidentiality of their vote. The risk level for this is noteworthy, considering the fact that many users do not update their computers or keep them completely secure. The voting application uses a Hypertext Transfer Protocol Secure (HTTPS) connection that offers protection from the vote data being sniffed, however an attacker can simply view the vote from a VNC shell on the local host as it is taking place. A second consequence was also noted, stating that an attacker could take control the voter's session once they log in, allowing the attacker to vote for who they want to win or denying the right for the voter to cast their legal vote. Even though this would be an easy task for an attacker to do, they may opt not to use it due to the fact that it would be visibly obvious when it happens and the election results would probably be voided. Compromising an insecure system is a fairly easy task, and there is no way of enforcing the user to make sure that their computer is secure prior to voting. Although we were not able to successfully compromise the vendor's systems, these possibilities are always a threat. No vote over such open networks can have complete confidentiality, but public eyes expect 100% and view any loss as calamitous.

We categorize information gained through scanning as a *low* risk. This information is by no means privileged and carries little weight on its own. The knowledge it provides is small in comparison to the working knowledge required for high-risk exploitations.

6. Recommended Controls

We recommend the immediate removal of the SSH login available on the Vendor-1 voting server. If it is necessary that it remain open, the password and username should be frequently changed. Furthermore, the rights provided in the command shell should be as low as possible required to meet its purpose.

Complete security on the voter's machine is not possible. However, as the voter is beginning the process, prior to entering their confidential information, they should be instructed on steps that they may take to ensure immunity to common threats. We recommend the delivery of flags and warnings should the voting client detect that the user lacks antivirus or antispyware programs. Voters' worries can be further calmed by accessibility to the vendor's help and technical support lines where they can be directed to methods of removing malware. It may also be wise to limit the amount of time a voter may be logged in to the voter application to reduce the chance of exploitation.

If possible, it would be wise to limit the information accessible by NMap and Nessus scans. The less a hacker can determine through scans, the less vulnerable the voting servers are. In fact, the vendors may use deception; by this, they may not only dissuade attackers, but divert them into dead ends. Thus, informational scans can be used as a reverse means against potential attackers.

7. Conclusion

In conclusion, we found the vendors Vendor-1, Vendor-2, and Vendor-3 to be admirably secure. Though vulnerabilities were identified in our test, we were unsuccessful in our attempts to exploit and did not achieve compromised systems. Within this report we specified the value of the three voting system vendors on both their confidentiality as well as integrity of each system. We identified low and medium level securities including an open SSH line and information about the machines running the systems. We discovered these threats by conducting reconnaissance and gaining physical access to the three vendor's end kiosk clients, and we elaborated on their impact in this document. Lastly, we suggested recommended controls on these systems such as limiting the amount of time on the servers and possibly the amount of information available on scanning tools open to the public such as Nessus and NMap. The logs of our attacks and scans are shown below in Appendix A and B, respectively.

Appendix A

Penetration Test Time Log

Vendor-3 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address [redacted]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
845	Scanned the internal voting workstation at [redacted] using Nessus		D
848	Scanned the external vendor web server at [redacted] using Nessus	See Appendix B for report of vulnerabilities	D
852	Ran internal scan on [redacted] using Nessus		A
900	Retrieved voting system web address	https:// [redacted]	A
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
913	Scanned the internal voting workstation at [redacted] using Nmap		E
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A
920	Started Cain	Found a workgroup called VENDOR-3_INT with one XP computer named COMP023	C

[redacted]

930	Used command prompt to ping URL https:// [redacted]	Discovered the IP address of voting system server which is [redacted]	B
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
958	Ran a PHP meterpreter, Reverse TCP Incline exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1000	Ran a PHP meterpreter, Reverse TCP Sager exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1010	Ran a multi/handler SSL exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1030	Ran a vlc_smb_url msf exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1045	started intense, all tcp on Vendor-3 laptop	was interrupted	F
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1125	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
1130	Scanned [redacted] using an intense scan with Nmap		B
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1302	tried to visit Vendor-3.com	failed-timed out	F
1305	Used Maltego and began running all transforms on Vendor-3.com	results gathered; no salient breakthroughs	F
1316	started nmap -T4 -A -v -PN [redacted] Vendor-3.com	started	F
1320	nMap completed	results saved, some interesting data, few conclusive, no breakthroughs	F
1330	Ran a SQL injection scan on voting system website using Webcruiser		B

[redacted]

1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1406	Attempted to scan range of IP addresses for network which the voting system web server is located [redacted] using Nmap	Scan never completed	E
1430	Ran scan on web server [redacted] using Nmap		B
1449	Scanned the external IP [redacted] using Nessus	No Vulnerabilities found	E
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-3 system is running Windows	B
1505	Scanned the external IP [redacted] using Nessus	See Appendix A for results	E

Date: 8/3/2011

Time	Action	Outcome	Team Member
900	Manually changed settings on voting workstation to allow remote desktop connection and added the user "Support" to list of users that may access it		A
951	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping	E
935	sent fake email to Vendor-3@Vendor-3.com as jason mulbrich, attempted to gain insight into workforce for social engineering	sent; no reply ever received	F
950	sent fake email to [redacted]@Vendor-3.com as "MS Outlook"	failed	F
958	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping	E
1000	Attempted to remote desktop into voting workstation	Unsuccessful connection	A
1000	Attempted to ping the internal voting workstation IP [redacted] using the command prompt	No response from the target IP address	A
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
1013	Attempted to ping the internal voting workstation IP [redacted] using the command prompt	Response back from targeted IP	E
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting workstation IP [redacted] using Armitage		B

[redacted]

1322	sqlite3 db_nmap scan of Vendor-3 laptop in BT4	completed in 40s, results gathered as before	F
1323	db_autopwn -p -t -e of Vendor-3 laptop	completed in 6seconds no sessions	F
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1500	Scanned the external IP [redacted] using Nmap		B

Date: 8/4/2011

Time	Action	Outcome	Team Member
816	Scanned the internal voting workstation IP [redacted] using Nmap -p 1-65535 command on Nmap		B
826	Scanned the internal voting workstation IP [redacted] using Nmap -5T -A -v command on Nmap		B
1000	started nmap scan of Vendor-3 server, intence scan no ping except -T4 changed to -T2 for stealth	started	F
1002	prematurely stopped nessus scan of Vendor-3 server (started about 30 mins prior)	results gathered, 14 vulnerabilities 1 med 13 low	F
1030	nmap scan of Vendor-3 server done	results lost… zenmap crashed	F
1052	nmap scan of Vendor-3 server again, intense scan no ping -T2	started	F
1054	nmap scan of Vendor-3 server done	results saved	F

[redacted]

Vendor-1 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:// [redacted]	C
820	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [redacted]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [redacted]	D
820	Vendor-1 laptop voting server: attempt SQLI 'or''1'='1'*/ 'or''1'='1'{('or''1'='1'(/	invalid	F
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
850	Ran internal scan on [redacted] using Nessus		A
851	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [redacted]	D
855	Scanned the external vendor web server at [redacted] using Nessus	No Vulnerabilities found	D
900	Retrieved voting system web address	https:// [redacted]	A
900	Gathered URL for voting site	https:// [redacted]	B
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
900	Used command prompt to ping the URL https:// [redacted]	Discovered the IP address of voting system server which is [redacted]	B
900	Used PuTTY to connect to port 22 (SSH) on vendor web server	Received a prompt for login	D
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *-u Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

[redacted]

920	Went to http://testbed.Vendor-1.com/robots.txt in web browser	Browser displayed- user-agent: * Disallow: /	E
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
957	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
958	Ran a web app scan on voting site using Nessus	No Vulnerabilities found	E
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1000	Used autopwn consisting of over 100 exploits on the web server [redacted] in order to establish a connection	No successful connection made	C
1005	nessus scan against server complete	2 low vulnerabilities	F
1005	Lost connection with voting site		E
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1040	Scanned the external web server IP [redacted] using Nmap	See Appendix B for results	D
1050	Scanned the external web server IP [redacted] using Nessus	See Appendix B for results	D
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1130	Scanned [redacted] using an intense scan with Nmap		B
1134	Scanned the internal voting workstation at IP [redacted] using Nessus		D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B

[redacted]

1420	Discovered administrative login page for Vendor-1.com	The administrative directory was listed in robots.txt for the website; Login page was a website built with Joomla software; Noted webpage source code uses Joomla 1.5	C
1430	Ran scan on web server [redacted] using Nmap		B
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-1 voting system is running Linux	B
1500	Attempted the Joomla 1.5 password reset token vulnerability on administrative login page	Failed attempt- website was patched to prevent this	C
1530	attempted metasploit psexec on EC laptop	no reply	F
1540	Ran a Joomla automated attack tool on the administrative login page	No Vulnerabilities found	C

Date: 8/3/2011			
Time	Action	Outcome	Team Member
850	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping; Problem with laptop	E
900	Used Vendor-1.com/index.php?option=com_NAME to see if webpage returned a 404 error or blank page	only component found: com_jce	C
900	Found a vulnerability for the com_jce componentvia Exploit-DB	SQL injection failed- the vulnerability was patched; continued running Hydra remote bruteforce	C
908	Scanned the internal voting workstation IP [redacted] using stealthy scan in Nmap		D
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting wokstation IP [redacted] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1440	Remote SSH puTTY attempt into Vendor-1 server [redacted]	opened login screen, attempted root and five passwords; failure	F
1500	Scanned the external IP range [redacted] using Nmap		B

[redacted]

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP : [redacted] using Nmap -p 1-65535 command on Nmap		B

[redacted]

Vendor-2 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:/ [redacted]	C
820	Pinged URL to retrieve external IP address	Discoved the IP address of voting system server which is [redacted]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [redacted]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command *ipconfig*in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [redacted]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [redacted]	B
850	Ran external scan on [redacted] using Nessus	Had open ports: 22, 80, 443	C
850	Used PuTTY to try and connect to Port 22 (SSH) on [redacted]	Received Login Prompt	C
853	Ran internal scan on [redacted] using Nessus		A
900	Retrieved voting system web address	https:/ [redacted]	A
900	Used command *ping* [redacted] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
915	nessus scan run against Vendor-2 laptop, saved results	3 low vulnerabilites	0
900	Made basic login attempts within the login prompt received when connecting to Port 22 (SSH) on [redacted] with PuTTY: User Names- Admin, Administrator, root, user ; Passwords- blank, same input as username	No successful match	C
919	Downloaded PsTools for Windows and ran the command *psexec* \\ [redacted] *-u Support cmd*in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

[redacted]

930	Used Command promt to ping URL https:/ [redacted]	Discoved the IP address of voting system server which is [redacted]	B
935	Ran the command *mstsc*in command prompt	Unable to connect to and establish a remote desktop on [redacted]	A
940	Went to http:/ [redacted] in web browser	Discovered later that we wanted [redacted] instead of [redacted]	E
950	Began running Hydra to attempt to brute-force the Login dialog prompted wheb connecting to Port 22 (SSH) with PuTTY: Defined Usernames- Administrator, user, root ; Passwords- 1.7 million common passwords file	No successful match	C
1000	Ran external scan on [redacted] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command *windows/smb/psexec/reverse_tcp* in Metasploit	Failed to establish a connection	B
1030	Ran internal scan on [redacted] using Nessus	Low vulnerabilities reported	B
1038	attempted BT5 psexec exploit on Vendor-2 laptop	failed-timed out	F
1044	Ran a slow internal scan on the internal workstation IP [redacted] using Nmap	See Appendix B for results	E
1053	Scanned the external web server IP [redacted] using Nessus	See Appendix B for results	D
1055	Scanned the external web server IP [redacted] using Nmap	See Appendix B for results	D
1100	Ran scan on internal IP address [redacted] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1126	Ran exploit Windows/smb/ms09_050smb2 on internal voting workstation using Metasploit	Unable to exploit vulnerability	D
1130	Scanned [redacted] using an intense scan with Nmap		B
1135	Scanned the internal voting workstation at IP [redacted] using Nessus		D
1240	Pinged URL using command prompt to verify response from voting website	Successful response and verification of communication established	D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1312	Attempted to scan range of IP addresses for network which the voting system web server is located [redacted] using Nmap	Scan never completed	E

[redacted]

1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1430	Ran scan on web server [redacted] using Nmap		B
1500	Completed scan on web server [redacted] using Nmap	Discovered that the Vendor-2 system is running Linux	B
1540	Scanned the external IP [redacted] using Nessus	See Appendix B for results	E
1544	Scanned the external IP [redacted] using Nessus	No Vulnerabilities found	E

Date: 8/3/2011			
Time	Action	Outcome	Team Member
1000	Ran intense scan on the internal voting workstation IP [redacted] using Nmap		B
845	Attempted to ping internal workstation IP [redacted] using the command prompt	No response to ping; Problem with laptop	E
958	Scanned the internal voting workstation IP [redacted] using Nmap		D
1030	Ran scan on the internal voting workstation IP [redacted] using Nessus		B
1300	Ran scan on the internal voting workstation IP [redacted] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [redacted] using Armitage		B
1500	Scanned the external IP range [redacted] using intense scan in Nmap	No response to ping	B

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP [redacted] using Nmap -p 1-65535 command on Nmap		B

[redacted]

Appendix B

NMap Scans of Vendor Systems

Vendor-2 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:06:38 2011

Scan Summary [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:06:38 2011 with these arguments:
nmap -T4 -A -v -PE -PS?2,25,80 -PA21,2;3,BQ, [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Used port: 43127/udp (closed)
OS match: Microsoft Windows Server 2006 (66%)
OS match: Microsoft Windows Server 2006 R2 (66%)
OS match: Microsoft Windows Server 2006 SP1 (66%)
OS match: Microsoft Windows Server 2006 SP2 (66%)
OS match: Microsoft Windows 7 (66%)
OS match: Microsoft Windows 7 Professional (88%)
OS match: Microsoft Windows 7 Ultimate (88%)
OS match: Microsoft Windows Longhorn (66%)
OS match: Microsoft Windows Vista (66%)
OS match: Microsoft Windows Vista Business (88%)

Traceroute Information (dick to expand)
Mise Metrics (dick to expand)

[redacted]

Vendor-2 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:25:49 2011

Scan Summary 1 [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:25:49 2011 with these arguments:
nmap -T5 -A -v -Pn [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

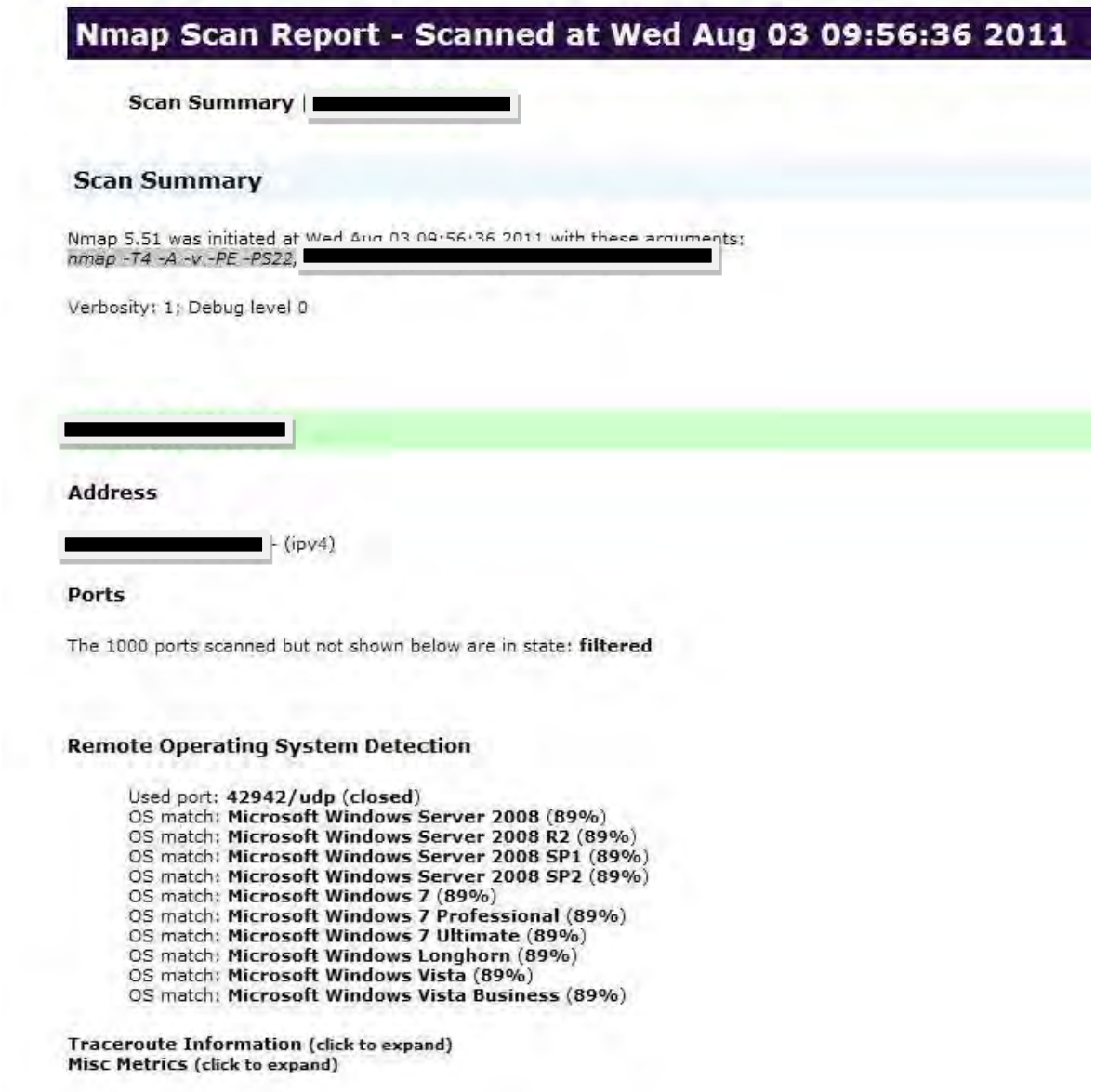
Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)
Mise Metrics (click to expand)

[redacted]

Vendor-1 Internal Computer Nmap Scan



Nmap Scan Report - Scanned at Wed Aug 03 09:56:36 2011

Scan Summary | [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 09:56:36 2011 with these arguments:
nmap -T4 -A -v -PE -PS22, [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Used port: **42942/udp (closed)**
OS match: **Microsoft Windows Server 2008 (89%)**
OS match: **Microsoft Windows Server 2008 R2 (89%)**
OS match: **Microsoft Windows Server 2008 SP1 (89%)**
OS match: **Microsoft Windows Server 2008 SP2 (89%)**
OS match: **Microsoft Windows 7 (89%)**
OS match: **Microsoft Windows 7 Professional (89%)**
OS match: **Microsoft Windows 7 Ultimate (89%)**
OS match: **Microsoft Windows Longhorn (89%)**
OS match: **Microsoft Windows Vista (89%)**
OS match: **Microsoft Windows Vista Business (89%)**

Traceroute Information (click to expand)
Misc Metrics (click to expand)

[redacted]

Vendor-1 ServerNmap Scan

Nmap Scan Report- Scanned at Thu Aug 04 09:25:06 2011

Scan Summary) lwdcdbo2.fa1 34.host4 . 24396 [redacted]

Scan Summary

Nmap S.Sl was initiated at Thu Aug 04 09:25:06 2011 with the-se arguments:
P"l<<l> *:::Ii .:A·v·Pn* ZJQ.JJ/$.4lj

Verbcsity:1: Debug level 0

[redacted] / lwdc.dbo.2.fa1-34.host4.24396 [redacted]

Address

[redacted] - (ipv4)

Hostnzames

lwdc. .dbo2.fa1- 34.host4.24396 [redacted] (PTR)

Ports

The 999 ports scanned but not shown below *are* in state: fittered

State (togle dosed (0) I filtered (OJ)	Product
o n	Aj>ache httpd

Remote Operating System Detection

use<! port: 443/tcp (open)
OS match: Unux x.x.x- x.x.xx (94%)
OS match: Unux x.x.x- x.x.xx (92%)
OS match: Unux x.x.x - x.x.xx (89%)
OS match: Linux x.x.xx (ContOS 5, x86_64, SHP) (89%)
OS match: ZoneAiarm Z100G WAP (89%)
OS match: linux x.x.xx (CentOS 5.2) (88%)
OS metch: Unwc x.x.x- xxx.stabxxx.xx-enterpri.se (CentOS 4.2 x:86} (86%)
OS match: Unux x.x. xx - x.x.xx
(88%) OS match: Unux x.x.xx (88%)
OS match: Unux x.x.xx (Centos 5.3) (88%)

Traceroute Information (dick to expaod)
HIsc Metrics (dick to expand)

[redacted]

Vendor-3 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:12:33 2011

Scan Summary : [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:12:33 2011 with these arguments:
oma R -T4 -A -v -PE -PSZ2 _ 80 -PA21.2J,S0,338 [redacted] -i!IO

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] - (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Used port: 40114/udp (closed)
OS match: Microsoft Windows Server 2008 (89%)
OS match: Microsoft Windows Server 2008 R2 (89%)
OS match: Microsoft Windows Server 2008 SP1 (89%)
OS match: Microsoft Windows Server 2008 SP2 (89%)
OS match: Microsoft Windows 7 (89%)
OS match: Microsoft Windows 7 Professional (89%)
OS match: Microsoft Windows 7 Ultimate (89%)
OS match: Microsoft Windows longhorn (89%)
OS match: Microsoft Windows Vista (89%)
OS match: Microsoft Windows Vista Business (89%)

Traceroute Information (dick to expand)
Mise Metrics (dick to expand)

[redacted]

Vendor-3 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:28:30 2011

Scan Summary 1 [redacted]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:28:30 2011 with these arguments:
nmap -T5 -A -v -Pn [redacted]

Verbosity: 1; Debug level 0

[redacted]

Address

[redacted] (ipv4)

Ports

The 999 ports scanned but not shown below are in state: filtered

State (toggle dosed (0]1 filtered (OJ)
open

Remote Operating System Detection

Used port: 443/tcp (open)
OS match: HP 170X print server or Inkjet 3000 printer (94%)
OS match: Crestron XPanel control system (900/o)
OS match: Netgear OG834G WAP (90%)
OS match: Nintendo Wii game console (860/o)
OS match: VodaviXTS-IP PBX (86%)
OS match: Brother MFC-7620N multifunction printer (65%)
OS match: Microsoft Xbox game console {modified, running XboxMediaCenter) (SSOJo)
OS match: Hirschmann L2E Railswitch (85%)

Traceroute nformation (dick to expand)
Mise Metrics (click to expand)

[redacted]

Nessus Scans of Vendor Servers

1. Vendor-2 System Server:

[redacted]

1.1 Port 0- TCP

1.2. Port 0- UDP

[redacted]

2. Vendor-1 Server:

[redacted]

2.1. Port 0- TCP

2.2. Port 0- UPD

[redacted]

2.3 Port 80- TCP

2.4. Port 443- TCP

[redacted]

3. Vendor-3 Server:

3.1. Port 0 – TCP

3.2. Port 0- UDP

3.3. Port 21-TCP

3.4. Port 25- TCP

3.5. Port 53- TCP

[redacted]

3.6. Port 443- TCP

3.7. Port 993- TCP

[redacted]

3.8. Port 5432- TCP