

Project report on **Penetration Testing**

sopra  steria

Undertaken at:

Noida

03-07-18 – 31-07-18

Submitted by: **Kartik Jaitly**
Btech. Information Technology

Under the guidance of: **Mrs. Bharti Dubey**
Infrastructure Lead
Sopra Steria Group
Noida

Acknowledgements

It is my proud privilege to express my profound gratitude to the entire management of Sopra Steria group for giving me this opportunity.

I am grateful to Mrs. Bharti Dubey for her astute guidance, constant encouragement and sincere encouragement and sincere support for this project work.

I would like to thank Sopra Steria for providing me with an opportunity to pursue my training, as it is an important part of the Btech course and it is the one that exposes you to industry standards and makes you adapt yourself to the latest trends and technologies. At the same time, it gives an experience of working on a project.

I feel pride and privileged in expressing my deep sense of gratitude to all those who have helped me in presenting this assignment. I would be failing in my endeavor if I do not place my acknowledgement.

About Sopra Steria

Sopra Steria, a European leader in digital transformation, provides one of the most comprehensive portfolios of end-to-end service offerings on the market: consulting, systems integration, software development, infrastructure management and business process services. Sopra Steria is trusted by leading private and public-sector organizations to deliver successful transformation programmes that address their most complex and critical business challenges. Combining high quality and performance services, added value and innovation, Sopra Steria enables its clients to make the best use of digital technology.

Table of Contents

Acknowledgements.....	I
Certificate.....	II
About Sopra Steria.....	III
Abstract.....	IV
Hardware and Software.....	V
Introduction.....	VI
Warning and Disclaimer.....	1
Document details.....	2
Summary, project scope.....	5
Timeline, Risk and Recommendations.....	5-7
Testing Methodology.....	7
Challenge 1 – Information Gathering.....	8-9
Challenge 2 – Network Scanning.....	10-18
Challenge 3 – OS Fingerprinting.....	19-20
Challenge 4 – Gaining Access.....	21-24
Challenge 5 – Erasing Tracks.....	25-27
Conclusions.....	VII
References and Bibliography	VIII

Abstract

This issue of security is very paramount in any organization, especially in today's digital age. Information Security is becoming graver in today world. And the first step to be taken towards it is by doing penetration testing of the organization's existing systems and networks, identifying the vulnerabilities and coming up with counter measures to cope up with these security flaws in the organization. Throughout this project I have learned the various tools to collect the necessary information, identify such vulnerabilities, identifying the exploits and break into the systems.

And finally coming up with the necessary and industry best practices to improve upon the security risks in the organization.

Hardware and Software

The hardware and software used are listed as follows:

- Hardware: The hardware of the system includes :
 1. 12 GB RAM
 2. Intel Core i5 Processor
- Software : The software used include majorly VM Ware, Metasploit, Armitage, SET Toolkit and various other Penetration Testing tools.

Introduction

This project is done by creating a lab environment on VM Ware. There is a small network system of several systems with different Operating System versions connected through internal network considered as the company's internal network and also connected to the internet. Penetration Testing is about trying to get into the organization through agreed upon testing tools. This project is completed in 5 major phases:

1. Foot printing and Reconnaissance: Reconnaissance is the act of gathering preliminary data or intelligence on your target. The data is gathered in order to better plan for your attack. Reconnaissance can be performed actively (meaning that you are directly touching the target) or passively (meaning that your recon is being performed through an intermediary).
2. Network Scanning and Service Enumeration: The phase of scanning requires the application of technical tools to gather further intelligence on your target, but in this case, the Intel being sought is more commonly about the systems that they have in place. A good example would be the use of a vulnerability scanner on a target network.
3. OS Fingerprinting: Operating System (OS) fingerprinting is the process of learning what operating system is running on a target device.
4. Gaining Access: Phase 3 gaining access requires taking control of one or more network devices in order to either extract data from the target, or to use that device to then launch attacks on other targets.
5. Covering Tracks: The final phase of covering tracks simply means that the attacker must take the steps necessary to remove all semblance of detection. Any changes that were made, authorizations that were escalated etc. all must return to a state of non-recognition by the host network's administrators.

I in this project have used Kali linux based machine as the testing machine to complete these phases.

PENETRATION TESTING FOR AAB LTD.

Warning:

This document and accompanying material is highly confidential and consists of highly critical information about the company. This document, and all accompanying materials, should be safeguarded at all times and maintained in a secure area when not in use. KJXSecurity assumes no responsibility or liability for the security of this document or any accompanying materials after delivery to the organization named herein. It is the organization's responsibility to safeguard this material after delivery.

Disclaimer:

The recommendations provided by KJX Security LLC, are in accordance to the best practices in the industry and might not take into account the changing and mitigating circumstances. Even if correctly applies cause conflicts on different operating systems. The recommendations should be tested out first in a non-production environment and then applied to the production systems.

KJX Security

INDIA

#8585983442

Document Details:

Document Title	Penetration Testing Report
Company	KJX Security
Recipient	AAB Ltd.
Date	July 2018
Classification	Confidential
Document Type	Report
Version	1.3
Author	Kartik
Pen Testers	Kartik
Reviewed By	Adam
Approved By	Adam

Version History Information:

Date	Version	Author	Comments
July 2018	v1.3	Kartik	Final Draft
July 2018	v1.2	Kartik	Checked for formatting and proofreading
July 2018	v1.1	Kartik	Edited and made changes to content

Recipient:

Name	Title	Company
Adam	Penetration Testing Report	ABB Ltd.

Summary:

This is a penetration testing conducted on the internal network and systems of the company AAB Ltd.

Project Scope:

The assessment performed was focused on AAB Ltd.'s internal network and its related application infrastructure. This result is intended to be an overall assessment of AAB Ltd. network, and those systems and subnets that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

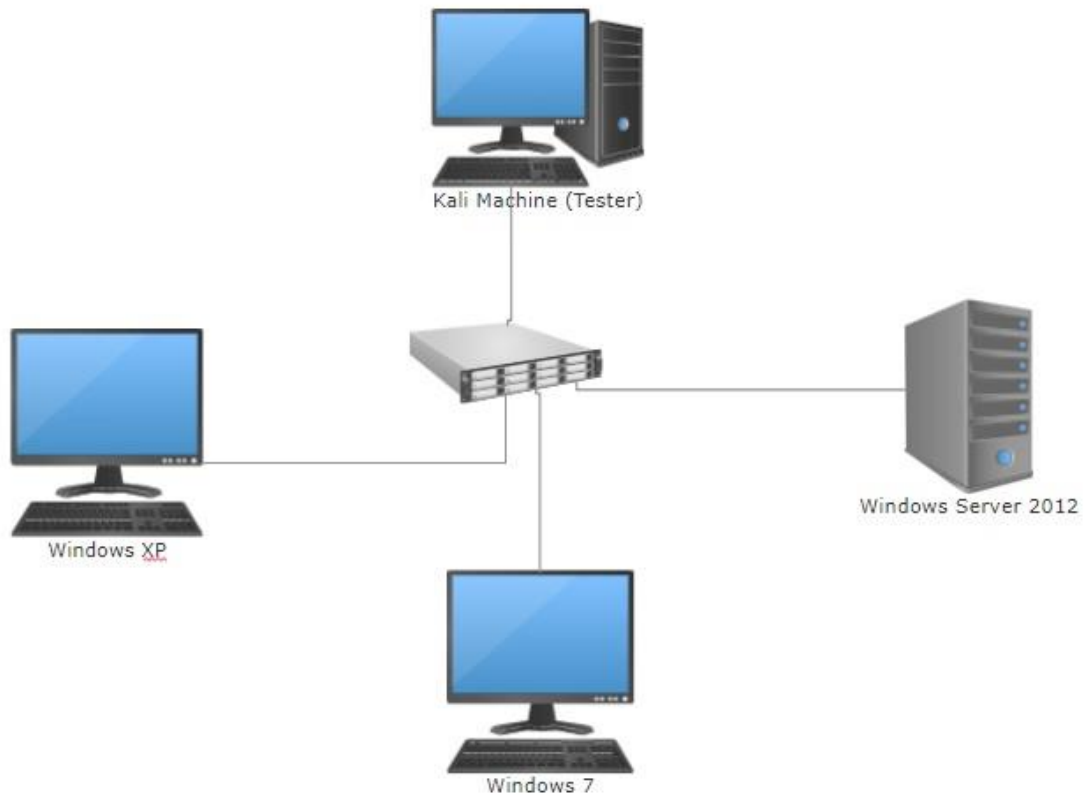
Project Objective:

The objective of AAB Ltd.'s network and application assessment is to determine the overall security by analyzing all possible transactions, user input variables, and application components that reside on network systems. For the testing, we attempted to perform a black-box test.

The objective of the security assessment and penetration test of the network infrastructure supporting the application is to determine the overall security of the network segments and hosts within the scope of the engagement.

Target Systems:

Target System Name	AAB Ltd.
Target System URL	http://aab.com
Test Type	Penetration Testing
IP Addresses Discovered	192.168.32.130, 192.168.32.128, 192.168.32.129
Network Details	Client-server
Web Server	192.168.32.130,
System Configuration	Intel core i5, 64-bit, 2.67GHz



Assumptions:

We assumed that all IP addresses are public IP addresses and the organization has implemented the security policies available with them.

Timeline:

Categories	Initiation Date/Time	Completion Date/Time
Foot printing and Reconnaissance	July 3	July 13
Network and Host Scanning	July 16	July 18
Enumeration	July 19	July 22
Exploitation	July 23	July 26
Post Exploitation	July 27	July 29
Clean-up	July 30	July 31

Risk Rating levels and Assessment Metrics:

5 Stars	*****	Critical	Intruders can easily gain control of hosts and network. This needs immediate attention.
4 Stars	****	High	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. This should be addressed as soon as possible.
3 Stars	***	Elevated	This could result in potential misuse of the host by intruders. Address this at your convenience but do as soon as possible.
2 Stars	**	Moderate	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Address this the next time you perform a minor reconfiguration of the host.
1 Stars	*	Low	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. Address this the next time you perform a major reconfiguration of the host.

L	Low	1-4
M	Medium	4-12
H	High	12-25

Summary of Findings:

Value	Number of Risks
Low	2
Medium	3
High	4

Summary of Recommendations:

1.1.1. Personnel Awareness

It was found out that an organization as big as AAB Ltd. Having a lot of employees results in Security Vulnerabilities due to lack of awareness. Hence, I recommend to improve the overall awareness of digital security threats in the organization.

1.1.2. Policies and Procedures

Security Policies and Procedures are recommended to be over viewed again and again due to ever rising security threats.

1.1.3. Critical Vulnerabilities

Critical Vulnerabilities are to be catered to immediately and the recommendation on each one is according to the Best Practices in the Industry and could change during the course of implementations of the said changes. KJX Security doesn't imply any responsibility to production or data loss during implementation.

1.1.4. Identification and Authentication

The identification and authentication is very important for the organization's security. The credentials holders should be authorized and authenticated to the data and information they need according to their role in the organization.

1.1.5. Intrusion Detection

KJX Security would suggest the best practices in intrusion detection of the network of the company. KJX Security doesn't imply any responsibility to production or data loss during implementation.

Testing Methodology:

Planning

During the planning, we gather information from the server in which the web application is installed. Then, we detect the path information and identifiable software and determined the running their versions.

Exploitation

Utilizing the information gathered during the planning, we start to find the vulnerability for each piece of software and service that we discovered after that trying to exploit it. All the exploitation attacks used in the Penetration Testing are in accordance with the checklist created during service agreement.

Reporting

Based on the results from the first two steps, we start analyzing the results. Our risk rating is based on this calculation:

Risk = Threat * Vulnerability * Impact

After calculating the risk rating, we start writing the report on each risk and how to mitigate it.

Comprehensive Technical Report

[Challenge 1:] Information Gathering:

Threat Description: Information gathering provides an indicator of the amount of organizational information available in the public domain that could help an attacker compromise the network. We obtained Internet Protocol (IP) address blocks assigned to the organization and queried for other indications of IP address ownership. We searched the organization's web site and used Internet search engines to obtain the organization's addresses, business hours, telephone and fax numbers, contact and e-mail addresses, privacy and security policies in place, links to other web sites or servers, employee names and information, product or technology endorsements and examples of organizational letterhead or officer signatures. We looked for electronic articles and newsgroup postings relating to partners, merger/acquisition news, network infrastructure equipment and application help requests.

Category: Authorization

Tools Used: Maltego CS

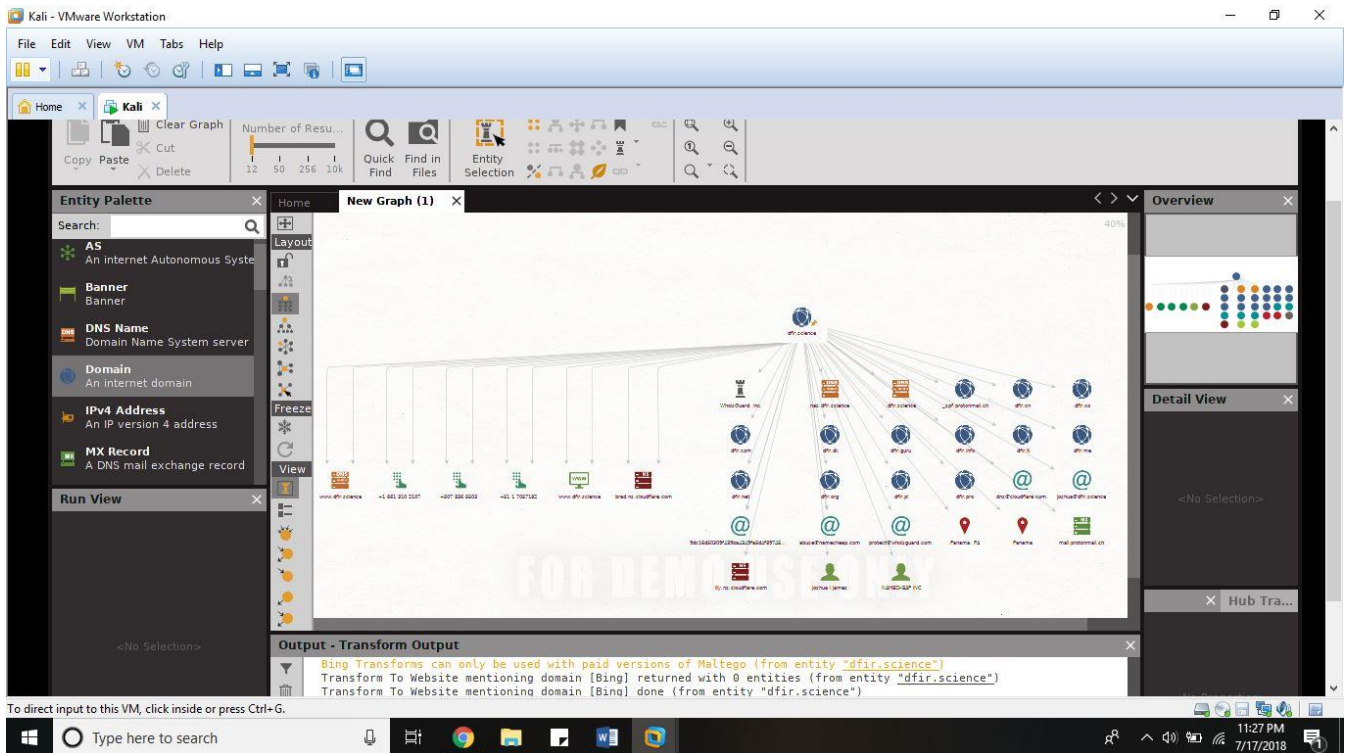
Vendor: Paterva

Methodology:

We used maltego CS for gathering information about the website or domain based of the entity we start with it shows all the relevant and non-relevant information about the domain name given to it and creates an informative graph about the findings.

Here we gather some information about the owner of the website www.dfir.science.

After the transforms are run on the above information the following graph is made. And information such as name, email address, hosting company, place of hosting and some telephone numbers appear along with some irrelevant domains.



[Challenge 2:] Network Scanning and Service Enumeration

Category: Authorization

Vendor Reference: Nmap 7.60

Threat Description:

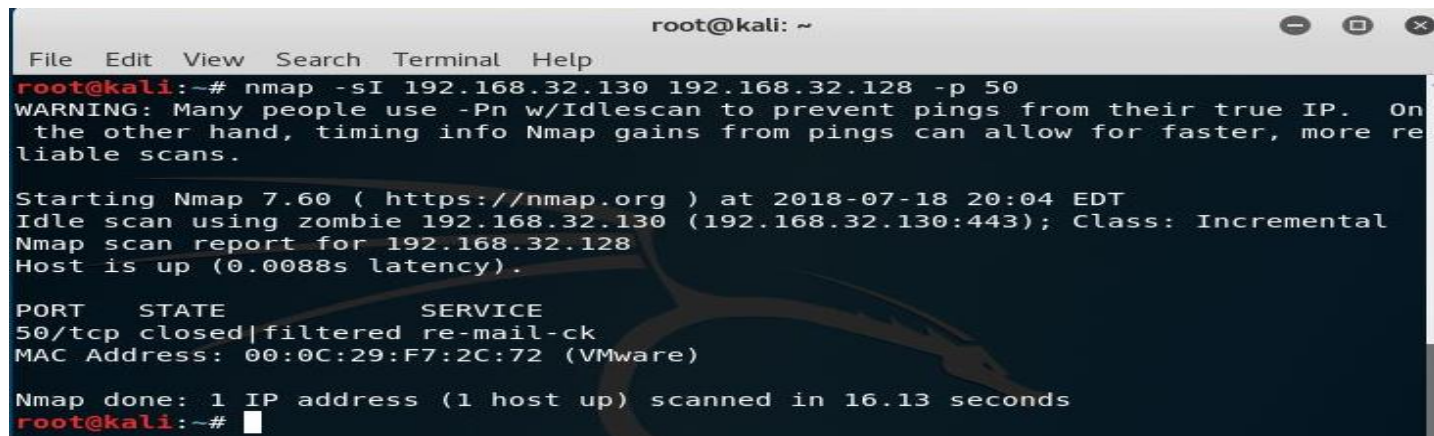
Once we identified the target system and completed the initial reconnaissance, as discussed in the above step, we started looking for a mode of entry into the target system. We conducted network scanning on IP addresses [] authorized for scanning by the organization on/from July 2018. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more about the target system by finding out what operating system is used, what services are running, and whether or not there are any configuration lapses in the target system. The attacker then tries to form an attack strategy based on facts learned during the scan.

Methodology:

Our tests were configured not to cause an intentional Denial of Service condition in a well-maintained network. This is normal when the IP address is not in use, the host assigned to the IP address is turned off, or a network protection device such as a firewall prevents scanning the host.

After repeated scanning, primarily with Nmap, and using hping of the IP addresses, we discovered following live hosts in the target network.

Nmap – Idle Scan



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sI 192.168.32.130 192.168.32.128 -p 50  
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On  
the other hand, timing info Nmap gains from pings can allow for faster, more re  
liable scans.  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-18 20:04 EDT  
Idle scan using zombie 192.168.32.130 (192.168.32.130:443); Class: Incremental  
Nmap scan report for 192.168.32.128  
Host is up (0.0088s latency).  
  
PORT      STATE      SERVICE  
50/tcp    closed|filtered re-mail-ck  
MAC Address: 00:0C:29:F7:2C:72 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 16.13 seconds  
root@kali:~#
```

No.	Time	Source	Destination	Protocol	Length	Info
315	609.294723	192.168.32.130	192.168.32.128	SMB	93	Tree Disconnect Request
316	609.294784	192.168.32.128	192.168.32.130	SMB	93	Tree Disconnect Response
317	609.295535	192.168.32.130	192.168.32.128	TCP	60	1045 → 139 [FIN, ACK] Seq=1850 Ack=1896 Win=63808 Len=0
318	609.295597	192.168.32.128	192.168.32.130	TCP	54	139 → 1045 [FIN, ACK] Seq=1896 Ack=1851 Win=63936 Len=0
319	609.296044	192.168.32.130	192.168.32.128	TCP	60	1045 → 139 [ACK] Seq=1851 Ack=1897 Win=63808 Len=0
320	610.459089	192.168.32.128	192.168.32.255	BROWSER	243	Local Master Announcement WIN-T60IRSJ7D9N, Workstation, Server, N...
321	614.332399	Vmware_75:2d:4a	Vmware_ee:60:48	ARP	60	Who has 192.168.32.254? Tell 192.168.32.131
322	614.332404	Vmware_ee:60:48	Vmware_75:2d:4a	ARP	60	192.168.32.254 is at 00:50:56:ee:60:48
323	651.204857	fe80::41e1:b6c:439d...	ff02::1:2	DHCPv6	157	Solicit XID: 0x40119d CID: 0001000122db127d000c295f3d0b
324	652.217824	fe80::41e1:b6c:439d...	ff02::1:2	DHCPv6	157	Solicit XID: 0x40119d CID: 0001000122db127d000c295f3d0b

Nmap – Full Scan

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sT 192.168.32.128 -p 21

Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-18 20:11 EDT
Nmap scan report for 192.168.32.128
Host is up (0.00035s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
MAC Address: 00:0C:29:F7:2C:72 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@kali:~#

```

No.	Time	Source	Destination	Protocol	Length	Info
66	43.627232	192.168.32.128	192.168.32.130	SMB	97	Logoff AndX Response
67	43.627847	192.168.32.130	192.168.32.128	SMB	93	Tree Disconnect Request
68	43.627917	192.168.32.128	192.168.32.130	SMB	93	Tree Disconnect Response
69	43.628801	192.168.32.130	192.168.32.128	TCP	60	1048 → 139 [FIN, ACK] Seq=1850 Ack=1896 Win=63808 Len=0
70	43.628862	192.168.32.128	192.168.32.130	TCP	54	139 → 1048 [FIN, ACK] Seq=1896 Ack=1851 Win=63936 Len=0
71	43.629259	192.168.32.130	192.168.32.128	TCP	60	1048 → 139 [ACK] Seq=1851 Ack=1897 Win=63808 Len=0
72	47.959178	192.168.32.131	192.168.32.128	TCP	74	43876 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=418...
73	48.068551	192.168.32.131	192.168.32.128	TCP	74	43878 → 21 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=418...
74	71.219612	192.168.32.131	192.168.32.254	DHCP	342	DHCP Request - Transaction ID 0x4791f813
75	71.219725	192.168.32.254	192.168.32.131	DHCP	342	DHCP ACK - Transaction ID 0x4791f813

Nmap-Half Stealth Scan

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.32.128 -p 21  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-18 20:14 EDT  
Nmap scan report for 192.168.32.128  
Host is up (0.00031s latency).  
  
PORT      STATE      SERVICE  
21/tcp    filtered  ftp  
MAC Address: 00:0C:29:F7:2C:72 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds  
root@kali:~#
```

Capturing from Local Area Connection 2

No.	Time	Source	Destination	Protocol	Length	Info
78	192.153285	Vmware_75:2d:4a	Broadcast	ARP	60	Who has 192.168.32.128? Tell 192.168.32.131
79	192.153316	Vmware_f7:2c:72	Vmware_75:2d:4a	ARP	42	192.168.32.128 is at 00:0c:29:f7:2c:72
80	192.154353	192.168.32.131	192.168.32.1	DNS	87	Standard query 0x07c4 PTR 128.32.168.192.in-addr.arpa
81	196.158204	192.168.32.131	192.168.32.1	DNS	87	Standard query 0x07c5 PTR 128.32.168.192.in-addr.arpa
82	197.235750	Vmware_c0:00:01	Vmware_75:2d:4a	ARP	60	192.168.32.1 is at 00:50:56:c0:00:01
83	197.235753	Vmware_75:2d:4a	Vmware_c0:00:01	ARP	60	Who has 192.168.32.1? Tell 192.168.32.131
84	200.165937	192.168.32.131	192.168.32.1	DNS	87	Standard query 0x07c6 PTR 128.32.168.192.in-addr.arpa
85	205.182565	192.168.32.131	192.168.32.128	TCP	60	42694 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
86	205.290316	192.168.32.131	192.168.32.128	TCP	60	42695 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
87	221.696387	fe80::41e1:b6c:439d...	ff02::1:2	DHCPv6	157	Solicit XID: 0x8711b1 CID: 0001000122db127d000c295f3d0b

Nmap- ACK Scan

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sA 192.168.32.128 -p 21  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-18 20:16 EDT  
Nmap scan report for 192.168.32.128  
Host is up (0.00042s latency).  
  
PORT      STATE      SERVICE  
21/tcp    filtered  ftp  
MAC Address: 00:0C:29:F7:2C:72 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds  
root@kali:~#
```

Capturing from Local Area Connection 2

No.	Time	Source	Destination	Protocol	Length	Info
102	307.477597	Vmware_f7:2c:72	Vmware_75:2d:4a	ARP	42	192.168.32.128 is at 00:0c:29:f7:2c:72
103	307.478617	192.168.32.131	192.168.32.1	DNS	87	Standard query 0xbfd4 PTR 128.32.168.192.in-addr.arpa
104	311.481157	192.168.32.131	192.168.32.1	DNS	87	Standard query 0xbfd5 PTR 128.32.168.192.in-addr.arpa
105	312.691698	Vmware_c0:00:01	Vmware_75:2d:4a	ARP	60	192.168.32.1 is at 00:50:56:c0:00:01
106	312.691700	Vmware_75:2d:4a	Vmware_c0:00:01	ARP	60	Who has 192.168.32.1? Tell 192.168.32.131
107	315.485841	192.168.32.131	192.168.32.1	DNS	87	Standard query 0xbfd6 PTR 128.32.168.192.in-addr.arpa
108	320.502565	192.168.32.131	192.168.32.128	TCP	60	34555 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
109	320.610135	192.168.32.131	192.168.32.128	TCP	60	34556 → 21 [ACK] Seq=1 Ack=1 Win=1024 Len=0
110	323.750216	fe80::9561:1b9d:7c1...	ff02::1:2	DHCPv6	157	Solicit XID: 0x7aaa8a CID: 0001000122db05da000c29f72c68
111	374.884329	192.168.32.130	192.168.32.255	BROWSER	243	Host Announcement KARTIK-F908DF89, Workstation, Server, NT Workstatio...

Nmap-RST Scan

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sV 192.168.32.128 -p 21  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-18 20:19 EDT  
Nmap scan report for 192.168.32.128  
Host is up (0.00031s latency).  
  
PORT      STATE      SERVICE VERSION  
21/tcp    filtered  ftp  
MAC Address: 00:0C:29:F7:2C:72 (VMware)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds  
root@kali:~#
```

Capturing from Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
203	522.483495	192.168.32.131	192.168.32.1	DNS	87	Standard query 0xbf45 PTR 128.32.168.192.in-addr.arpa
204	523.635271	Vmware_c0:00:01	Vmware_75:2d:4a	ARP	60	192.168.32.1 is at 00:50:56:c0:00:01
205	523.635274	Vmware_75:2d:4a	Vmware_c0:00:01	ARP	60	Who has 192.168.32.1? Tell 192.168.32.131
206	526.499143	192.168.32.131	192.168.32.1	DNS	87	Standard query 0xbf46 PTR 128.32.168.192.in-addr.arpa
207	531.515983	192.168.32.131	192.168.32.128	TCP	60	38560 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
208	531.623685	192.168.32.131	192.168.32.128	TCP	60	38561 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
209	550.009192	Vmware_b7:06:20	Broadcast	ARP	60	Who has 192.168.32.254? Tell 192.168.32.130
210	550.009273	Vmware_ee:60:48	Vmware_b7:06:20	ARP	60	192.168.32.254 is at 00:50:56:ee:60:48
211	550.009325	192.168.32.130	192.168.32.254	DHCP	361	DHCP Request - Transaction ID 0xe0086496
212	550.009525	192.168.32.254	192.168.32.130	DHCP	342	DHCP ACK - Transaction ID 0xe0086496

Tool Name: Nessus

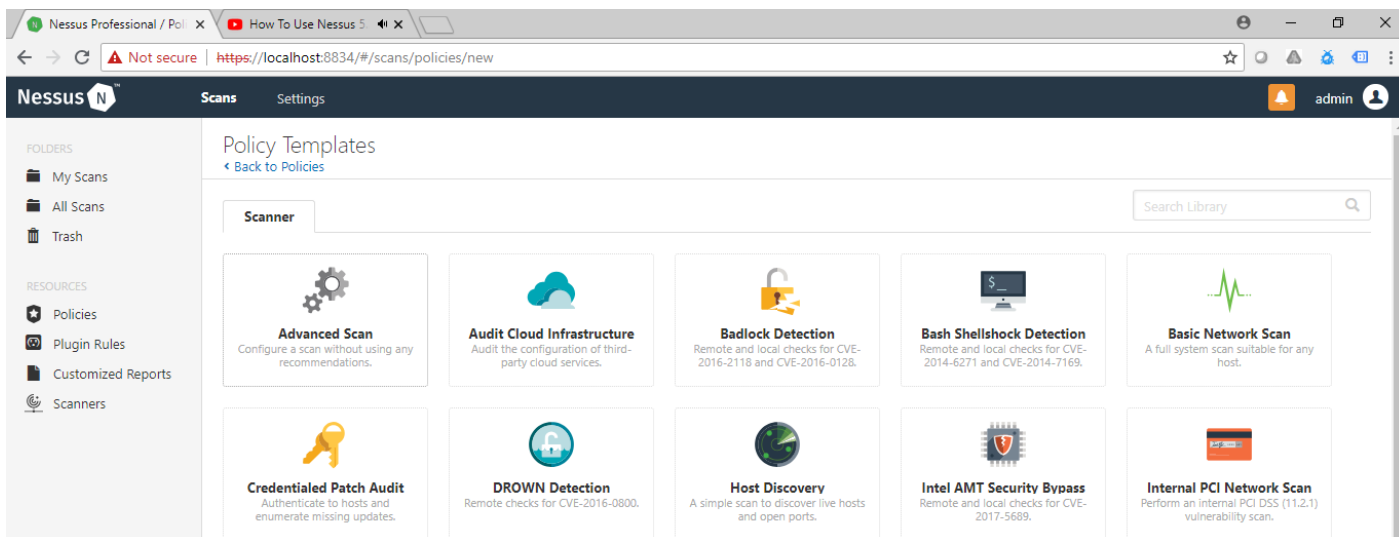
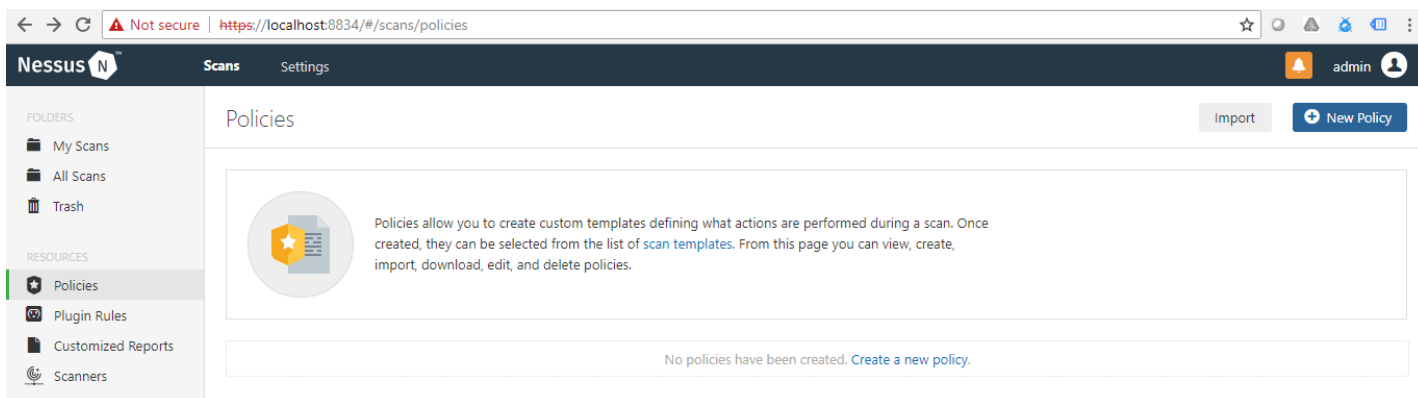
Vendor Reference: Tenable

Methodology:

After setting up Nessus, we log onto the web client using local host 8834 and create a new policy under the policies option. After creating the policy, we schedule a new scan and set the policy to the prior set Basic Scan. We click on launch Scan now and let it run. On completion we can see various types of vulnerabilities with detailed description of the threat level and available exploits. Follow the screenshots and the pdf attached in this document.



Basic_Scan_2n3fgt.pdf



← → ↻

Not secure | https://localhost:8834/#/scans/folders/my-scans

☆ 🔔 🛡️ 📄

Nessus

Scans Settings

🔔 admin

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

My Scans

Import New Folder New Scan

Search Scans

1 Scan

<input type="checkbox"/>	Name	Schedule	Running	Last Modified
<input type="checkbox"/>	Basic Scan	On Demand	<div>🔄 Today at 4:17 PM</div>	⏸

Basic Scan

[Back to My Scans](#)

Configure Audit Trail Launch Export

Hosts 6 Vulnerabilities 61 History 1

Filter Search Hosts 6 Hosts

<input type="checkbox"/>	Host	Vulnerabilities	
<input type="checkbox"/>	192.168.32.1	<div><div>7</div><div>92</div></div>	×
<input type="checkbox"/>	192.168.32.128	<div><div>2</div><div>32</div></div>	×
<input type="checkbox"/>	192.168.32.130	<div><div>4</div><div>2</div><div>26</div></div>	×
<input type="checkbox"/>	192.168.32.129	<div><div>2</div><div>30</div></div>	×
<input type="checkbox"/>	192.168.32.131	<div><div>5</div></div>	×
<input type="checkbox"/>	192.168.32.254	<div><div>1</div><div>3</div></div>	×

Scan Details

Name: Basic Scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:14 PM
End: Today at 4:39 PM
Elapsed: 25 minutes

Vulnerabilities



Back to My Scans

Configure Add Hosts Launch Export

Hosts 6 Vulnerabilities 61 History 1

Filter Search Vulnerabilities 61 Vulnerabilities

Sev	Name	Family	Count	
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB...	Windows	2	
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1	
CRITICAL	Microsoft Windows XP Unsupported Installation Detecti...	Windows	1	
CRITICAL	Unsupported Windows OS	Windows	1	
HIGH	SSL Version 2 and 3 Protocol Detection	Service detection	1	
MEDIUM	SMB Signing not required	Misc.	4	
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote ...	Windows	2	
MEDIUM	SSL Certificate Cannot Be Trusted	General	2	
MEDIUM	Microsoft Windows SMB NULL Session Authentication	Windows	1	
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1	

Scan Details

Name: Basic Scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 4:14 PM
End: Today at 4:39 PM
Elapsed: 25 minutes

Vulnerabilities



Plugin Details

Severity: Critical
ID: 97833
Version: 1.18
Type: remote
Family: Windows
Published: March 20, 2017
Modified: July 16, 2018

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.7
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 14, 2017
Vulnerability Pub Date: March 14, 2017

CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server (4013389...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

Scans Settings

admin

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, 10, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

<https://technet.microsoft.com/library/security/MS17-010>
<http://www.nessus.org/u?321523eb>
<http://www.nessus.org/u?7bec1941>
<http://www.nessus.org/u?d9f569cf>
<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
<https://support.microsoft.com/en-us/kb/2696547>
<http://www.nessus.org/u?8dcab5e4>
<http://www.nessus.org/u?36fd3072>
<http://www.nessus.org/u?4c7e0cf3>
<https://github.com/stamparm/EternalRocks/>
<http://www.nessus.org/u?59db5b5b>

Output

No output recorded.

Port	Hosts
445 / tcp / cifs	192.168.32.128 192.168.32.130

Vulnerability Information

CPE: cpe:/o:microsoft:windows
 Exploit Available: true
 Exploit Ease: Exploits are available
 Patch Pub Date: March 14, 2017
 Vulnerability Pub Date: March 14, 2017
 In the news: true

Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote
 Windows Kernel Pool Corruption)
 CANVAS ()
 Core Impact

Reference Information

EDB-ID: 41891, 41987
 MSFT: MS17-010
 BID: 96703, 96704, 96705, 96706, 96707, 96709
 IAVA: 2017-A-0065
 MSKB: 4012212, 4012213, 4012214, 4012215,
 4012216, 4012217, 4012606, 4013198, 4013429,
 4012598, 4012212, 4012213, 4012214, 4012215,
 4012216, 4012217, 4012606, 4013198, 4013429,
 4012598
 CVE: CVE-2017-0143 CVE-2017-0144 CVE-2017-

Nessus

Scans Settings

admin

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Basic Scan

Back to My Scans

Configure Audit Trail Launch Export

Hosts 6 Vulnerabilities 61 History 1

Filter Search Hosts 6 Hosts

Host	Vulnerabilities
192.168.32.1	7 92
192.168.32.128	2 32
192.168.32.130	4 2 26
192.168.32.129	2 30
192.168.32.131	5
192.168.32.254	1 3

Scan Details

Name: Basic Scan

Status: Completed

Policy: Basic Network Scan

Scanner: Local Scanner

Start: Today at 4:14 PM

End: Today at 4:39 PM

Elapsed: 25 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

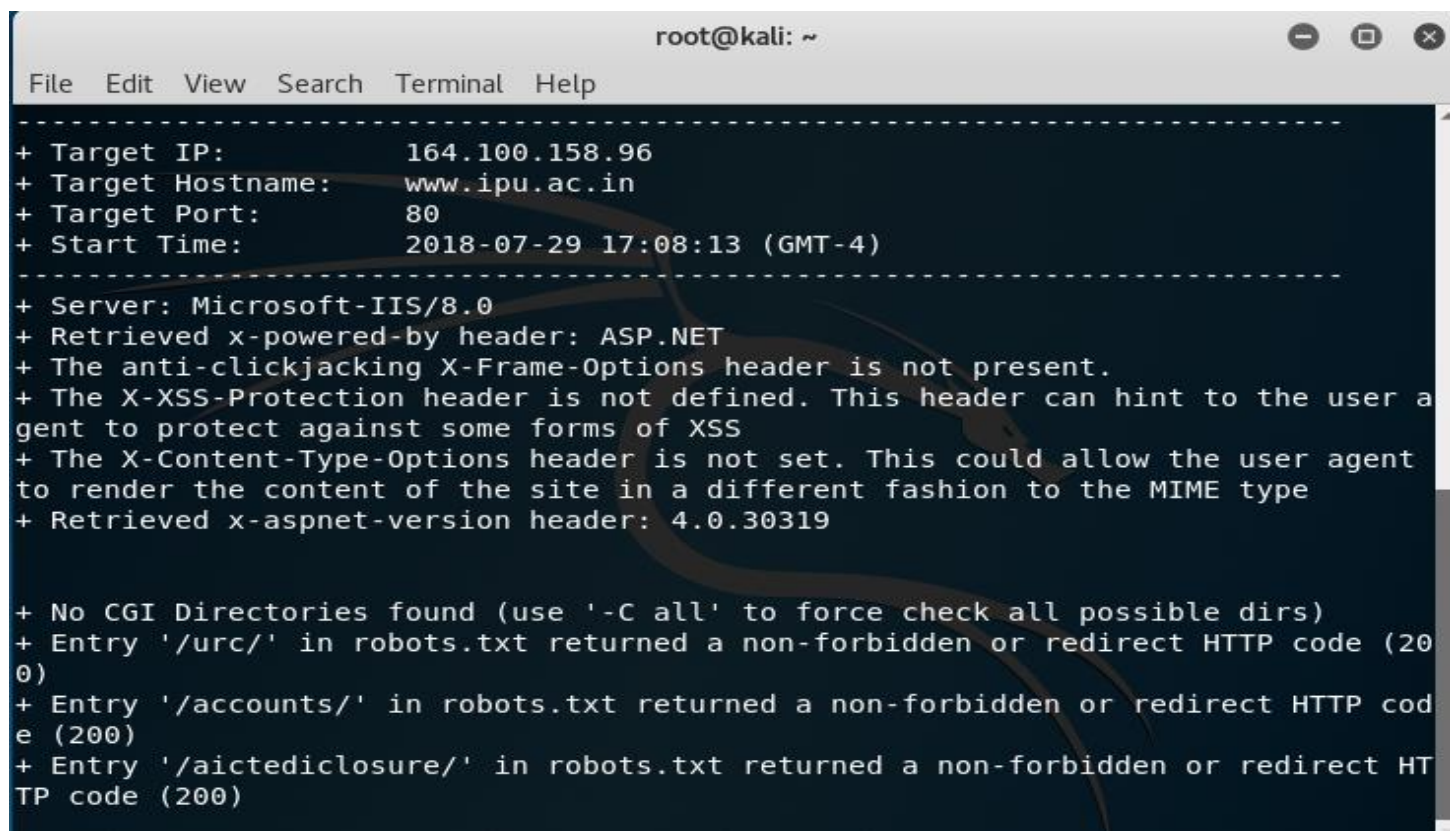
Tool Name: Nikto

Vendor Reference: SecTools

Methodology:

Nikto Web Scanner is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. The Nikto code itself is Open Source (GPL), however the data files it uses to drive the program are not.

We used nikto to scan our university's website; www.ipu.ac.in to find out the servers' OS and it's vulnerabilities and found the following output:

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the output of a Nikto scan. The output is divided into two sections by dashed lines. The first section lists target information: Target IP (164.100.158.96), Target Hostname (www.ipu.ac.in), Target Port (80), and Start Time (2018-07-29 17:08:13 (GMT-4)). The second section lists scan results: Server (Microsoft-IIS/8.0), Retrieved x-powered-by header (ASP.NET), and several security warnings about missing headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options) and the x-aspnet-version header (4.0.30319). The final section lists robots.txt findings, showing that entries for '/urc/', '/accounts/', and '/aictediclosure/' all returned a non-forbidden or redirect HTTP code (200).

```
root@kali: ~
File Edit View Search Terminal Help
-----
+ Target IP:          164.100.158.96
+ Target Hostname:    www.ipu.ac.in
+ Target Port:        80
+ Start Time:         2018-07-29 17:08:13 (GMT-4)
-----
+ Server: Microsoft-IIS/8.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319

+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/urc/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/accounts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/aictediclosure/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
```

[Challenge 3:] OS Fingerprinting:

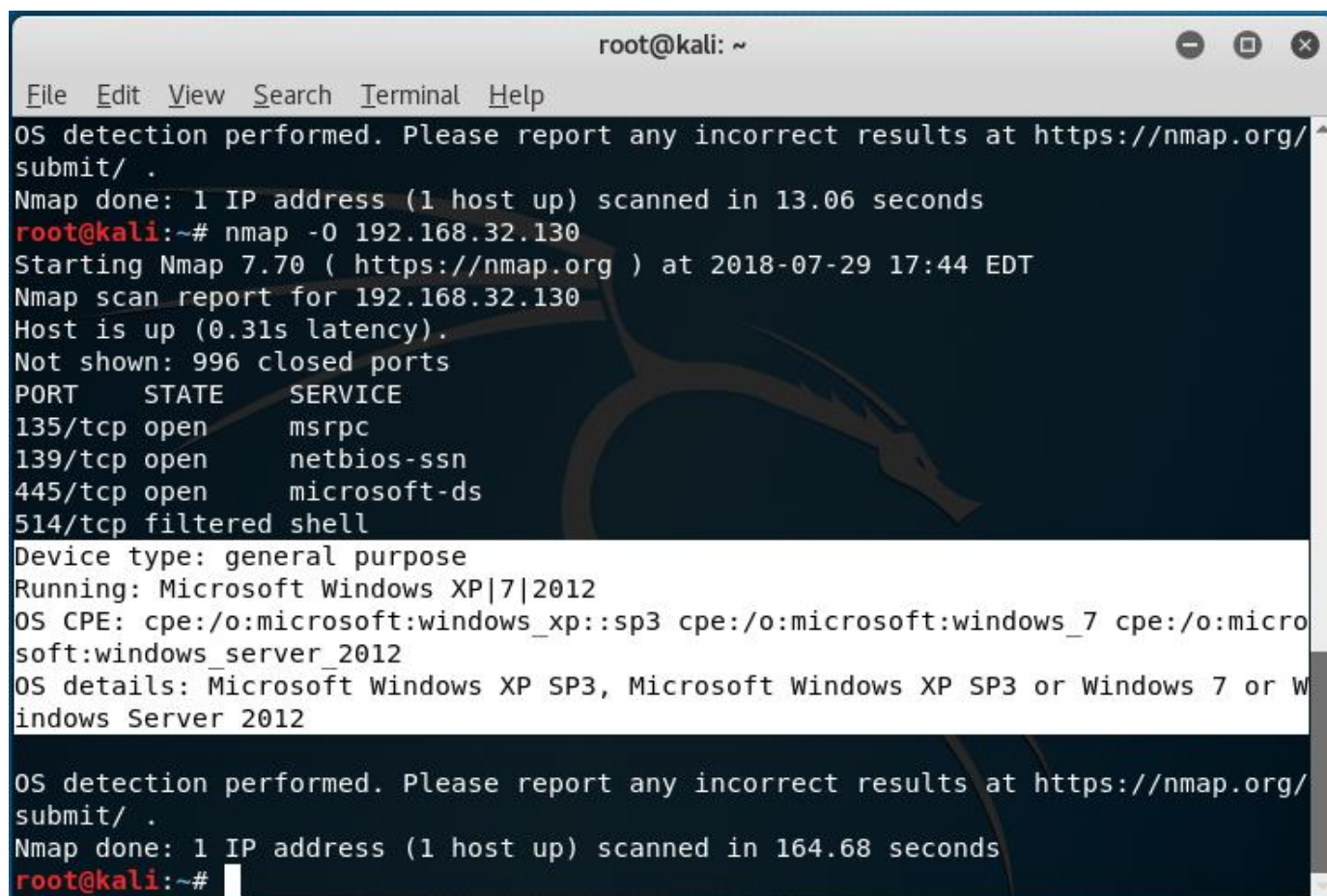
OS fingerprinting is the process of determining the operating system used by a host on a network.

Tool Name: Nmap

Vendor Reference: Nmap 7.70

Methodology:

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. We used this to identify the OS of the machines running in our network.



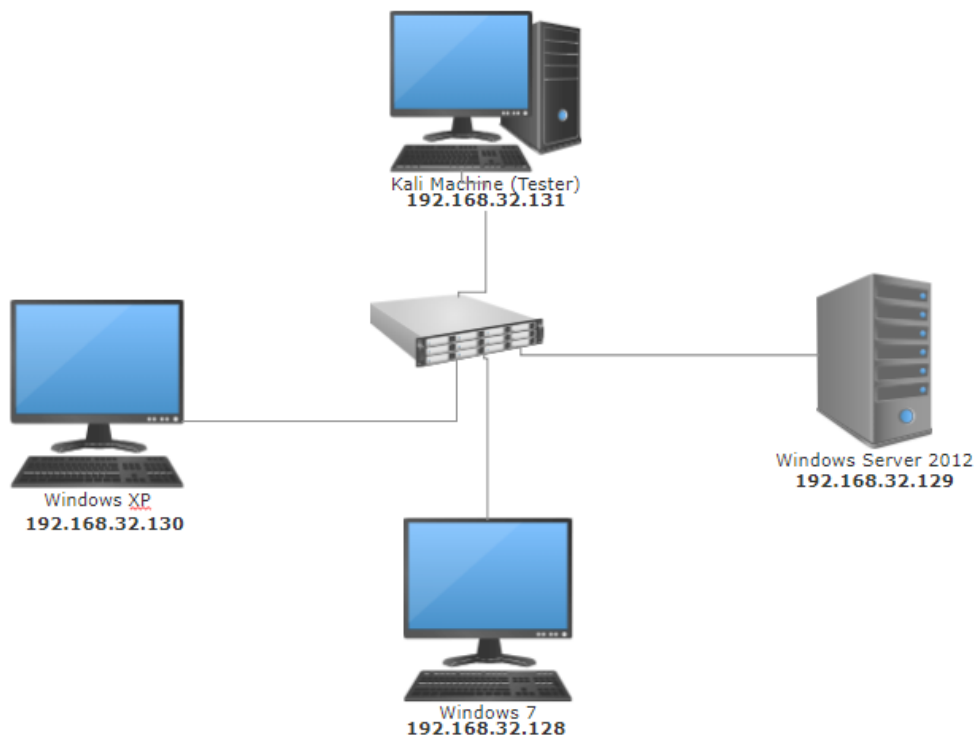
```
root@kali: ~
File Edit View Search Terminal Help
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~# nmap -O 192.168.32.130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-29 17:44 EDT
Nmap scan report for 192.168.32.130
Host is up (0.31s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
135/tcp    open       msrpc
139/tcp    open       netbios-ssn
445/tcp    open       microsoft-ds
514/tcp    filtered  shell
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.68 seconds
root@kali:~#
```

The results of the Network Scanning and Enumeration and OS Fingerprinting phases can be seen as below:

Network Hosts:

IP Address	Operating System
192.168.32.128	Windows XP, SP 3
192.168.32.129	Windows 7
192.168.32.130	Windows Server 2012 R2
192.168.32.131	Kali Linux, 2018.1

Network Topology:



[Challenge 4:] Gaining Access:

Tool Name: Armitage (Metasploit)

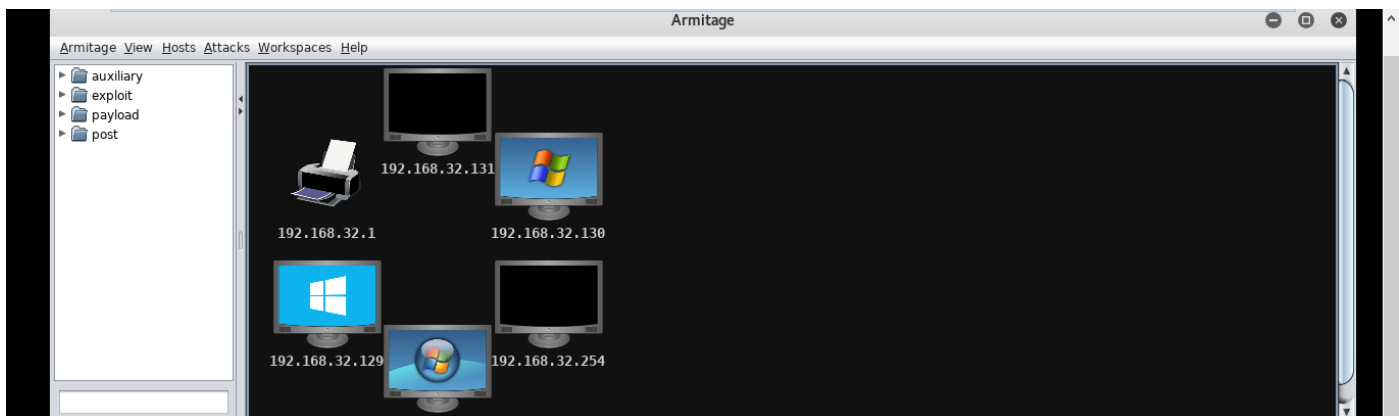
Vendor Reference: Offensive Security

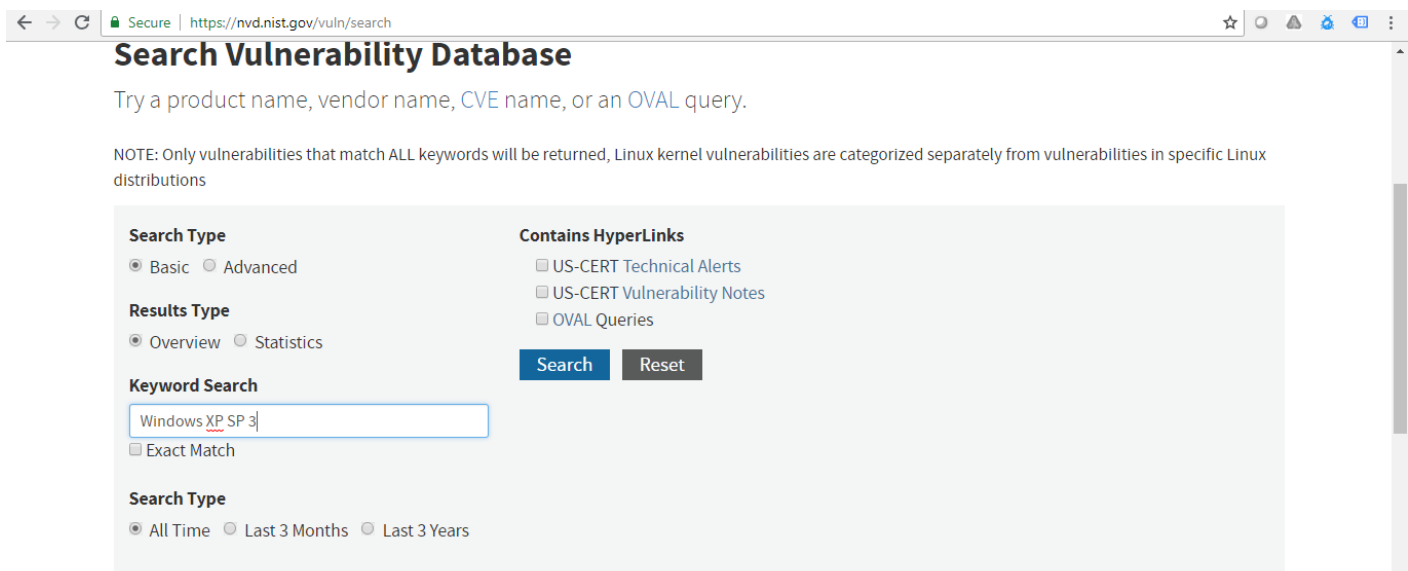
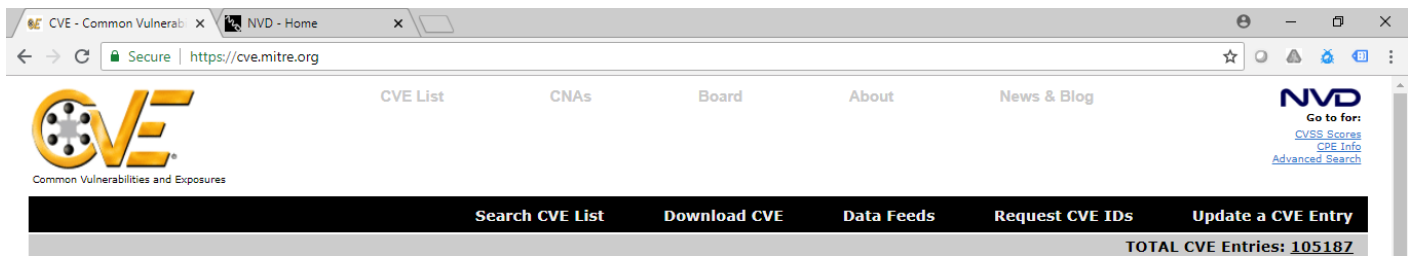
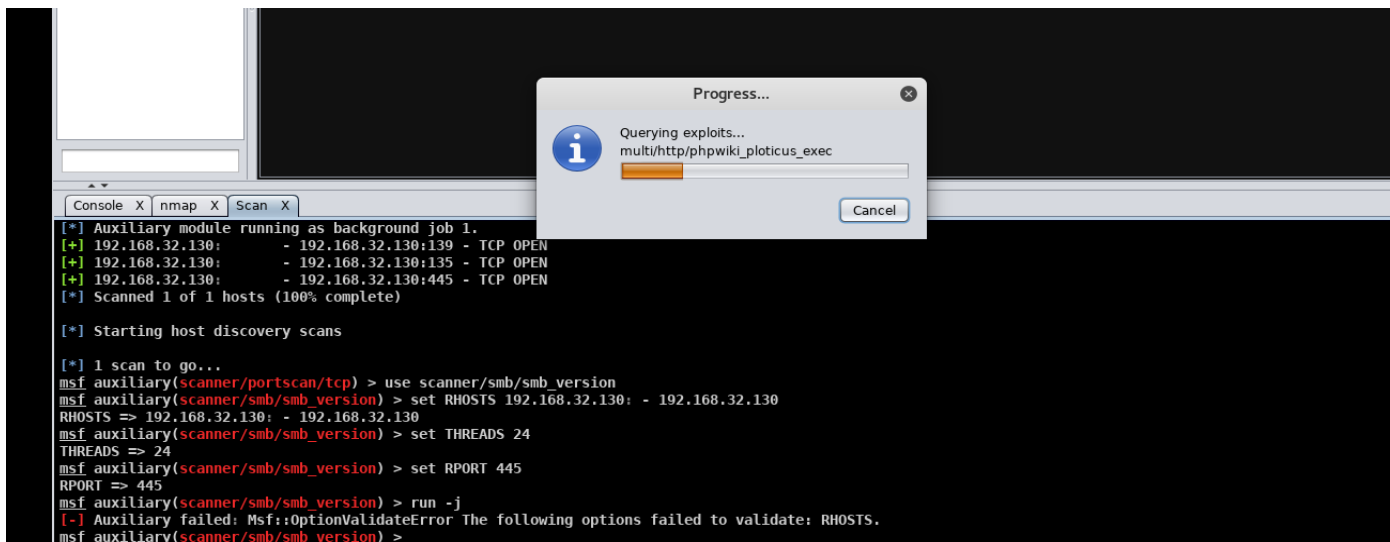
Methodology:

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open source network security tool notable for its contributions to red team collaboration allowing for: shared sessions, data, and communication through a single Metasploit instance. Armitage is written and supported by Raphael Mudge.

We used Metasploit Armitage to try and exploit the most common and popular vulnerabilities of the various Operating Systems in the network.

However, I found that the OS was patched against major vulnerabilities and exploits which were researched upon using CVEmitre.org or <https://nvd.nist.gov/> for all the latest vulnerabilities, their exploits and their solutions.





Vuln ID 卷

Summary ⓘ

CVSS Severity ⓘ

CVE-2018-2942

Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). Supported versions that are affected are Java SE: 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).

Published: July 18, 2018; 09:29:02 AM -04:00

V3: 8.3 HIGH

V2: 5.1 MEDIUM

CVE-2018-4858

A vulnerability has been identified in IEC 61850 system configurator (All versions < V5.80), DIGSI 5 (affected as IEC 61850 system configurator is incorporated) (All versions < V7.80), DIGSI 4 (All versions), SICAM PAS/PQS (All versions < V8.11), SICAM PQ Analyzer (All versions < V3.11), SICAM SCC (All versions). A service of the affected products listening on all of the host's network interfaces on either port 4884/TCP, 5885/TCP, or port 5886/TCP could allow an attacker to either exfiltrate limited data from the system or to execute code with Microsoft Windows user permissions. Successful

Secure | https://www.exploit-db.com/google-hacking-database/



Home

Exploits

Shellcode

Papers

Google Hacking Database

Submit

Search

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

CVE-2018-2942

SEARCH

Date	Title	Category
2018-07-20	"air confirmation" "passenger(s)"	Files Containing Juicy Info
2018-07-19	intitle:HTTP Server Test Page powered by CentOS	Web Server Detection
2018-07-17	inurl:"debug/default/view?panel=config"	Files Containing Juicy Info
2018-07-16	inurl:configuration.php and intext:"var \$password="	Files Containing Passwords

The screenshot shows the Exploit-DB website with a search for CVE-2018-2942. The search results table is as follows:

Date	Title	Summary
2018-06-21	"2004 - 2018 iboss, Inc. All rights reserved."	Pages Containing Login Portals Find iBoss login portals. ~ CrimsonTorso
2018-05-31	intext:2001.-,2018.umbraco.org ext:aspx	Pages Containing Login Portals Identify admin login portals for websites built with Umbraco CMS. Author: Raj Kiran P
2018-05-11	intext:"this login can be used only once" inurl:user intitle:"reset password"	Pages Containing Login Portals This dork can hunt out vulnerable drupal websites with their password reset pages of various accounts for account takeover. *Description*: Drupal...

Tool Name: SetToolKit

Vendor Reference: THC

Methodology:

After the exploits didn't work to get into the system, we had to gain access through social engineering. And for this SET Tool Kit was used. Using the payload and listener method I was able to gain access to these systems and establish a session.

The screenshot shows a Windows Internet Explorer browser window displaying the index of a directory at http://192.168.32.131/. The index lists a file named `payload.exe` with a size of 72K, last modified on 2018-07-30 at 13:59. The browser also shows the Apache/2.4.33 (Debian) Server at 192.168.32.131 Port 80.

```
msf exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 192.168.32.130
[*] Meterpreter session 1 opened (192.168.32.131:443 -> 192.168.32.130:1090) at 2018-07-30 14:06:05 -0400

msf exploit(multi/handler) > sessions -i

Active sessions
=====
Id  Name  Type           Information                                     Connection
--  --
1   meterpreter x86/windows KARTIK-F908DF89\Administrator @ KARTIK-F908DF89 192.168.32.131:443 -> 192.168.32.130:1090 (192.168.32.130)
```

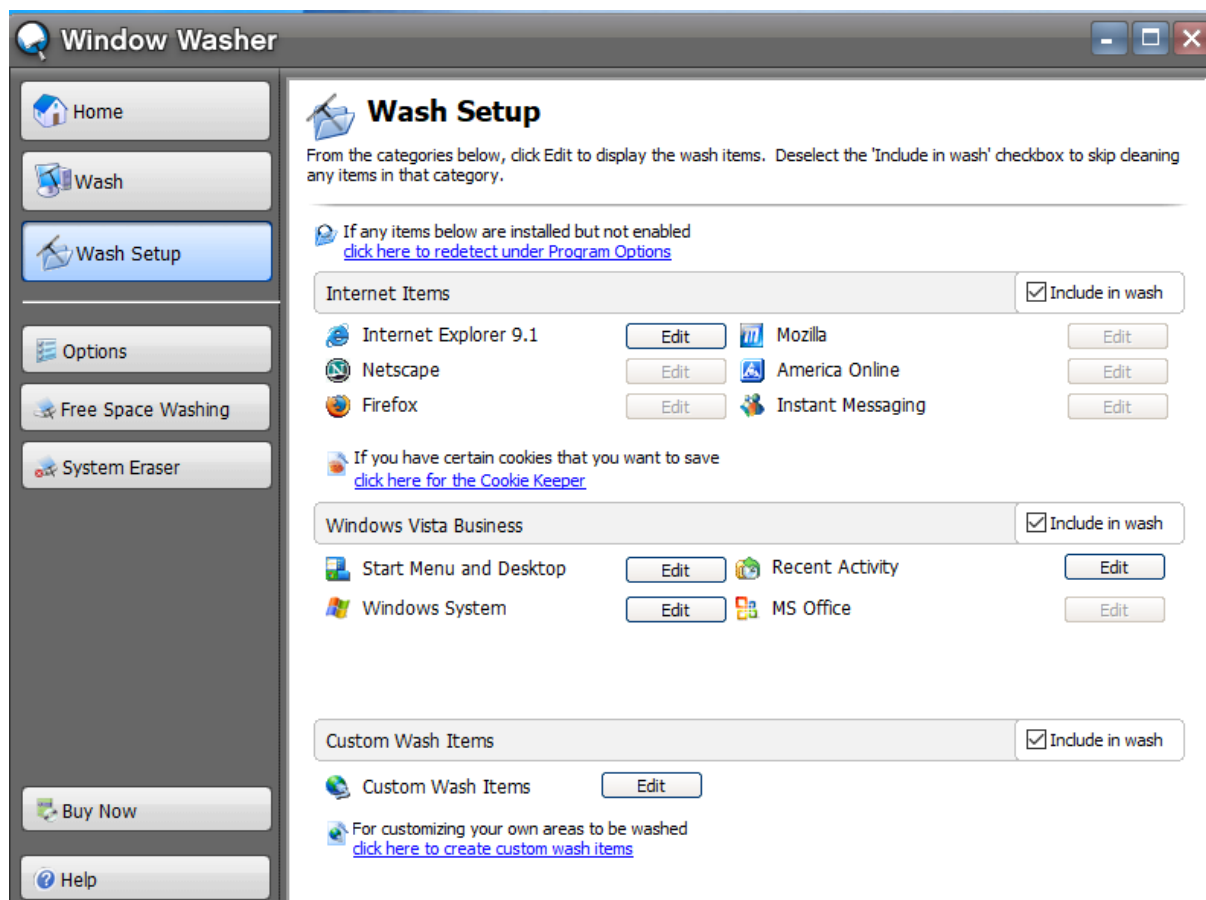
[Challenge 5:] Erasing Tracks:

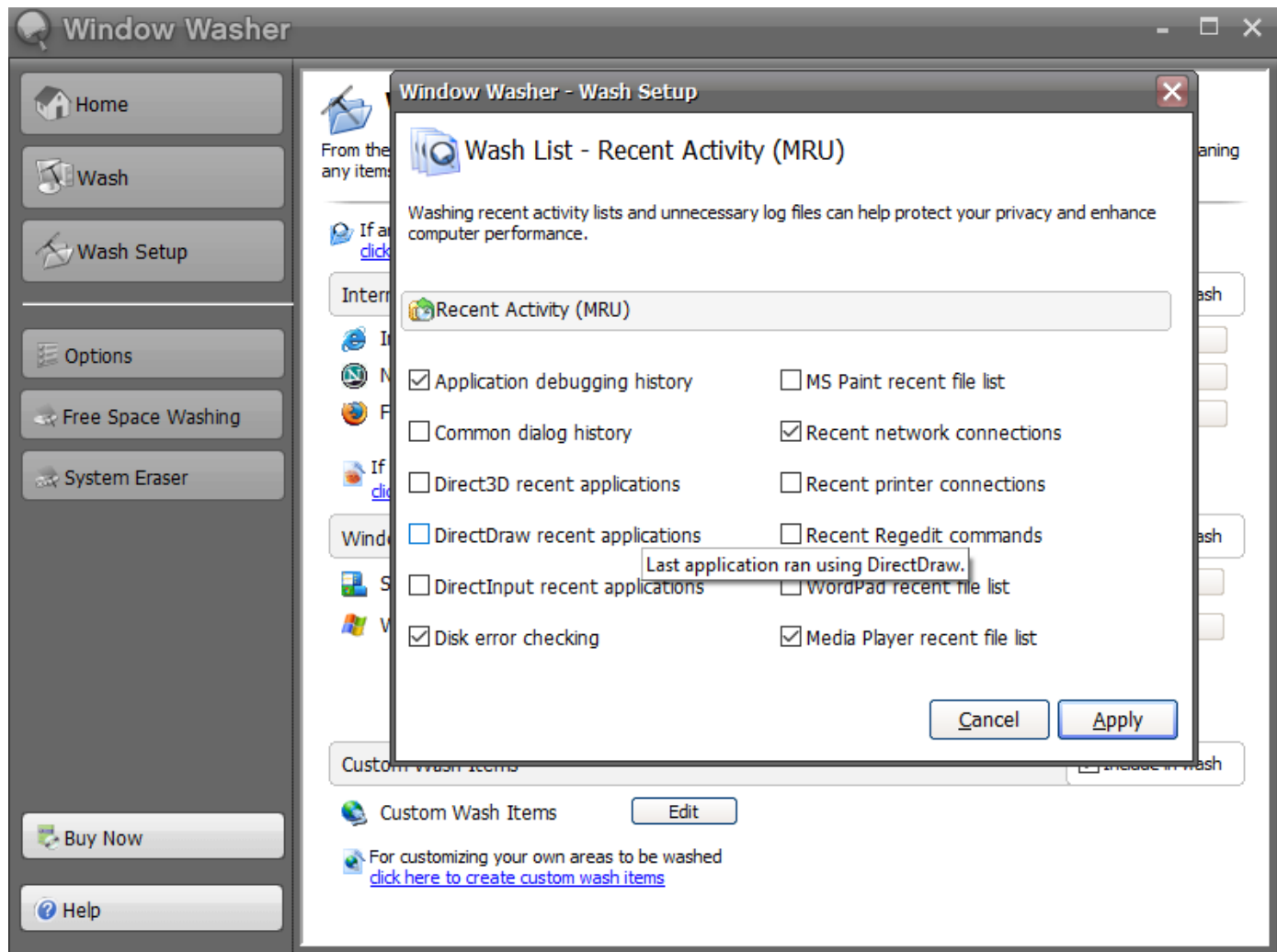
Tool Name: Window Washer

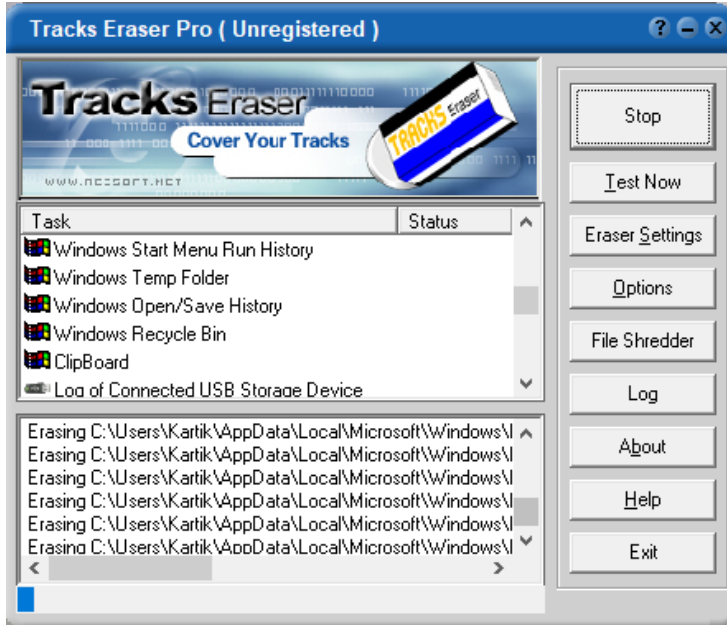
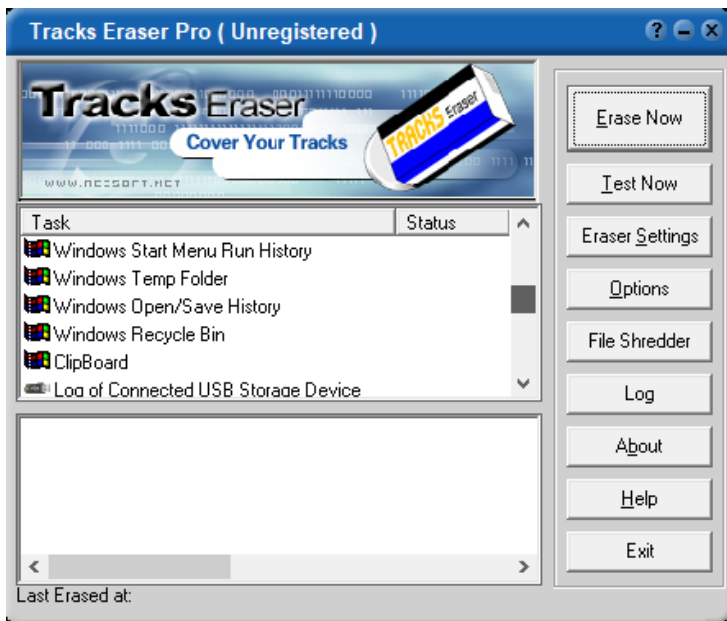
Vendor Reference:

Methodology:

Webroot Window Washer was a tool designed to protect user's privacy by permanently deleting all traces of web browsing history and other personal information files on a computer running Microsoft Windows. Currently, no further versions are planned as the program is no longer being updated. We can easily delete any system logs by this tool and erase and cover our tracks. The Windows systems were found vulnerable to this tool and some other tools such as Tracks Eraser Pro for erasing logs of information.







Conclusions

The conclusion drawn from the above penetration testing project could be listed as follows:

Penetration testing is the first step towards a better and secured system in any organization. Information security is the front of the minds of companies in any sector. Throughout this project I have tried to implement and test out industry standard tools in a lab environment.

This project work could be concluded as an example of what are the real vulnerabilities in large organization with a large number of employees pose a threat to the prices information of the company or its employees.

These vulnerabilities are to be found out completely and according to the risks it poses to the organization should be fixed with the appropriate recommendation. Risk versus production plays a crucial role whether or not these recommendations are feasible or not. Nevertheless, any organization should always keep security as a major consideration point.

References & Bibliography

- <https://nmap.org/>
- https://en.wikipedia.org/wiki/Information_security
- <https://www.exploit-db.com/google-hacking-database/>
- <https://nvd.nist.gov/vuln/search>
- <https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/>

