Project report on

Penetration Testing

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.

Certificate

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 programmers 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

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.

Contact:

Name	Kartik Jaitly
Address	J11/114 New Delhi .
Phone	8585983442

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.

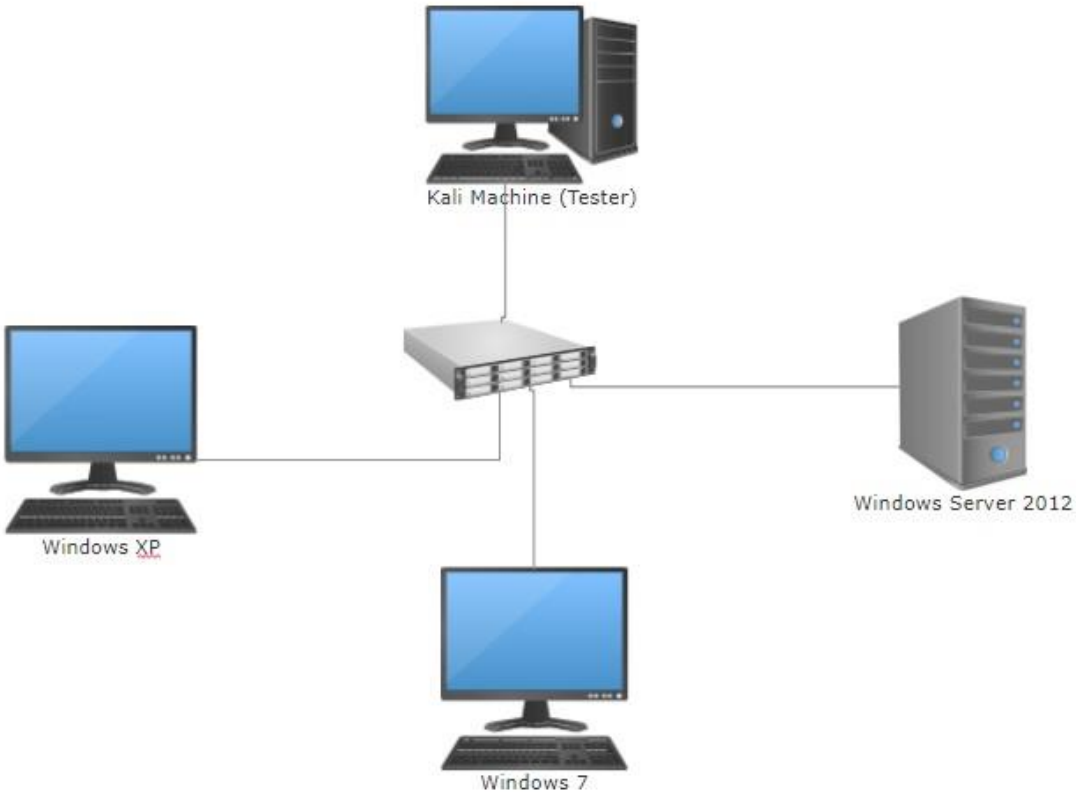
Project Objective:

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


Kali Machine (Tester)
Windows XP
Windows Server 2012
Windows 7

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

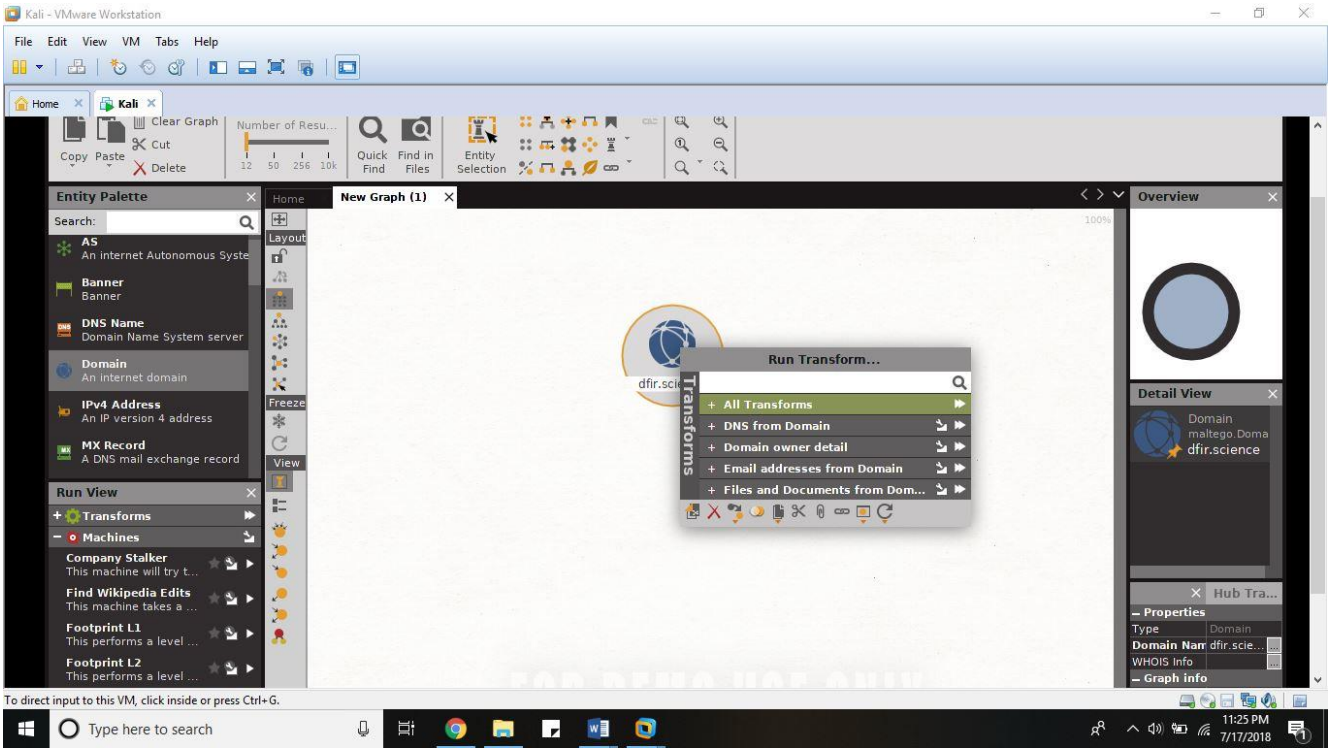
Vendor: Paterva

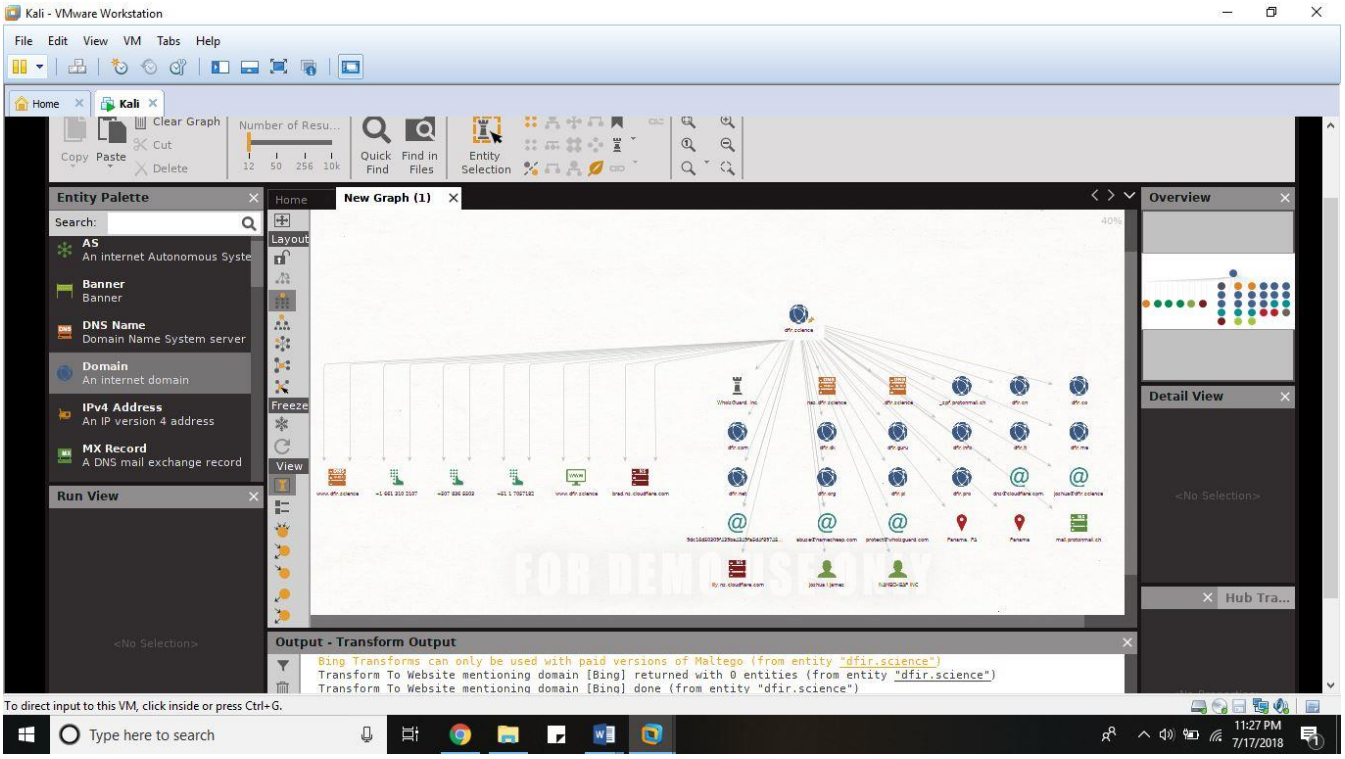
Methodology:

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.


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Clear Graph
Cut
Delete
Copy
Paste
Number of Resu...
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
AS
An internet Autonomous Syste
Banner
Banner
DNS Name
Domain Name System server
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
Run View
Transforms
Machines
Company Stalker
This machine will try t...
Find Wikipedia Edits
This machine takes a ...
Footprint L1
This performs a level ...
Footprint L2
This performs a level ...
New Graph (1)
Layout
Freeze
View
Run Transform...
Transforms
All Transforms
DNS from Domain
Domain owner detail
Email addresses from Domain
Files and Documents from Dom...
Overview
Detail View
Domain
maltego.Doma
dfir.science
Hub Tra...
Properties
Type
Domain
Domain Nam
dfir.scie...
WHOIS Info
Graph info
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
11:25 PM
7/17/2018


Kali - VMware Workstation
File Edit View VM Tabs Help
Home
Kali
Clear Graph
Cut
Delete
Copy
Paste
Number of Resu...
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
AS
An internet Autonomous Syste
Banner
Banner
DNS Name
Domain Name System server
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
Run View
<No Selection>
New Graph (1)
Layout
Freeze
View
Overview
Detail View
<No Selection>
Hub Tra...
Output - Transform Output
Bing Transforms can only be used with paid versions of Maltego (from entity "dfir.science")
Transform To Website mentioning domain [Bing] returned with 0 entities (from entity "dfir.science")
Transform To Website mentioning domain [Bing] done (from entity "dfir.science")
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
11:27 PM
7/17/2018

[Challenge 2:] Network Scanning and Service Enumeration

Category: Authorization

Vendor Reference: Nmap 7.60

Threat Description:

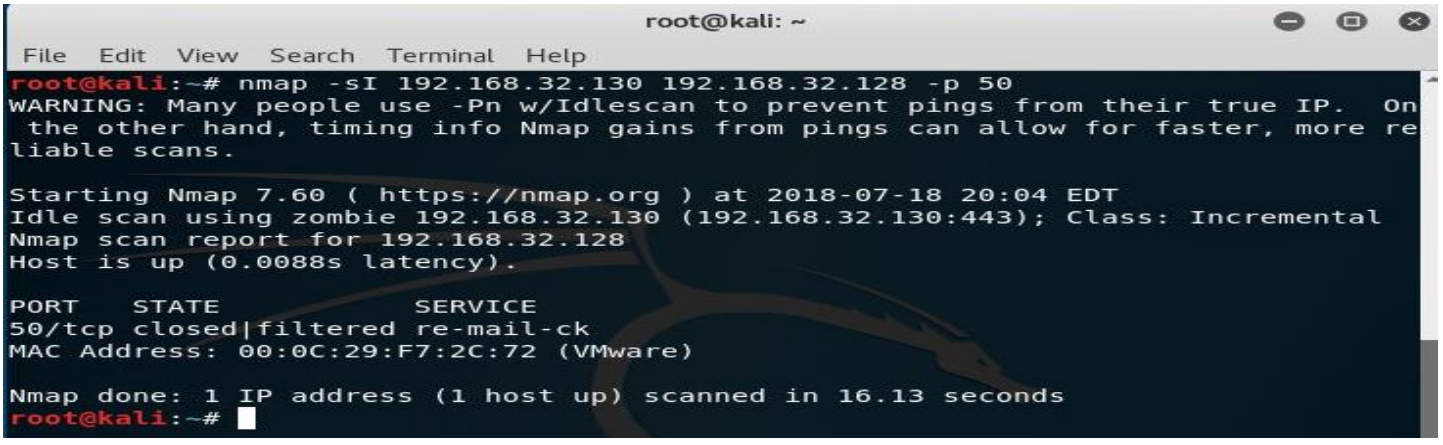
Once we identified the target system and completed the initial reconnaissance, as discussed in the above step, we started looking for a mode of entry into the target system. We conducted network scanning on IP addresses [ ] authorized for scanning by the organization on/from July 2018. The purpose of 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.

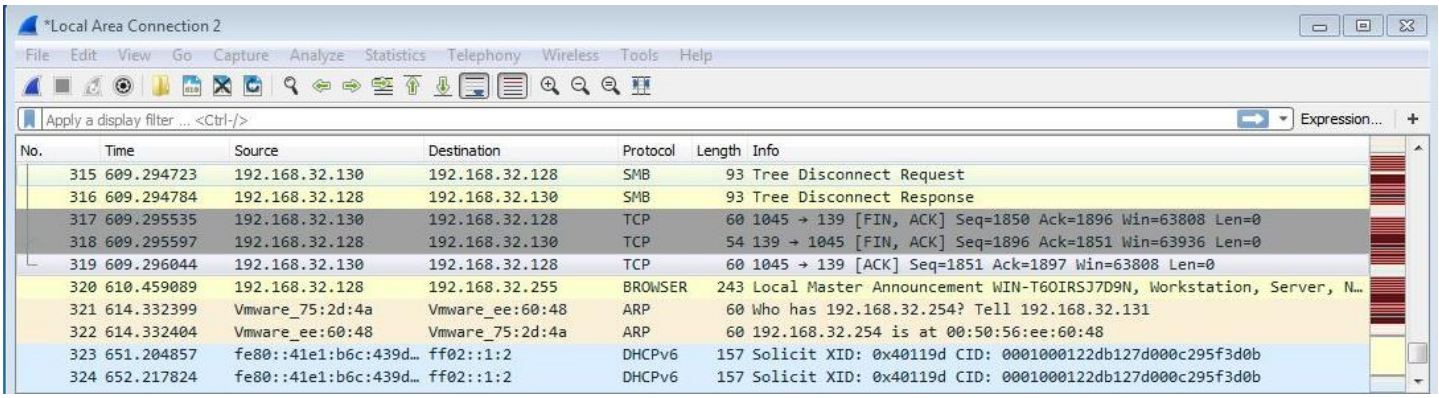
Methodology:

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.

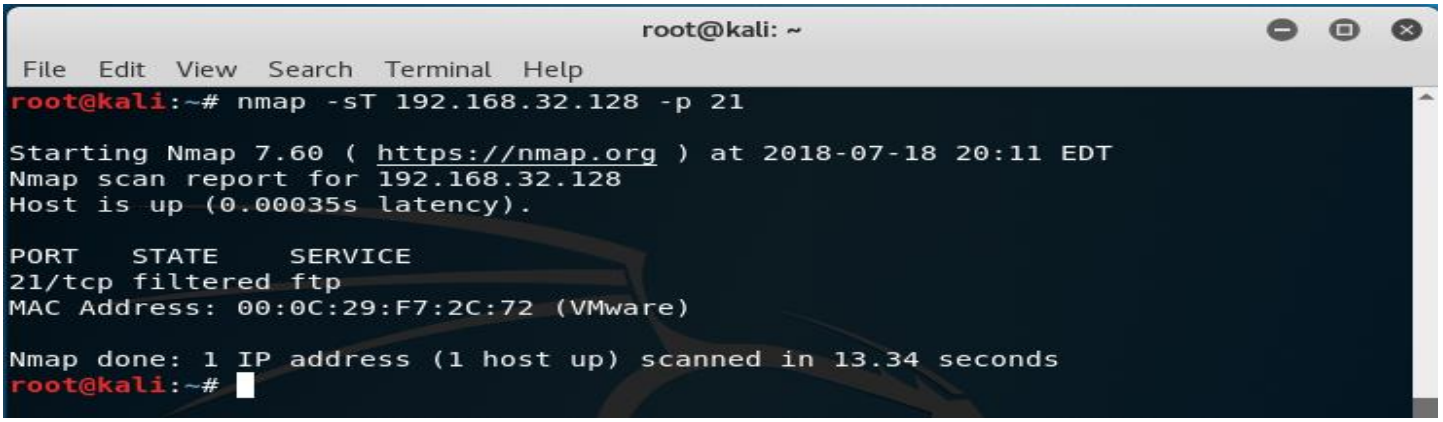
After repeated scanning, primarily with Nmap, and using hping of the IP addresses, we discovered following live hosts in the target network.

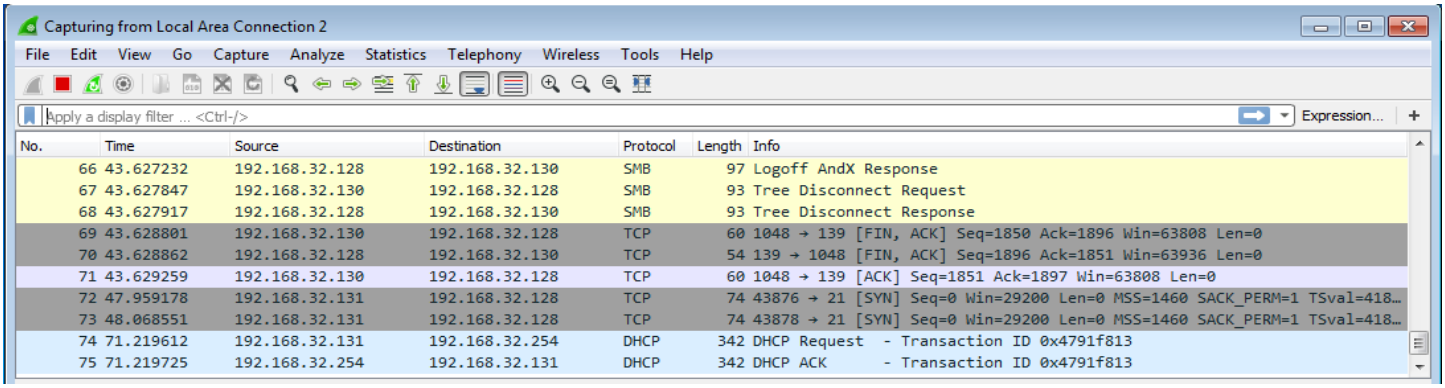
Nmap – Idle Scan



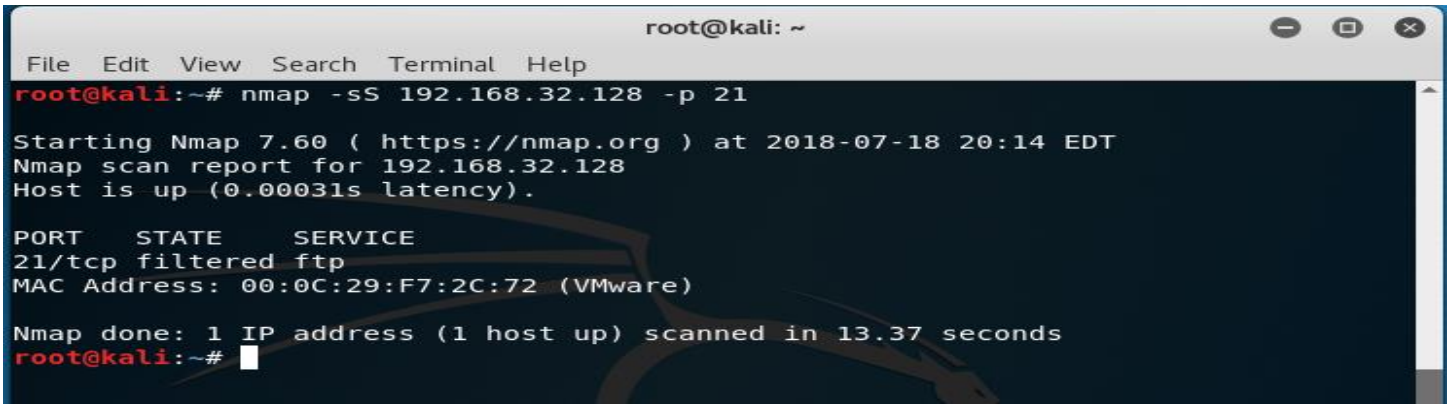


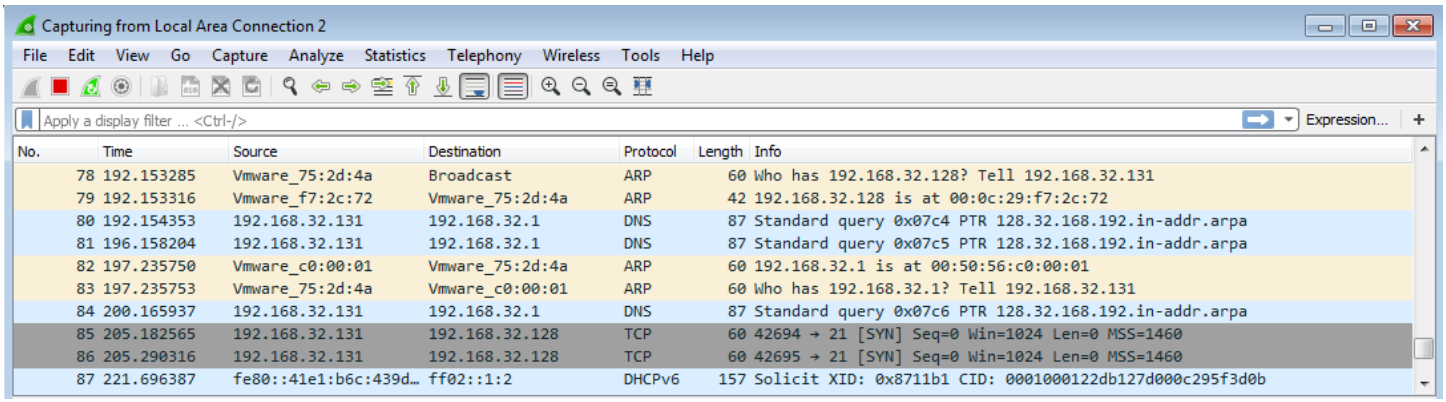
Nmap – Full Scan



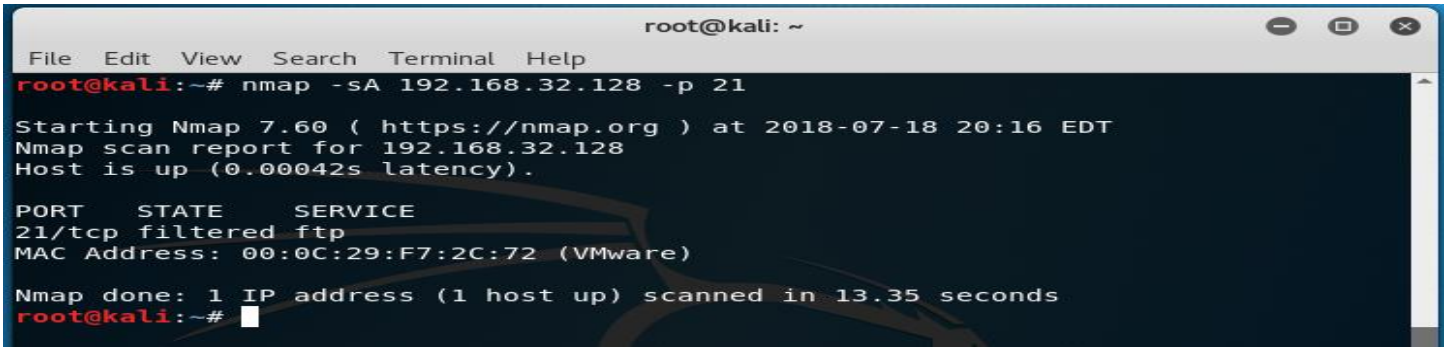


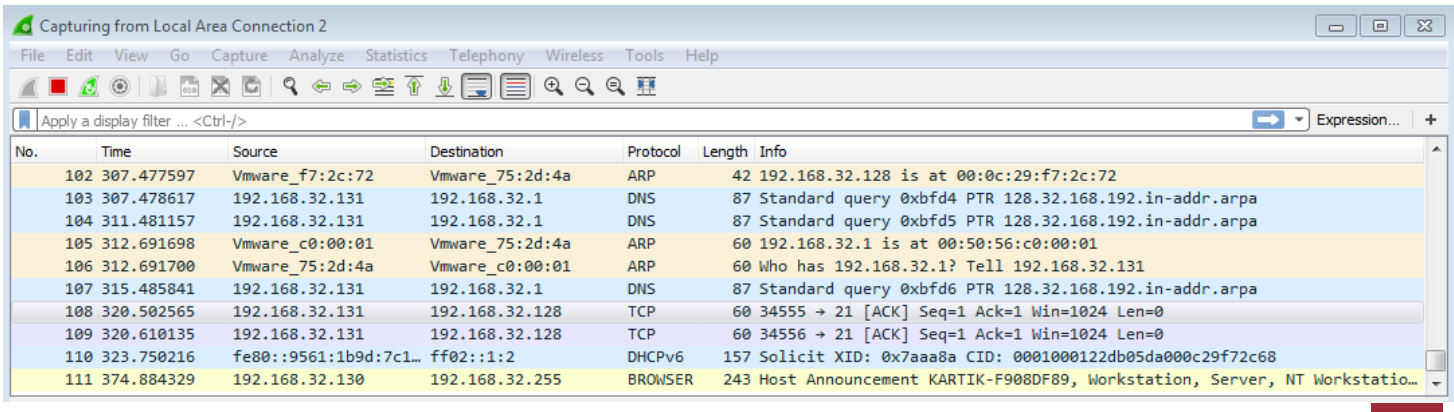
Nmap-Half Stealth Scan



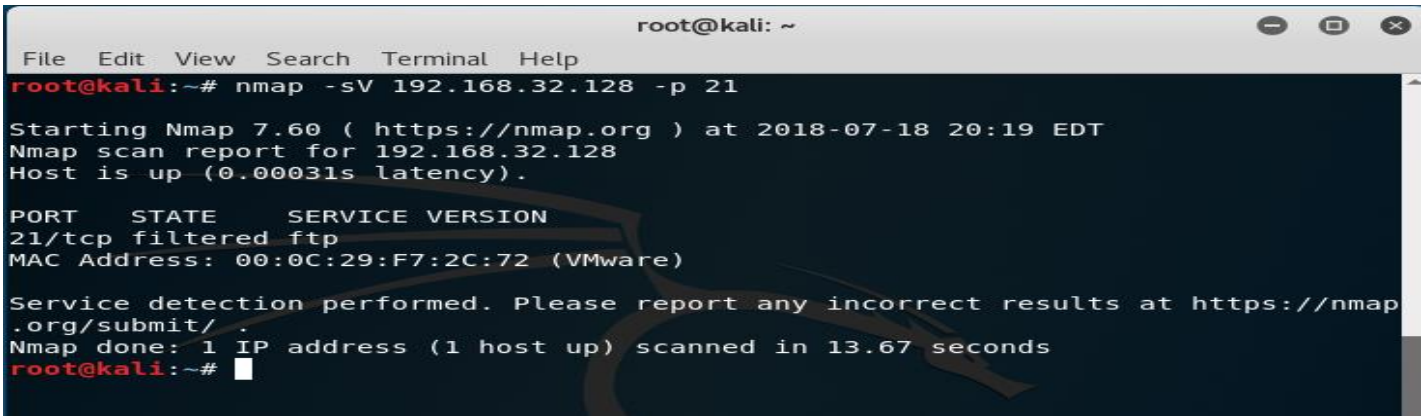


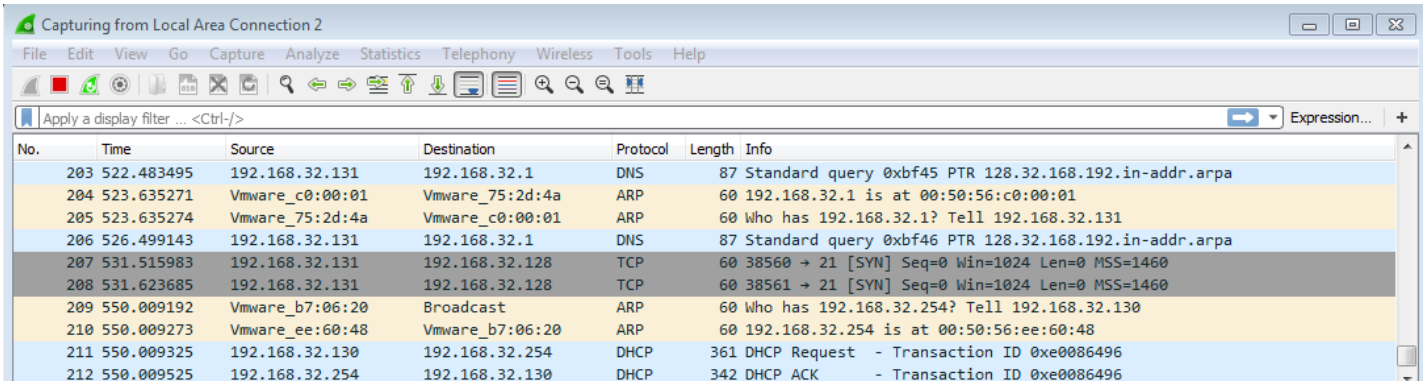
Nmap- ACK Scan





Nmap-RST Scan





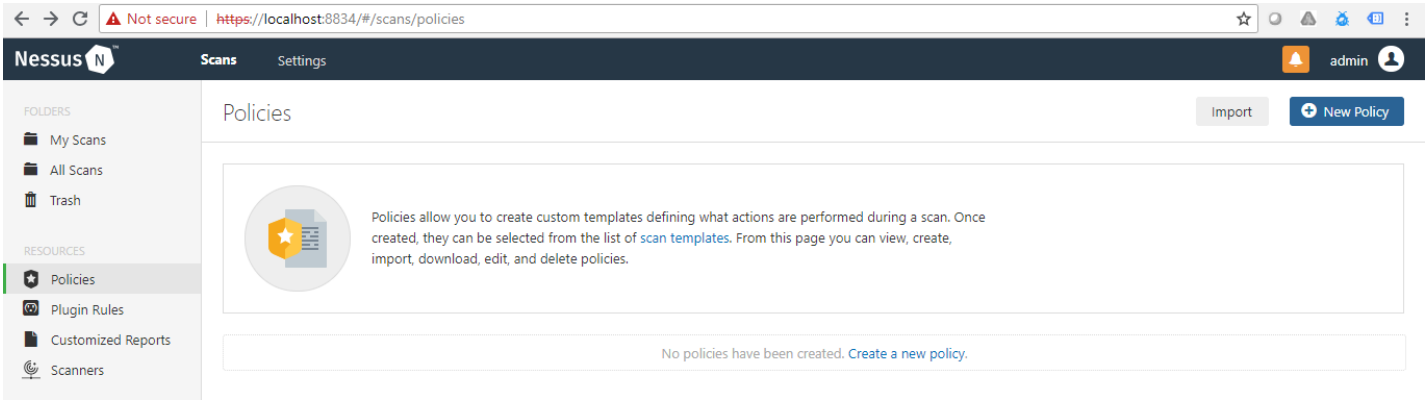
Tool Name: Nessus

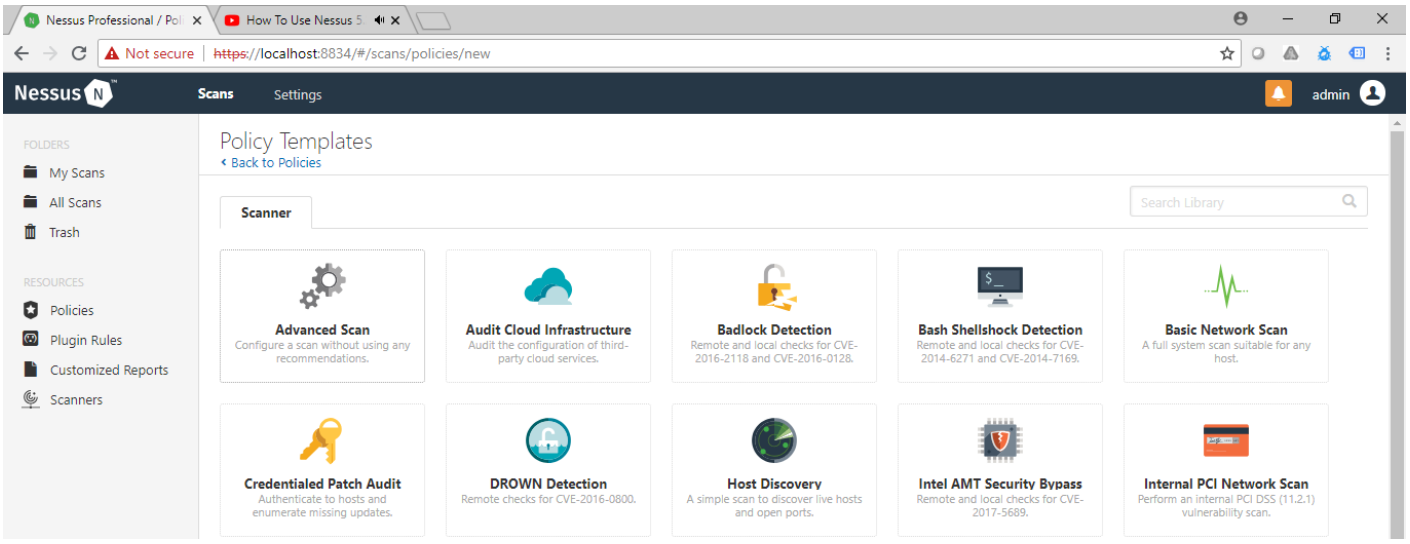
Vendor Reference: Tenable

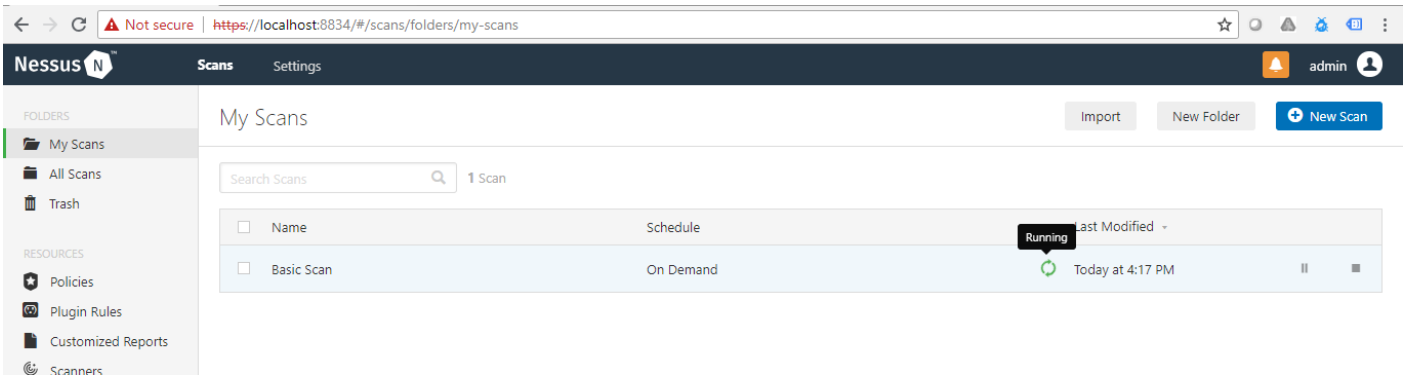
Methodology:

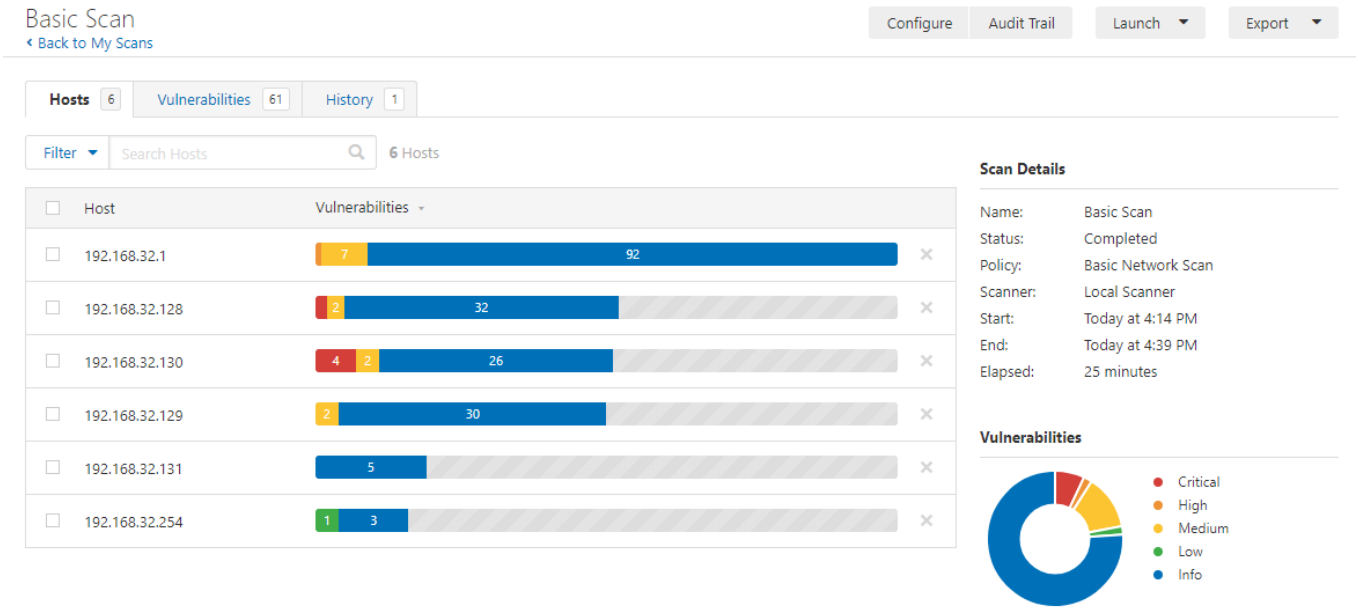
After setting up Nessus, we log onto the web client using local host 8834 and create a new policy under the policies option. After creating the policy, we schedule a new scan and set the policy to the prior set Basic Scan. We click on launch Scan now and let it run. On completion we can see various types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

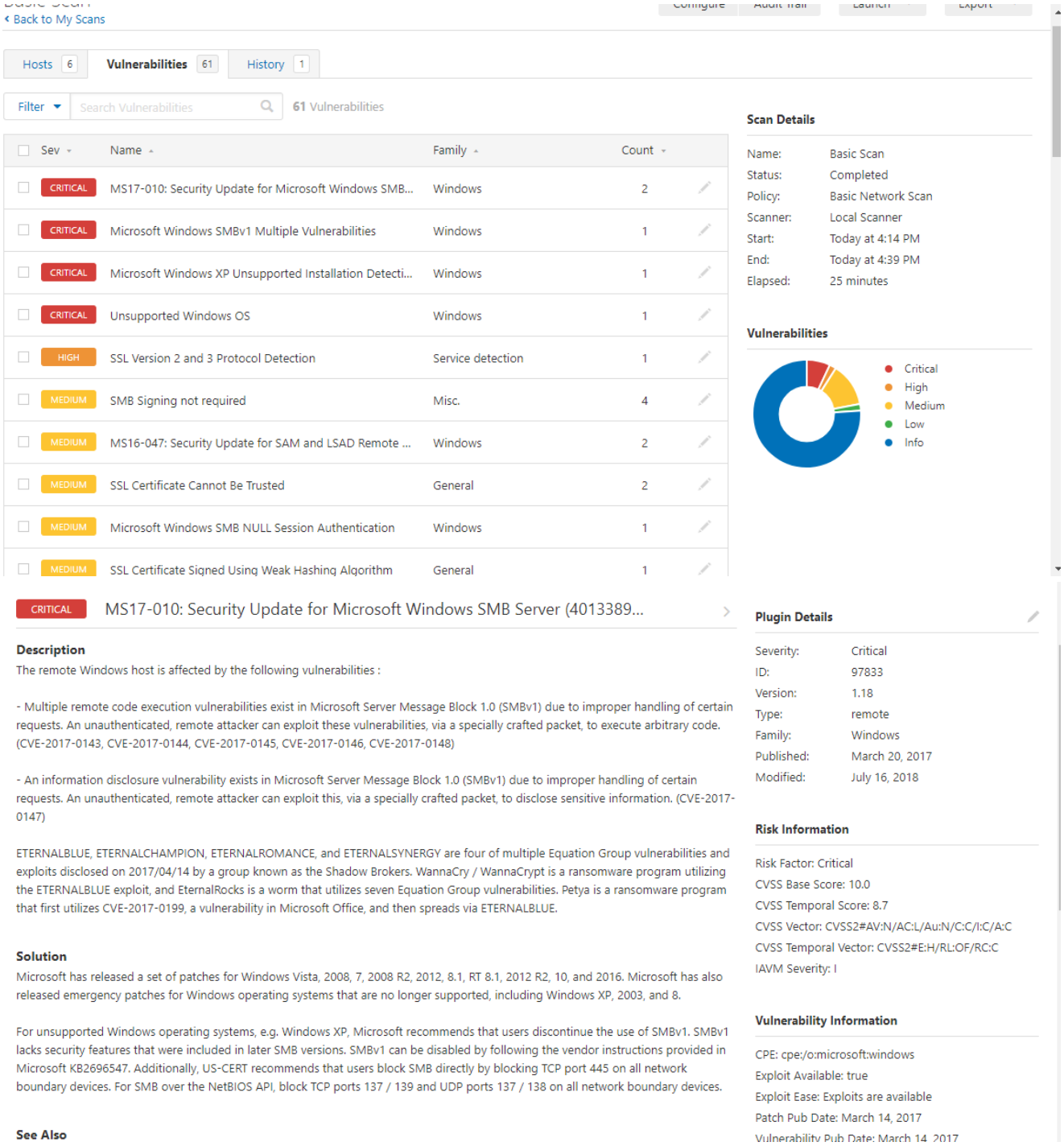
Basic_Scan_2n3fgt.pdf

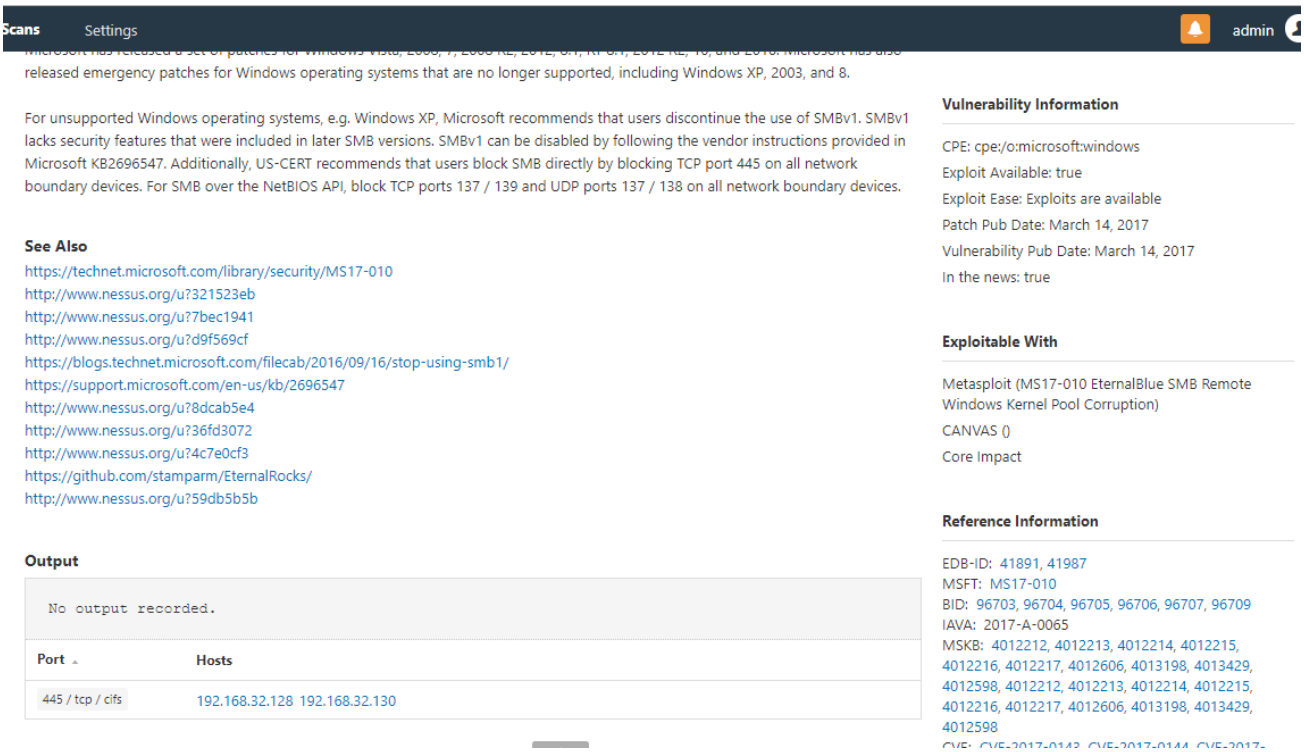


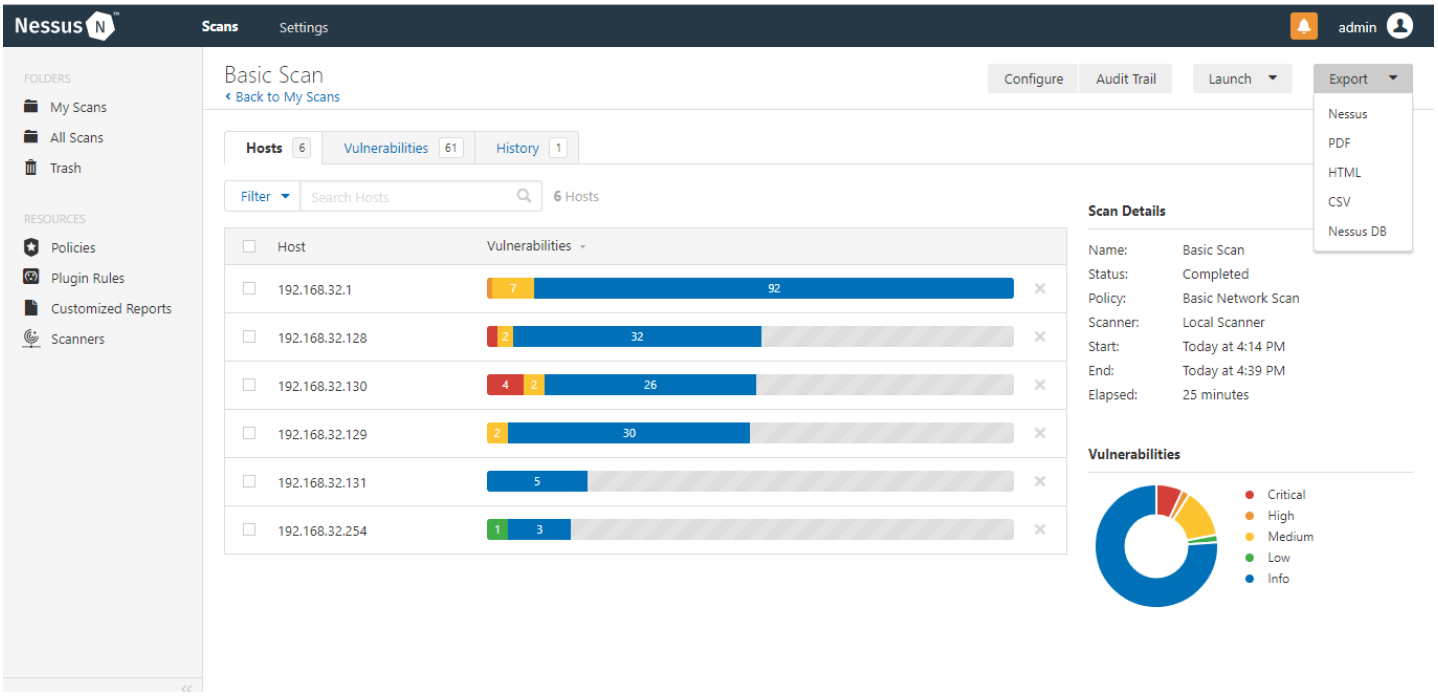



Not secure
https://localhost:8834/#/scans/folders/my-scans
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
Basic Scan
On Demand
Running
Today at 4:17 PM


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
192.168.32.128
192.168.32.130
192.168.32.129
192.168.32.131
192.168.32.254
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


Back to My Scans
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
Critical
High
Medium
Low
Info
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
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


Scans
Settings
admin
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


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
Nessus
PDF
HTML
CSV
Nessus DB
Hosts 6
Vulnerabilities 61
History 1
Filter
Search Hosts
6 Hosts
Host
Vulnerabilities
192.168.32.1
192.168.32.128
192.168.32.130
192.168.32.129
192.168.32.131
192.168.32.254
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

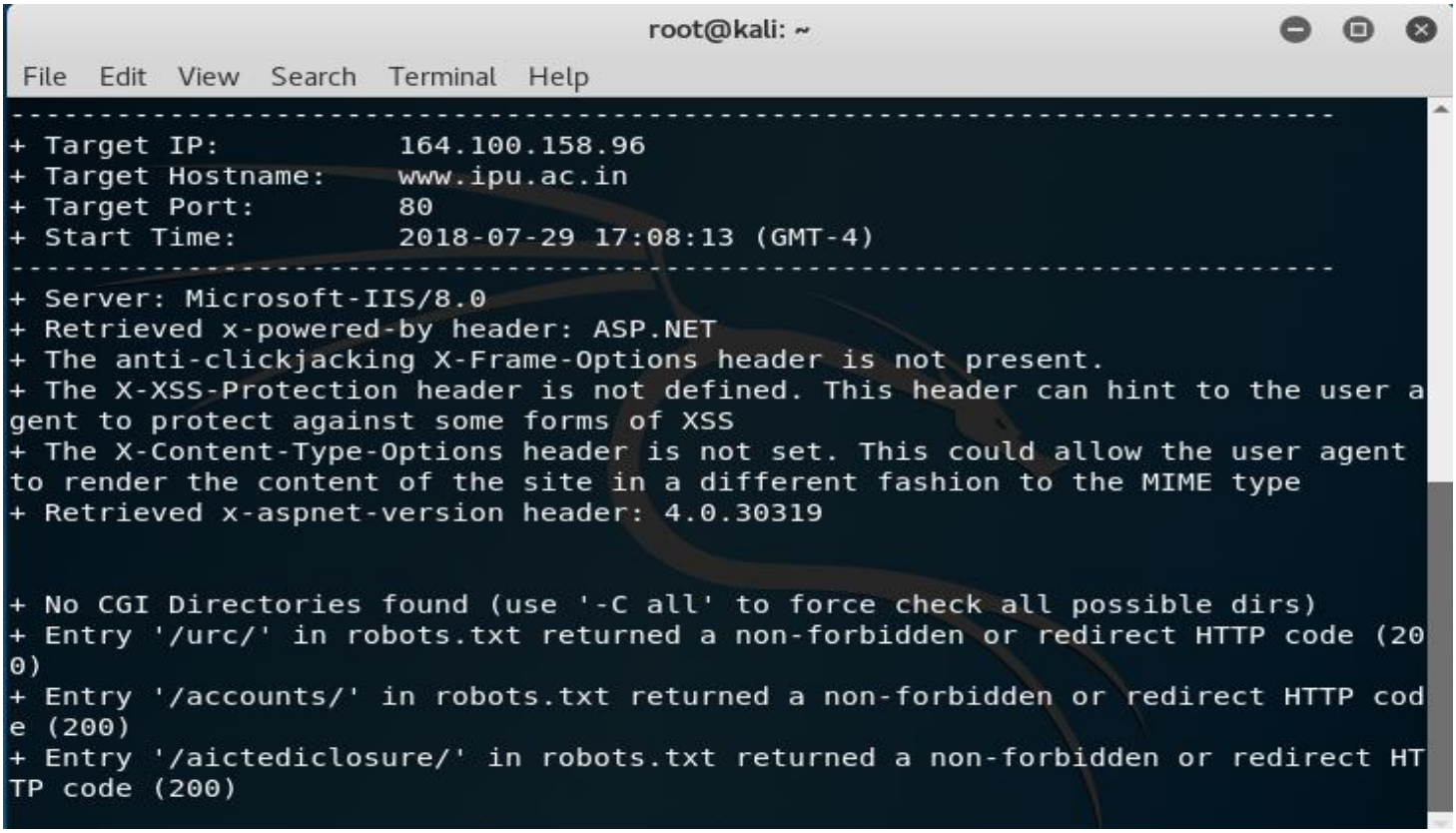
Tool Name: Nikto

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:



[Challenge 3:] OS Fingerprinting:

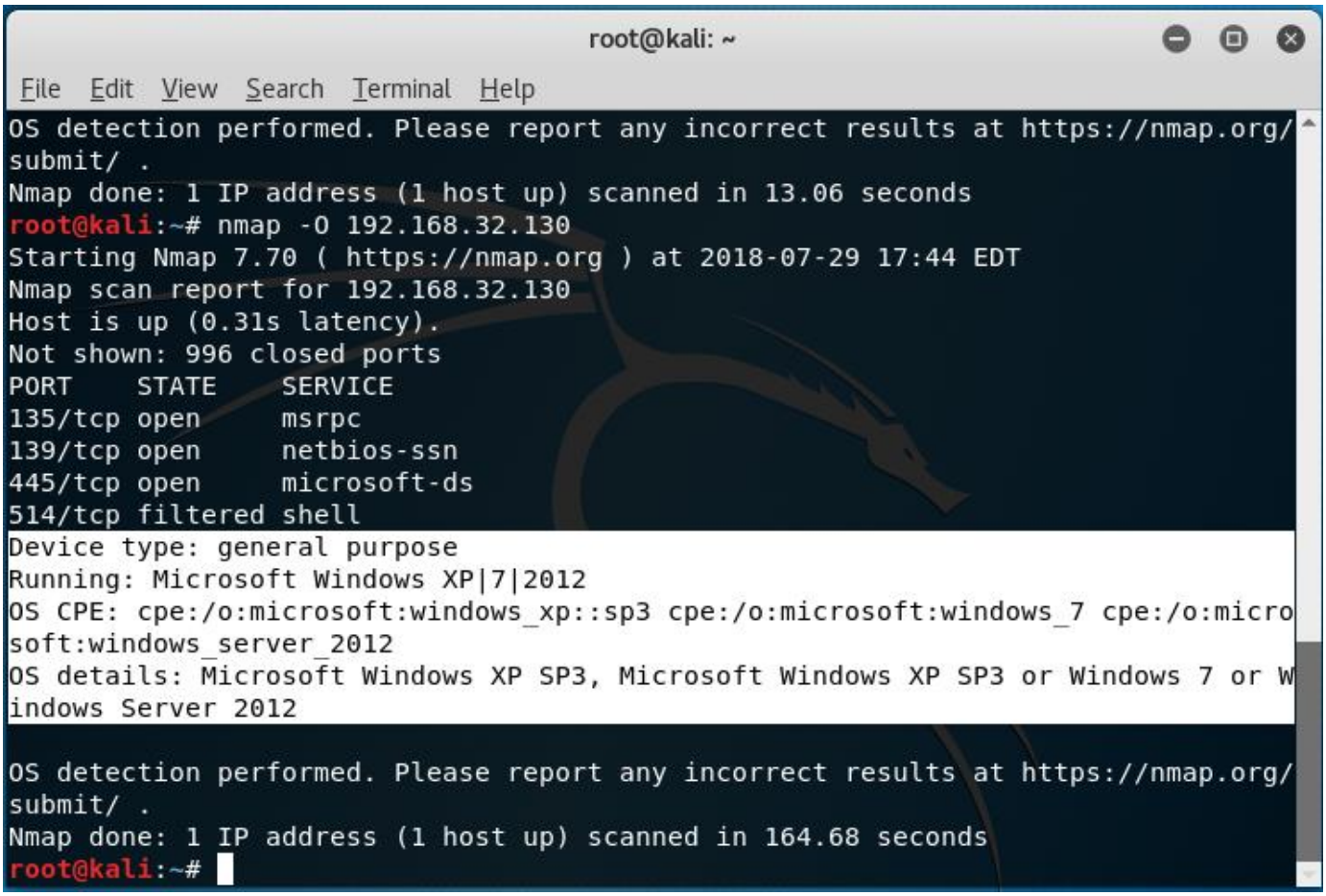
OS fingerprinting is the process of determining the operating system used by a host on a network.

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 identify the OS of the machines running in our network.

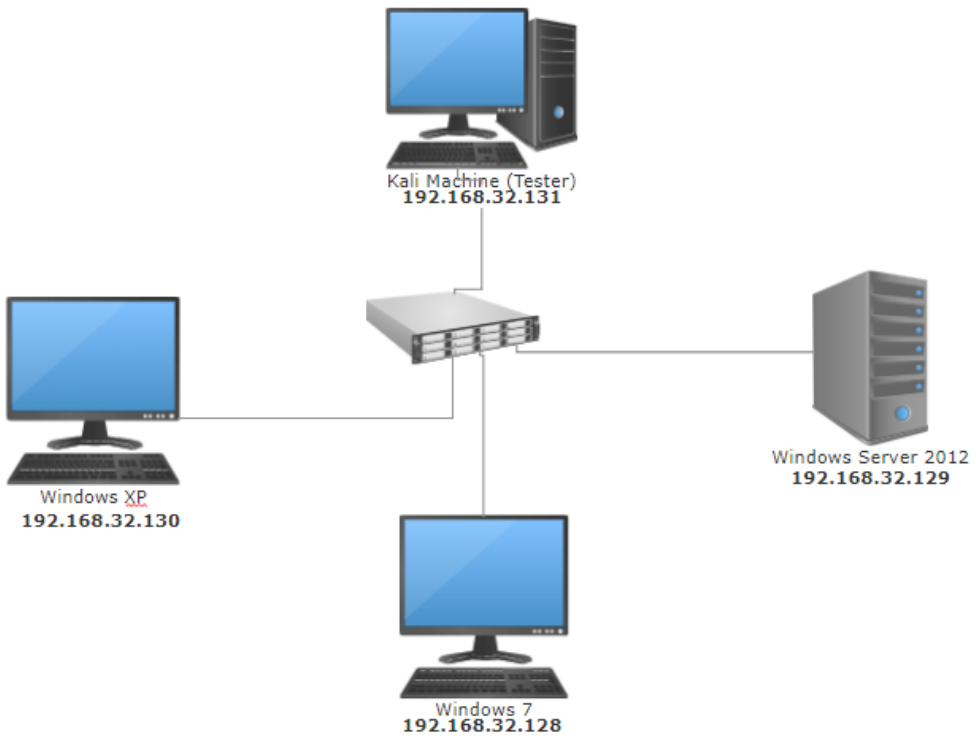


The results of the Network Scanning and Enumeration and OS Fingerprinting phases can be seen as below:

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)

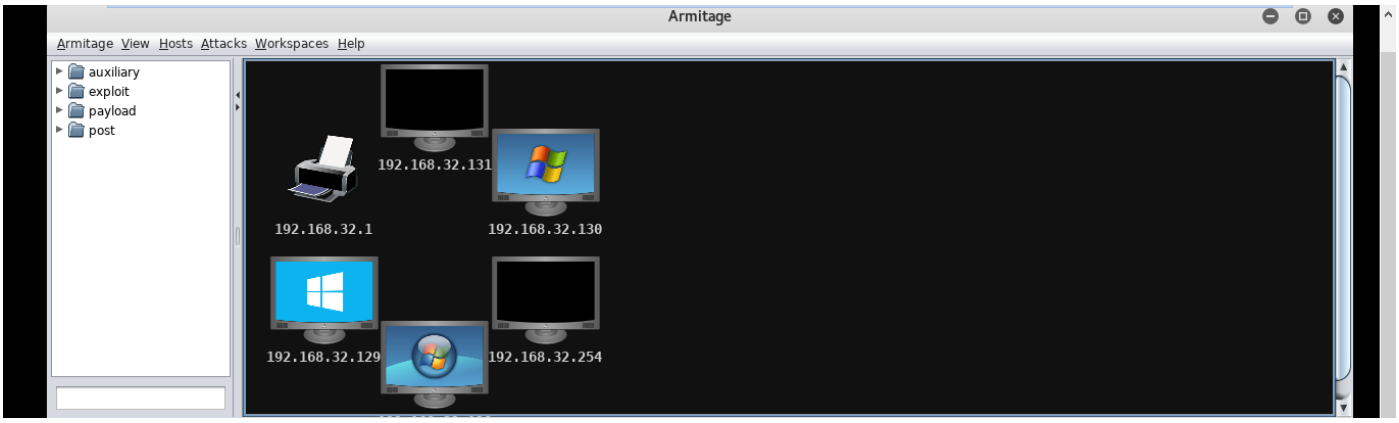
Vendor Reference: Offensive Security

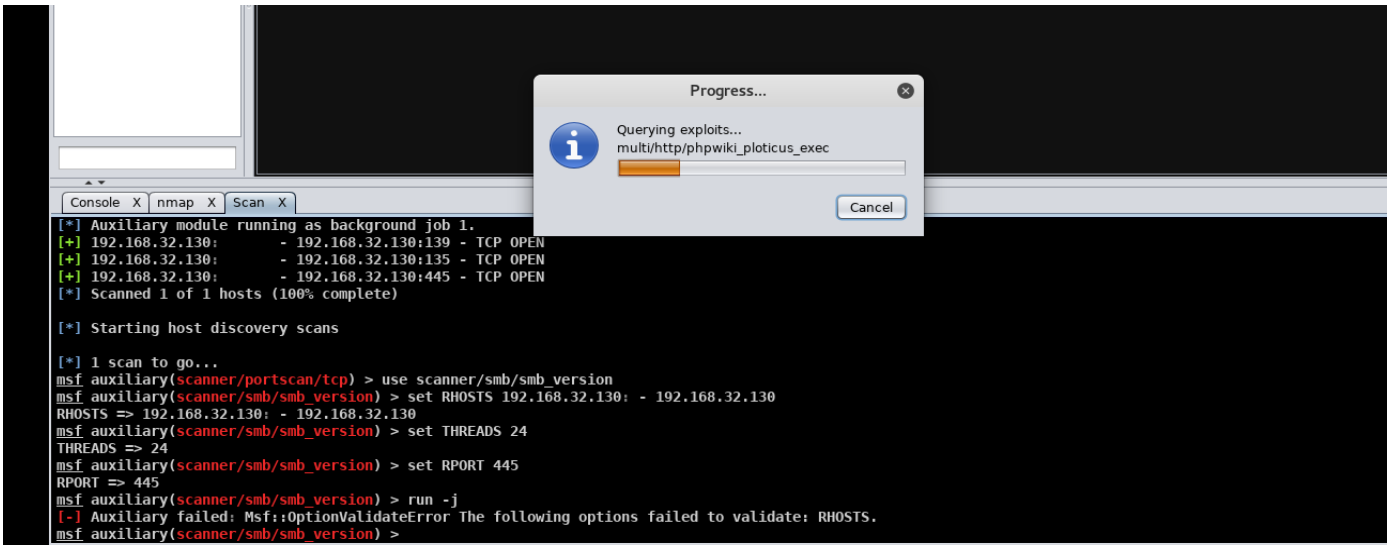
Methodology:

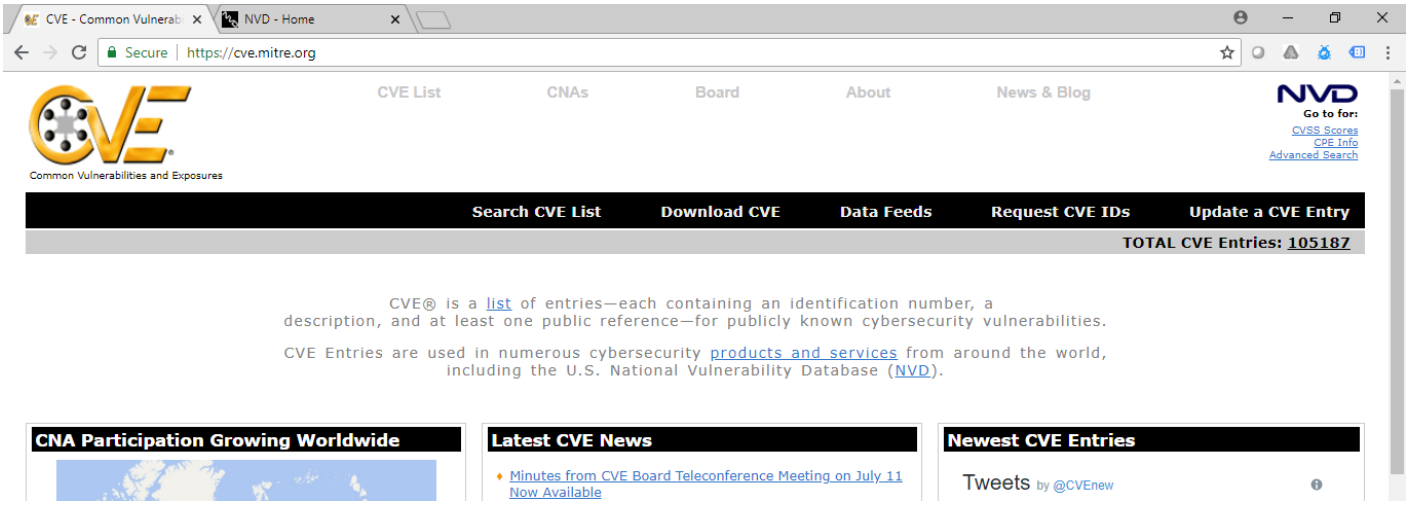
Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open source network security tool notable for its contributions to red team collaboration allowing for: shared sessions, data, and communication through a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

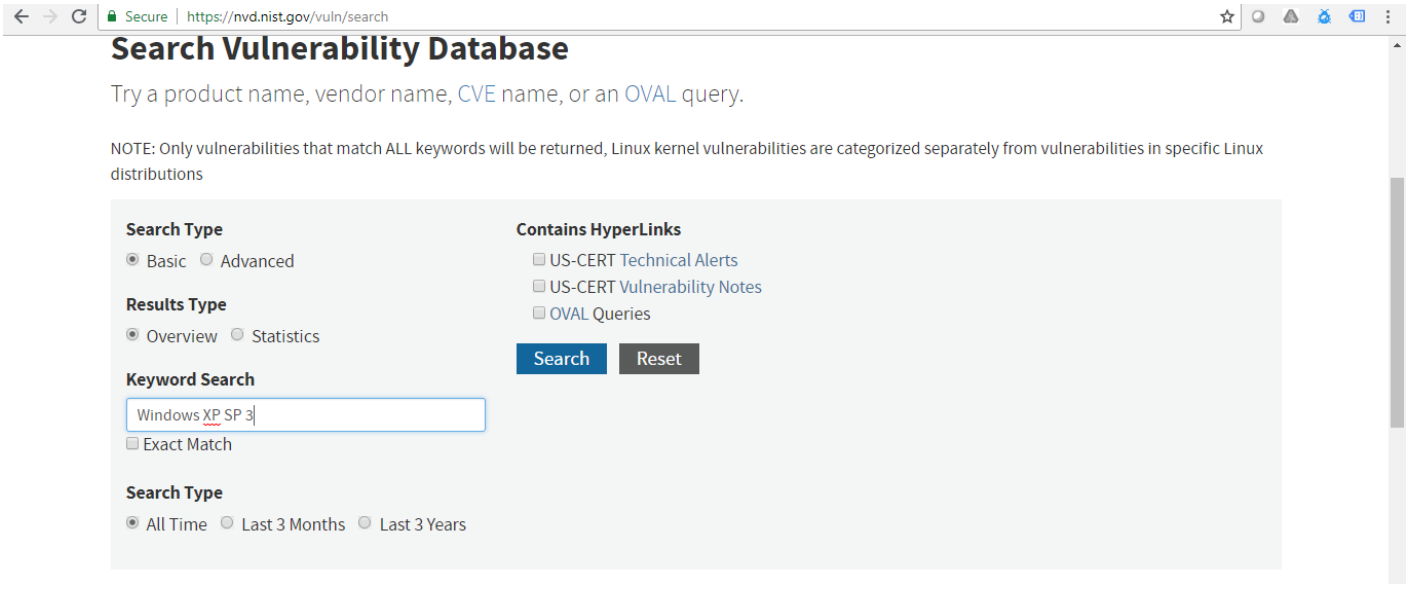
We used Metasploit Armitage to try and exploit the most common and popular vulnerabilities of the various Operating Systems in the network.

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.




Progress...
Querying exploits...
multi/http/phpwiki_ploticus_exec
Cancel
Console X
nmap X
Scan X
[*] Auxiliary module running as background job 1.
[+] 192.168.32.130: - 192.168.32.130:139 - TCP OPEN
[+] 192.168.32.130: - 192.168.32.130:135 - TCP OPEN
[+] 192.168.32.130: - 192.168.32.130:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Starting host discovery scans
[*] 1 scan to go...
msf auxiliary(scanner/portscan/tcp) > use scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.32.130: - 192.168.32.130
RHOSTS => 192.168.32.130: - 192.168.32.130
msf auxiliary(scanner/smb/smb_version) > set THREADS 24
THREADS => 24
msf auxiliary(scanner/smb/smb_version) > set RPORT 445
RPORT => 445
msf auxiliary(scanner/smb/smb_version) > run -j
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf auxiliary(scanner/smb/smb_version) >


CVE - Common Vulnerab
NVD - Home
Secure | https://cve.mitre.org
CVE List
CNAs
Board
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search
Common Vulnerabilities and Exposures
Search CVE List
Download CVE
Data Feeds
Request CVE IDs
Update a CVE Entry
TOTAL CVE Entries: 105187
CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).
CNA Participation Growing Worldwide
Latest CVE News
Minutes from CVE Board Teleconference Meeting on July 11 Now Available
Newest CVE Entries
Tweets by @CVEnew


Secure | https://nvd.nist.gov/vuln/search
Search Vulnerability Database
Try a product name, vendor name, CVE name, or an OVAL query.
NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions
Search Type
Basic Advanced
Results Type
Overview Statistics
Keyword Search
Windows XP SP 3
Exact Match
Search Type
All Time Last 3 Months Last 3 Years
Contains HyperLinks
US-CERT Technical Alerts
US-CERT Vulnerability Notes
OVAL Queries
Search
Reset

Vuln ID	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	(not available)

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

EXPLOIT DATABASE

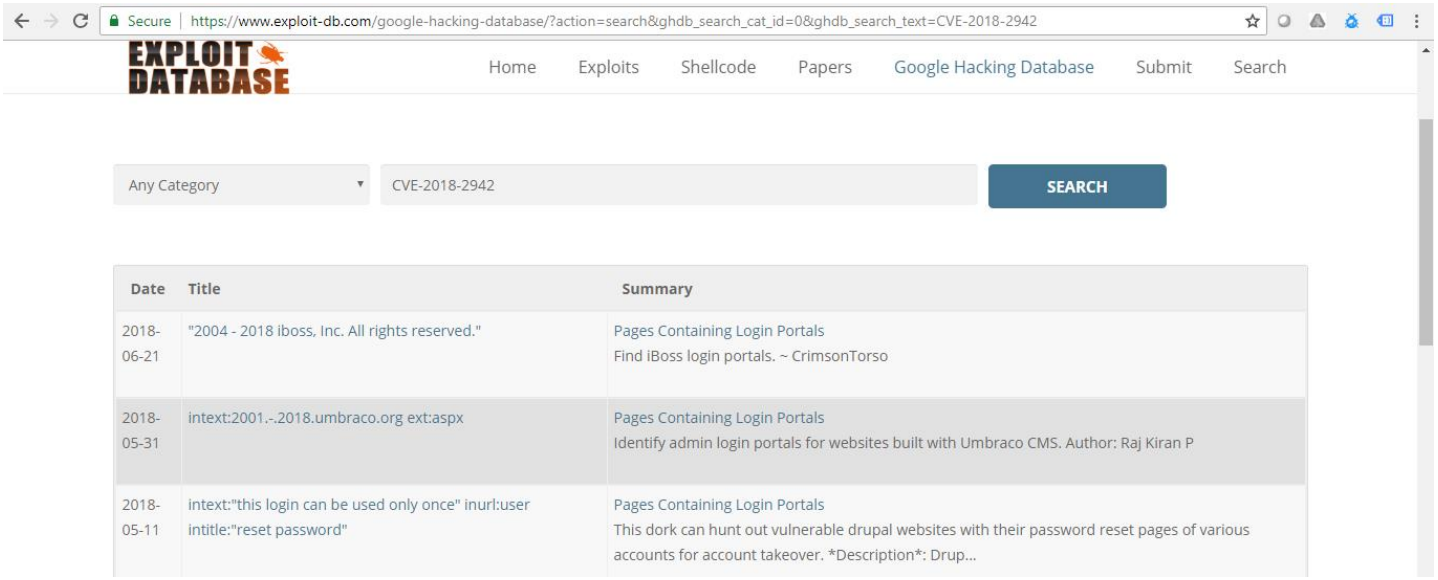
Home Exploits Shellcode Papers Google Hacking Database Submit Search

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

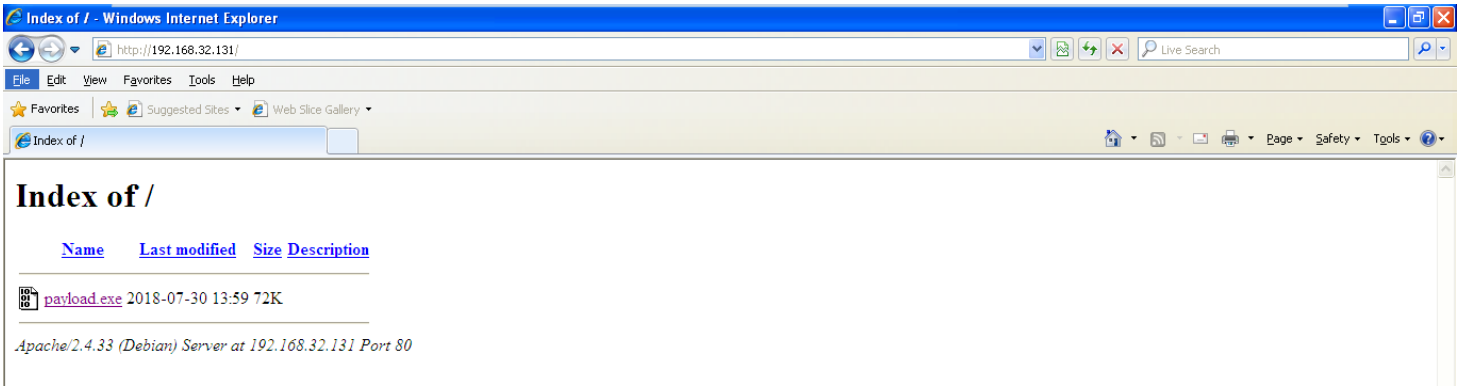


Tool Name: SetToolKit

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.




```
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)
```

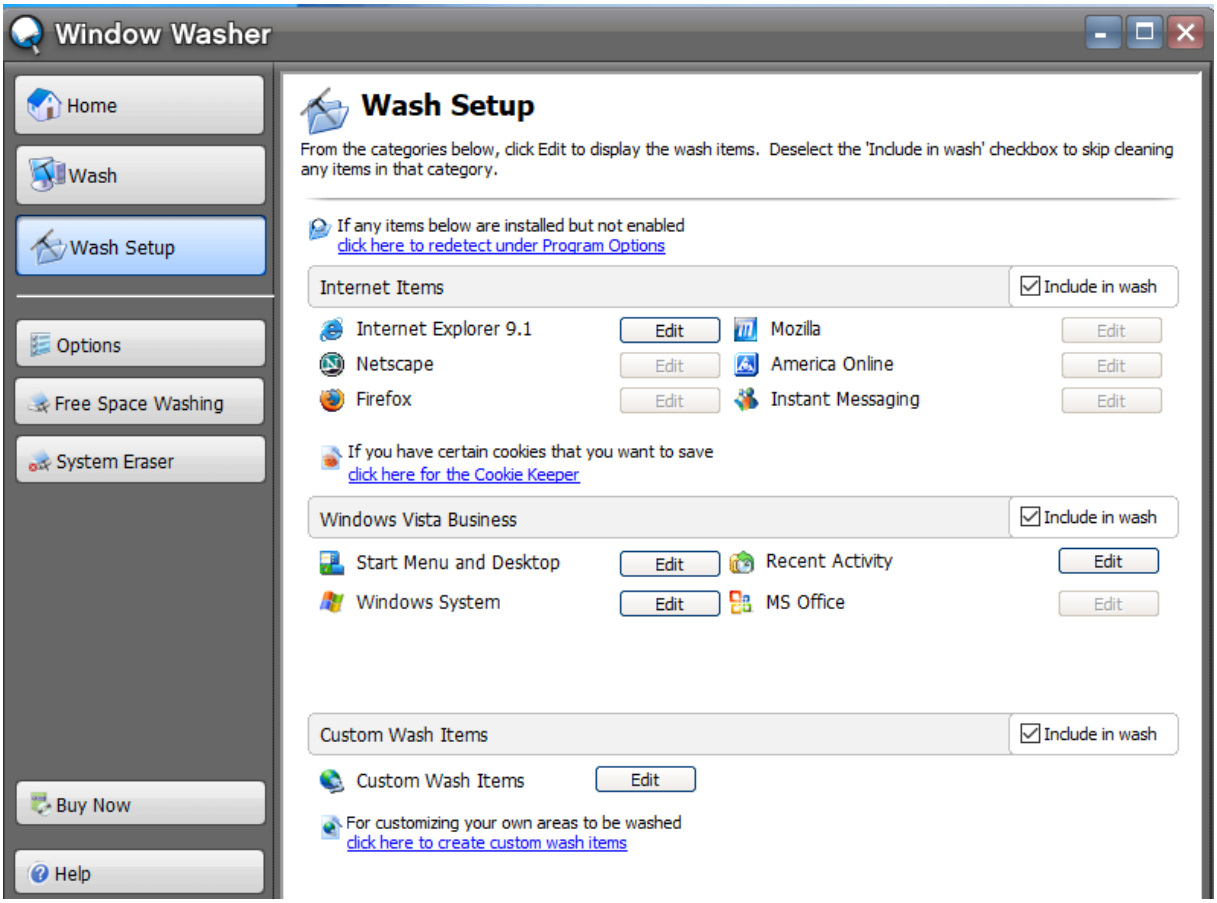
[Challenge 5:] Erasing Tracks:

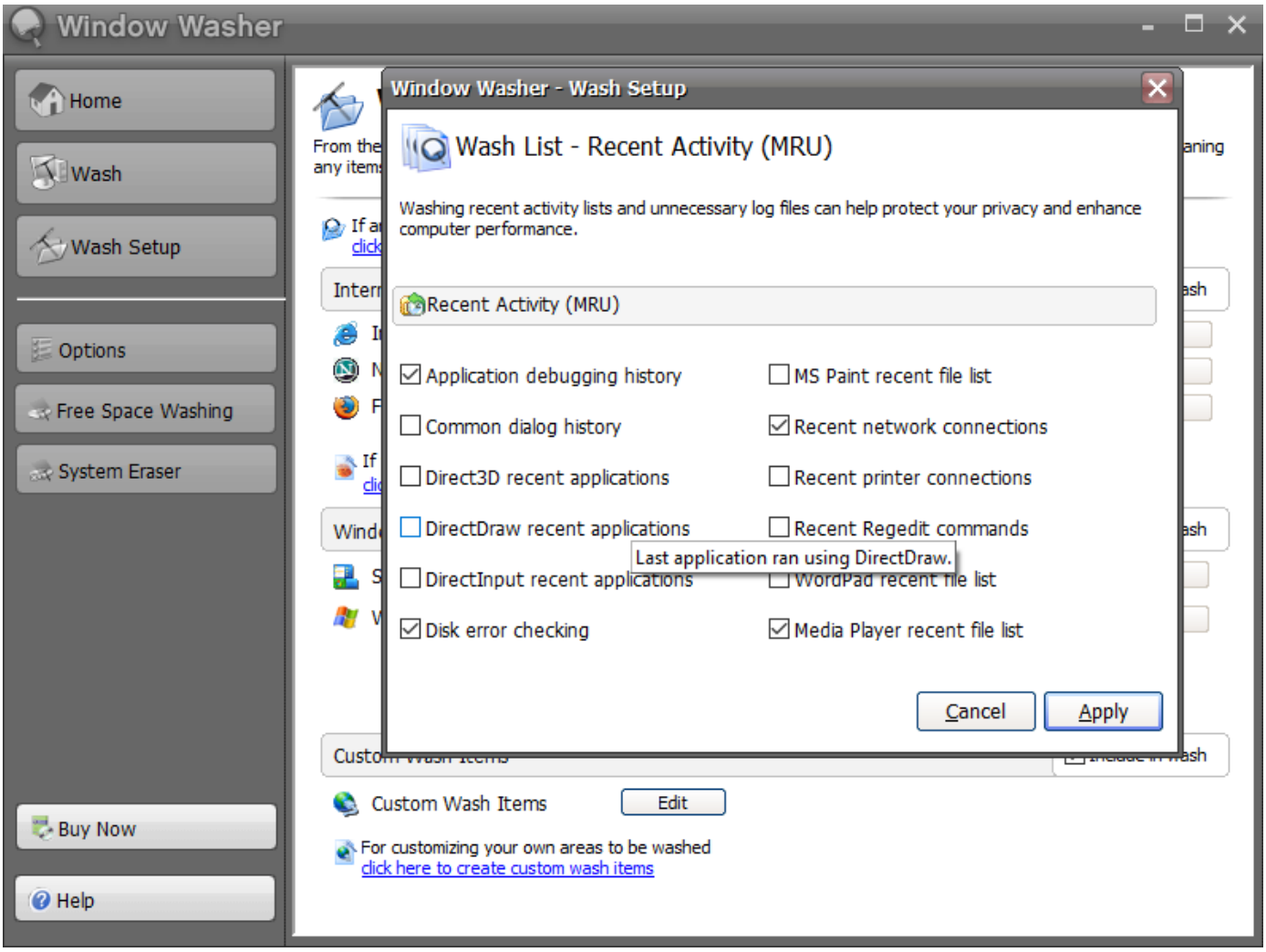
Tool Name: Window Washer

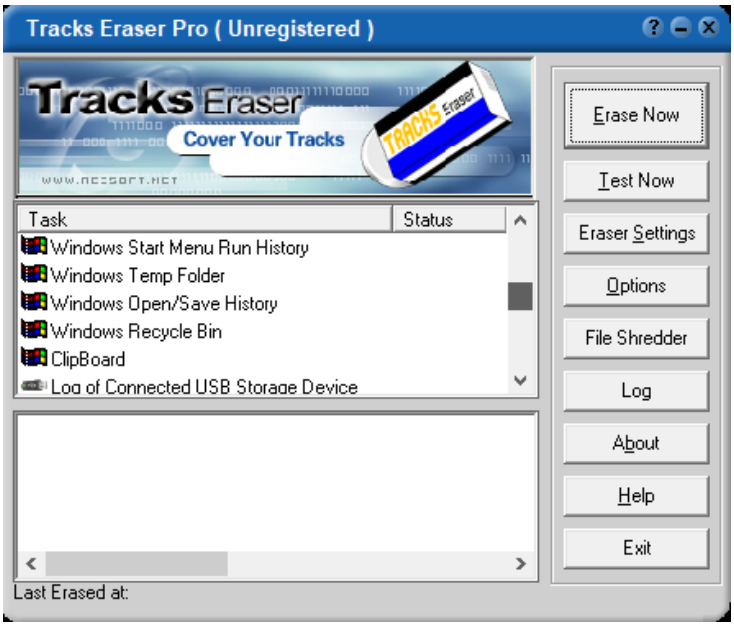
Vendor Reference:

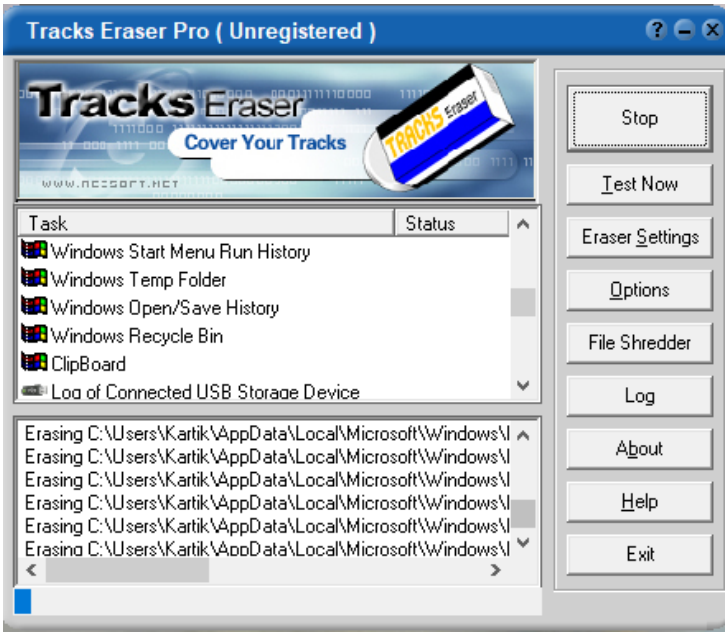
Methodology:

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.




Window Washer
Home
Wash
Wash Setup
Options
Free Space Washing
System Eraser
Buy Now
Help
Window Washer - Wash Setup
Wash List - Recent Activity (MRU)
Washing recent activity lists and unnecessary log files can help protect your privacy and enhance computer performance.
Recent Activity (MRU)
Application debugging history
MS Paint recent file list
Common dialog history
Recent network connections
Direct3D recent applications
Recent printer connections
DirectDraw recent applications
Recent Regedit commands
Last application ran using DirectDraw.
DirectInput recent applications
WordPad recent file list
Disk error checking
Media Player recent file list
Cancel
Apply
Custom Wash Items
Edit
For customizing your own areas to be washed
click here to create custom wash items


Tracks Eraser Pro (Unregistered)
Tracks Eraser
Cover Your Tracks
Task
Status
Windows Start Menu Run History
Windows Temp Folder
Windows Open/Save History
Windows Recycle Bin
ClipBoard
Log of Connected USB Storage Device
Erase Now
Test Now
Eraser Settings
Options
File Shredder
Log
About
Help
Exit
Last Erased at:


Tracks Eraser Pro (Unregistered)
Tracks Eraser
Cover Your Tracks
Task
Status
Windows Start Menu Run History
Windows Temp Folder
Windows Open/Save History
Windows Recycle Bin
ClipBoard
Log of Connected USB Storage Device
Erasing C:\Users\Kartik\AppData\Local\Microsoft\Windows\I
Stop
Test Now
Eraser Settings
Options
File Shredder
Log
About
Help
Exit

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/