A logo of a globe with a graduation cap

Description automatically generated

**Penetration Testing Report**

**(Metasploitable2)**

**Submitted by:**

|  |
| --- |
| **Names** |
| **Shady Mohamed Abdel Gawad** |
| **Hussein Al-Yemeni Zain Al-Din** |
| **Mohamed Ashraf Mohamed Lotfy** |
| **Abdel Rahman Ahmed Abdel Hamid** |
| **Omar Ahmed Badr** |
| **Ziad Alaa** |

**Under the supervision of:**

**Eng. Khaled Taha**

**Metasploitable Vulnerabilities Report**

**Executive Summary:**

**A vulnerability assessment and penetration test were conducted on one domain Metasploitable 2 to determine its exposure to a targeted cyber-attack. All tests were conducted in a manner that simulated a malicious attacker engaged in a cyber-attack against Metasploitable 2 with the following goals,**

**• Identify whether a remote attacker can penetrate defenses of Metasploitable 2.**

**• Determine the impact of a security breach of confidentiality and integrity of the**

**private data of the system, availability of information systems of Metasploitable 2 and internal infrastructure.**

**Security vulnerabilities that might give a remote attacker unauthorized access to sensitive data have been identified and exploited**

**Scope:**

|  |  |
| --- | --- |
| **IP address** | **192.168.21.129** |
| **Name** | **Metasploitable 2.0** |
| **System Type** | **Host** |
| **OS Information** | **Ubuntu 8.04 (hardy) on Linux kernel 2.6** |

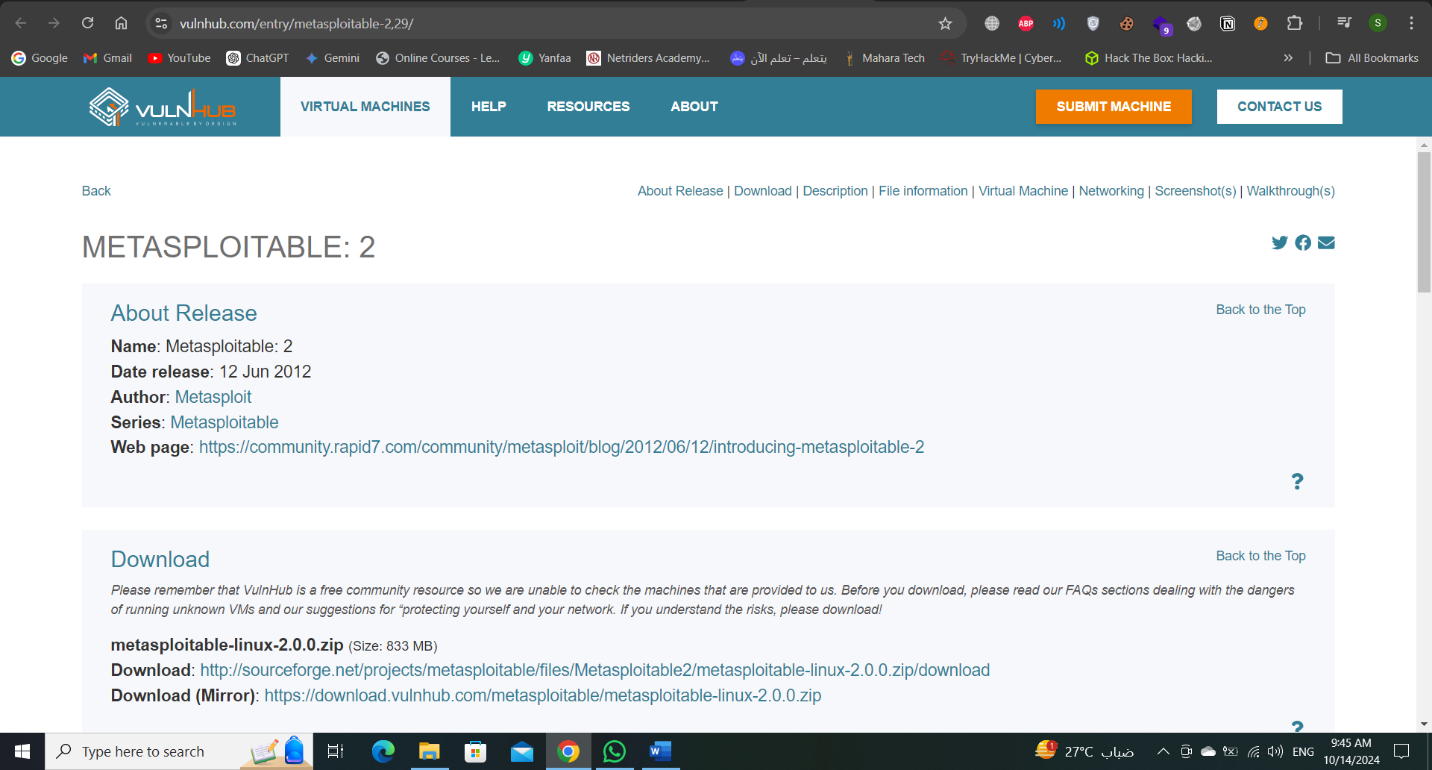
**Methodology:**

**Penetration testing tools and frameworks were used for the vulnerability assessment and penetration test including Nmap, Nessus Metasploit Framework, various information gathering tools, Kali Linux penetration testing tools and automated vulnerability scanners.**

**Summary of Findings:**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Vulnerability** | **Risk** | **Testing scale** |
| **1)** | **Detected a Bind Shell Backdoor** | **High** | **Exploited** |
| **2)** | **FTP Backdoor Detection** | **High** | **Exploited** |
| **3)** | **Password not Set for MySQL root User** | **High** | **Exploited** |
| **4)** | **Weak Credentials Used in VNC** | **High** | **Exploited** |
| **5)** | **Detected Backdoor in IRC** | **High** | **Exploited** |
| **6)** | **Default Credentials Used in Apache Tomcat** | **High** | **Exploited** |
| **7)** | **Weak Credentials Used in SSH** | **High** | **Exploited** |
| **8)** | **Anonymous FTP Login Enabled** | **Medium** | **Exploited** |
| **9)** | **Weak Credentials Used in FTP** | **Medium** | **Exploited** |
| **10)** | **Cleartext Authentication is Supported by FTP** | **Low** | **Not Exploited** |

**Installation of Machine:**

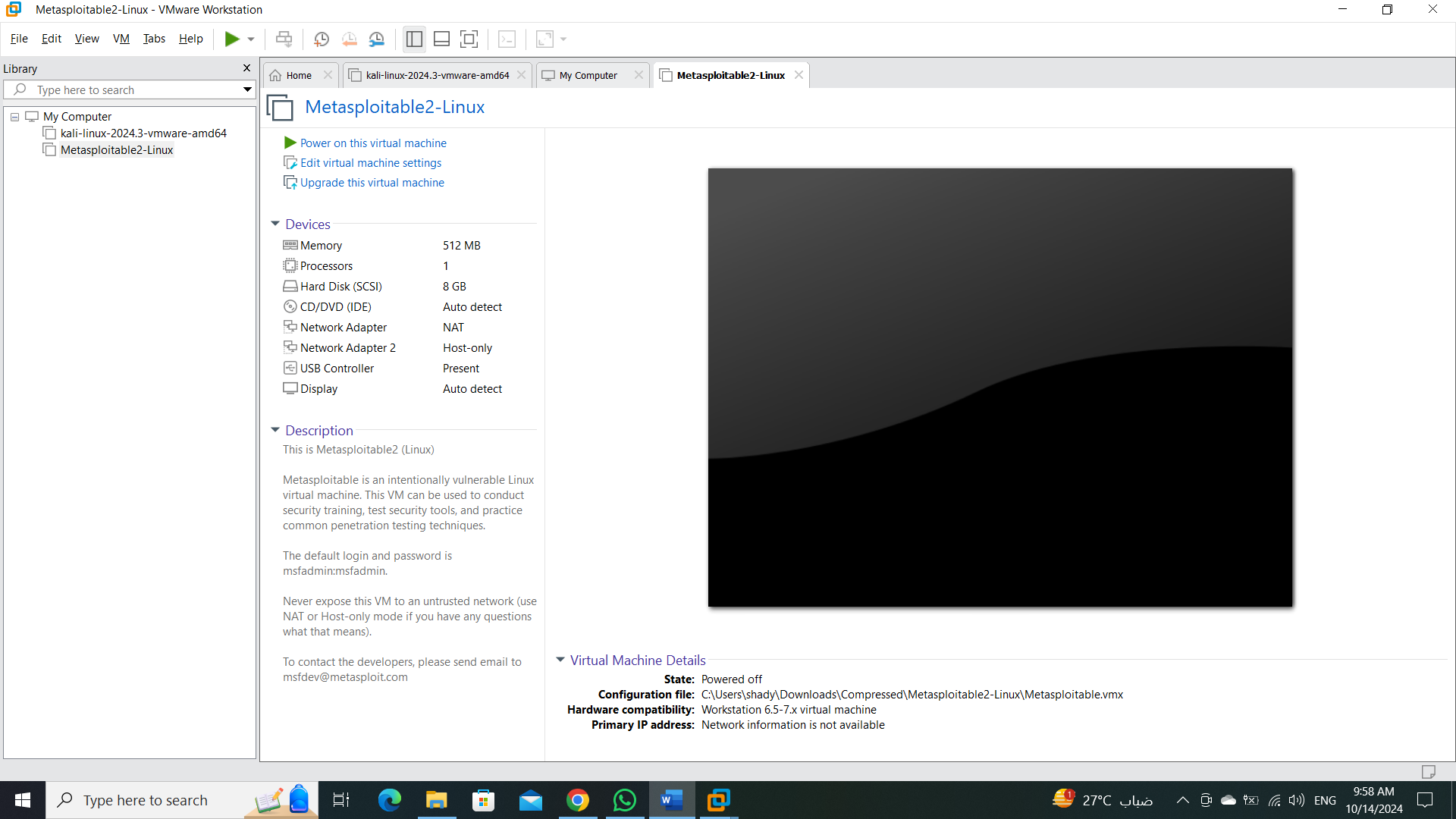
**We should have VirtualBox or VMware to install on it the machine that it became the target and should download metasploitable from VulnHub and download the mirror version to apply the penetration testing phase.**

**After downloading this version, go extract the file to get the files.**

**After this Operation, we should open the VirtualBox or VMware to install and open the machine to work**

صورة تحتوي على نص, لقطة شاشة, برمجيات, أيقونة الحاسوب

تم إنشاء الوصف تلقائياً**In home page , enter into “Open a Virtual Machine” and go to the path that the machine save in it and open the “.vmdk” format.**

صورة تحتوي على نص, لقطة شاشة, برمجيات, أيقونة الحاسوب

تم إنشاء الوصف تلقائياً

**We successfully install the machine and now we start to work on it.**

صورة تحتوي على نص, لقطة شاشة, برمجيات, برامج الوسائط المتعددة

تم إنشاء الوصف تلقائياً**We should open the machine and discovery it to understand what is it.**

**Once opened, it asks for a login, and it might be difficult, but the credentials (msfadmin/msfadmin) are provided in the last line, and we must take these credentials and log in with them so that we can deal with the machine, and also so that the machine can take an IP address and appear on the Internet, and thus I can carry out the Penetration testing phases with ease.**

صورة تحتوي على نص, لقطة شاشة, برمجيات, عرض

تم إنشاء الوصف تلقائياً

صورة تحتوي على نص, لقطة شاشة, برمجيات, الحاسوب

تم إنشاء الوصف تلقائياً**Once the machine is opened, we can go to Kali Linux to start working.**

**Phase 1: Footprinting and Scanning:**

صورة تحتوي على نص, لقطة شاشة, برمجيات, الحاسوب

تم إنشاء الوصف تلقائياً**To know the IP address of the machine, we enter the “ifconfig “command to show the IP to help us to make scanning and another operation.**

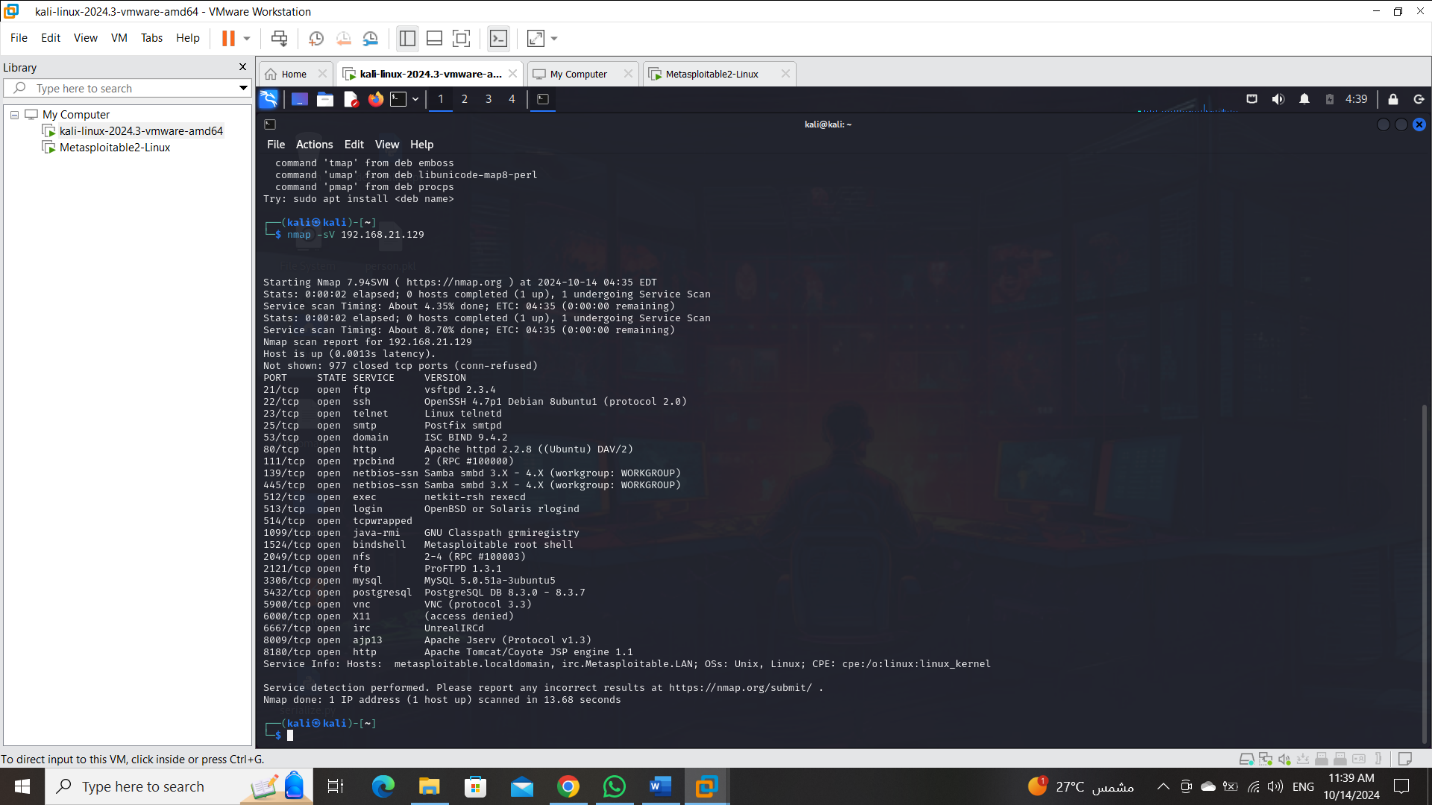
**We found the IP address => 192.168.21.129**

**And this IP address< we use to make the Footprinting and Scanning.**

**Let’s get things started with a simple Nmap scan.**

**. Nmap -sV 192.168.21.129**

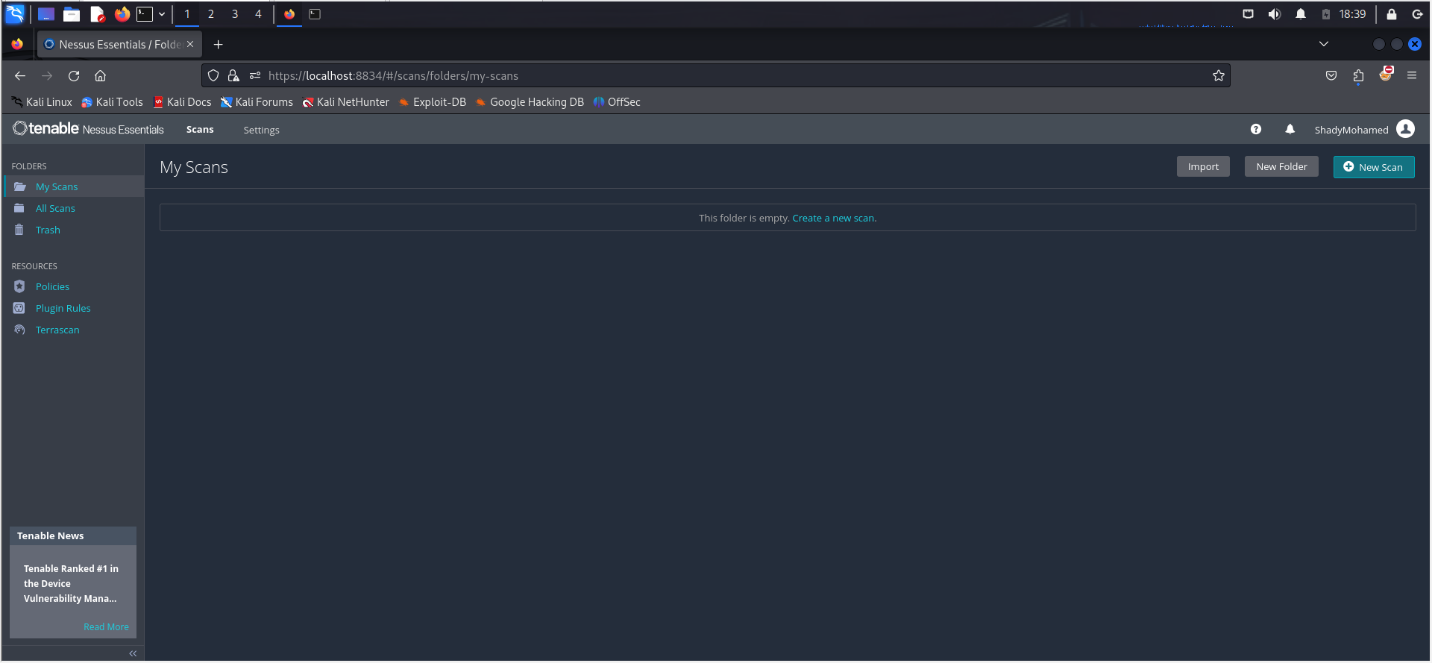
**“The -sV option in Nmap is used to perform version detection on open ports and when you use -sV, Nmap tries to determine the versions of the services running on those ports and in some cases, the service version may also provide clues about the operating system.**



**Now, we find many ports opened like FTP, SSH, HTTP and …. etc.**

**After that, we will try to assessment all of the vulnerabilities to make sure the riskiness of each vulnerability to decision which vulnerability that more riskiness to exploit it in the exploitation phase.**

**Phase 2: Vulnerability Assessments:**

**In the first, we need to install Nessus in the localhost and use it to assessments the vulnerability.**

صورة تحتوي على نص, لقطة شاشة, برمجيات, برامج الوسائط المتعددة

تم إنشاء الوصف تلقائياً

صورة تحتوي على لقطة شاشة, نص, برمجيات, برامج الوسائط المتعددة

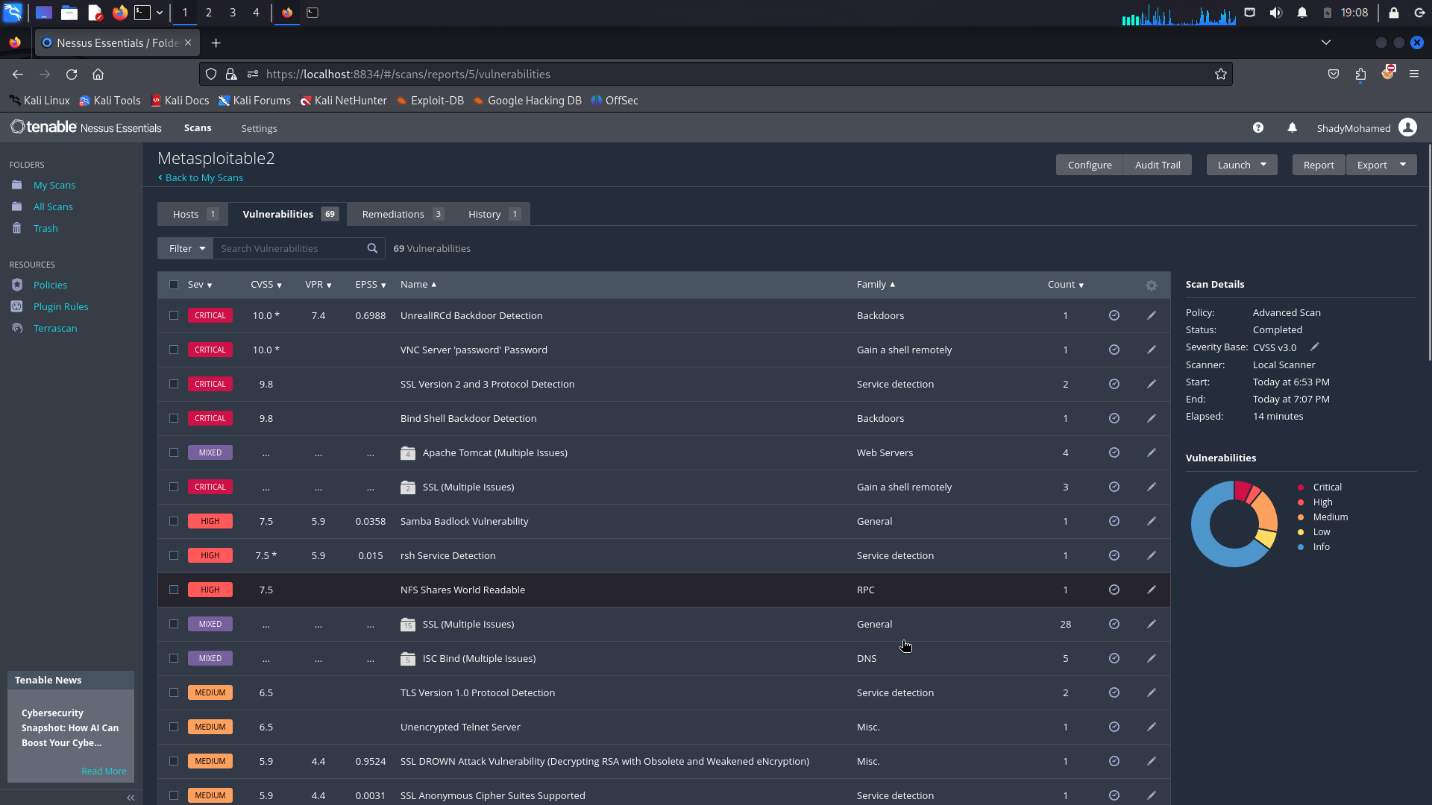
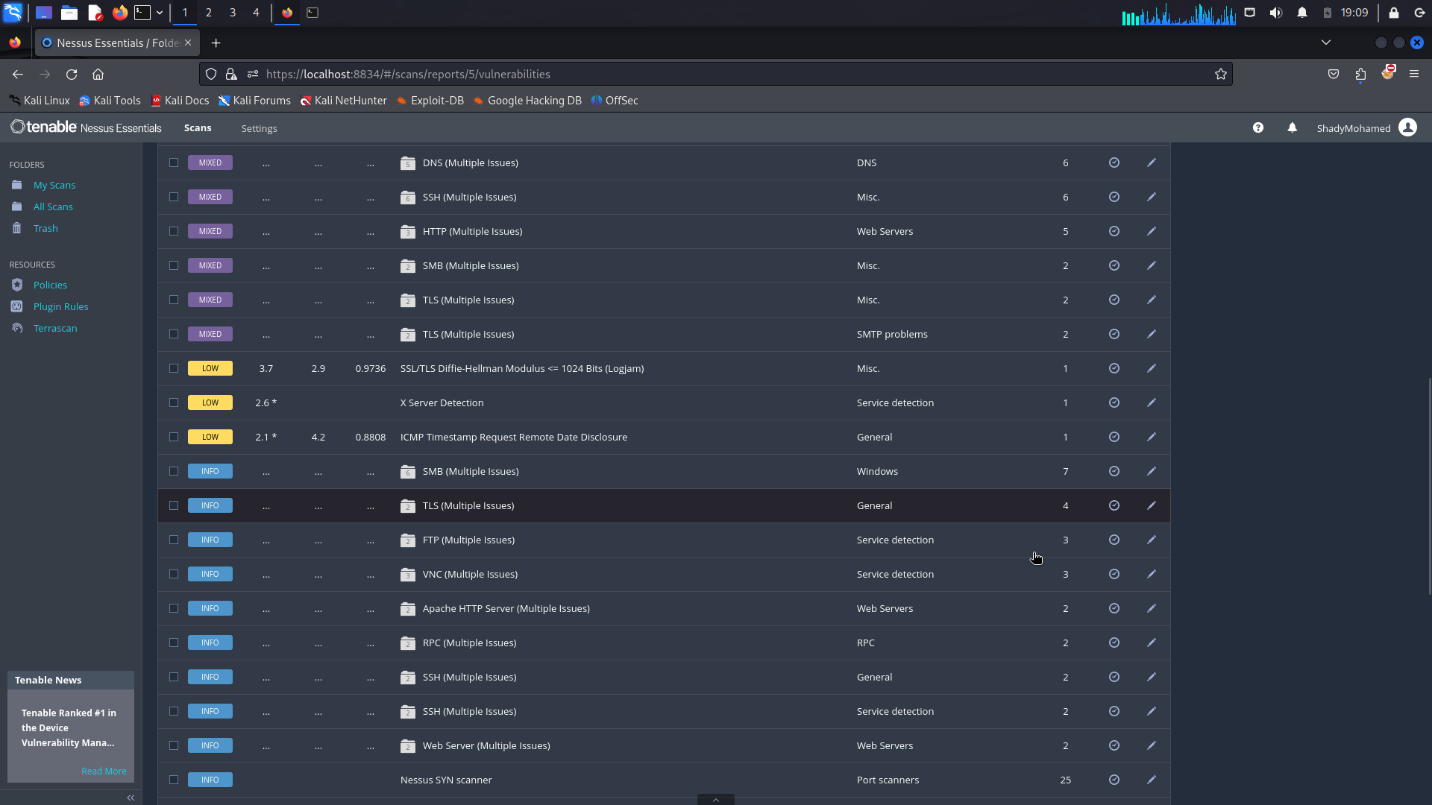
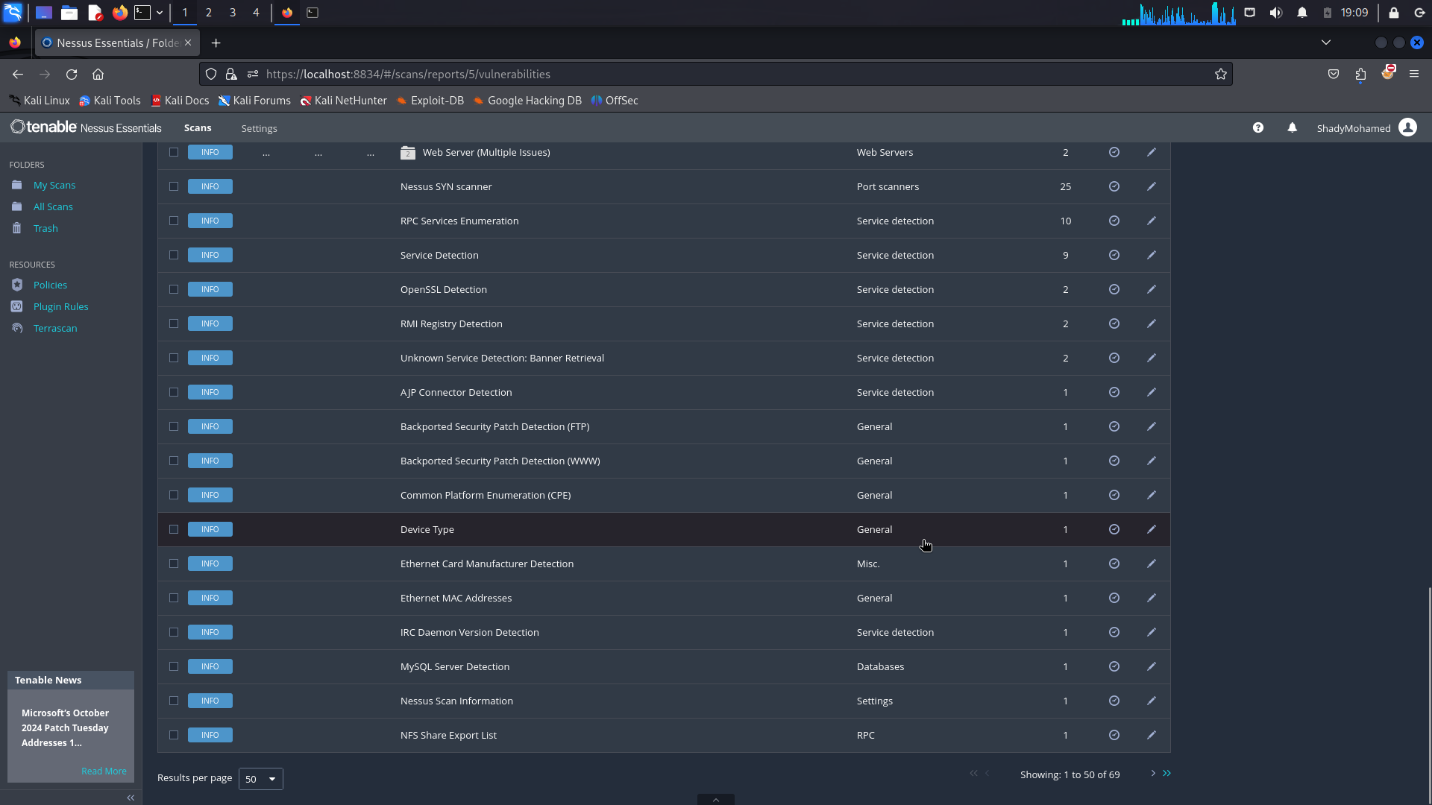
تم إنشاء الوصف تلقائياًصورة تحتوي على لقطة شاشة, نص, برمجيات, برامج الوسائط المتعددة

تم إنشاء الوصف تلقائياً

2

3

1

****

**After that assessment, we found that there are more than 60 Vulnerabilities between info, low, medium, high and critical.**

**So, in the exploitation phase-in the first- we focus on critical vulnerability and go to high and so on.**

**And we found that critical vulnerabilities make more damage in the system so we try to exploit those vulnerabilities to show how this damage can occur, and we try to find the mitigation of each vulnerability to fix this issue that it is caused.**

**Phase 3: Exploitation:**

**In this phase, we try to exploit each ports that see in the scanning phase. In the following, we show the vulnerability and its exploitation of this.**

1. **SMTP on port 25/tcp:**

**We try to use how SMTP enumeration scanner and what that does is it allows you to look for a valid for user account then we could potentially crack the passwords and have authenticated access to an SMTP server all right, so to do this we’re going to use Metasploit.**

**We use grep to show the scanner type and then we’re going to search SMTP.**

**And after this, we use the smtp\_enum.**

**We should show option because sometimes we find the options that are required to make the exploit.**

**We found “RHOST” that required and no value in here, so we should set the “RHOST” option by the target machine.**

**And exploit this payload.**

**This problem may allow an attacker to steal a victim’s emails.**

