


# SSH Penetration Testing

 [medium.verylazytech.com/ssh-penetration-testing-be4fc8517286](https://medium.verylazytech.com/ssh-penetration-testing-be4fc8517286)

Very Lazy Tech 

9 сентября 2024 г.

Top highlight



Very Lazy Tech 

Secure Shell (SSH) is a widely used cryptographic protocol designed for secure communication over an unsecured network. Its primary use is for remote server management, secure data transfers, and remote command execution. However, as with any service, it can be vulnerable to various types of attacks. This guide delves into SSH penetration testing techniques, exploiting its vulnerabilities, and applying real-world methods to enhance your offensive security skills.



Photo by on

This article is tailored for professionals aiming to improve their understanding of SSH's security mechanisms while enhancing their penetration testing toolkit.

## Lab Setup

Before jumping into SSH exploitation techniques, it is essential to have a lab setup for practice.

- : Ubuntu Server (192.168.31.205)
- : Kali Linux (192.168.31.141)

SSH is installed by default on most Linux distributions, and in this setup, we'll exploit it using the above machines.

```
sudo apt install openssh-server
```

Verify the SSH service:

```
sudo systemctl ssh
```

## Enumeration

---

**Enumeration** is the first and most crucial step in penetration testing. Nmap can be used to detect the version of SSH running on a target.

```
nmap -sV
```

If SSH is detected on the default port **22**, it's crucial to note the version as some older versions may have known vulnerabilities.

## Password Cracking Using Hydra

---

Hydra is a powerful tool for brute-forcing services like SSH.

Prepare a username and password list:

```
hydra -L users - pass . ssh
```

Once Hydra cracks the password, log into the SSH service:

```
ssh username.168.31.205
```

**Best Practice:** For real-world testing, make sure to use custom wordlists derived from intelligence gathering on your target.

## Exploiting SSH with Metasploit

---

For SSH penetration testing, **Metasploit** provides built-in modules that make the process more efficient.

```
use exploit/multi/ssh/sshexec rhosts 192.168.31.205 username pentest password 123exploit
```

**Pro Tip:** Use Metasploit to automate post-exploitation tasks once inside the machine.

## Key-based Authentication and Attacks

---

SSH key-based authentication is a more secure alternative to password authentication. However, it can still be exploited if misconfigurations exist.

:

ssh-keygen

:

sshid

: If you can steal the private key (`id_rsa`), SSH can be bypassed:

```
ssh -i id_rsa username.168.31.205
```

## Port Redirection

---

Port redirection can be used to pivot through compromised hosts. For example, if SSH is available but a web application is running on an internal port, you can set up local port forwarding:

```
ssh -L . username..
```

Access the internal web app via `http://localhost:8080` on your attacker machine.

## Nmap SSH Brute-Force Script

---

Nmap has built-in scripts to automate brute-force attacks against SSH:

```
nmap ssh-brute - .
```

You can customize the username and password files to improve success rates:

```
nmap
```

## Post-Exploitation with Metasploit

---

Once you've gained access to an SSH session, leverage **post-exploitation modules** for persistence and data exfiltration:

```
use post/linux/manage/sshkey_persistence session 1exploit
```

Another effective module is **ssh\_creds**, which retrieves SSH keys from the compromised machine:

```
use post/multi/gather/ssh_creds session 1exploit
```

## Advanced Techniques

---

- : If you find active SSH sessions, you can hijack them with tools like SSH hijacker.
- : Use tools like `ssh2john` and John the Ripper to crack SSH private key passphrases.

```
ssh2john id_rsa > sshhash john --wordlist=share/wordlists/rockyou. sshhash
```

: Send a reverse shell to gain complete control of the system:

```
ssh pentest.168.31.205
```

## Key Takeaways

---

1. : Always identify the SSH version and configuration.
2. : Key-based authentication is harder to crack but not impossible.
3. : Gaining initial access is only the first step — post-exploitation can yield more valuable information.
4. : These techniques can be game-changers in internal network pivoting.

SSH is a critical protocol in modern infrastructure. As a penetration tester or security researcher, mastering SSH attack vectors is crucial. From password brute-forcing with Hydra to key-based authentication exploits and advanced post-exploitation techniques with Metasploit, this guide has covered practical tools and methods to enhance your security testing. Always remember, the success of any penetration test lies in the precision of your enumeration and the efficiency of your attack strategy.

**Secure Shell (SSH) is a widely used cryptographic protocol designed for secure communication over an unsecured network...**

---

[buymeacoffee.com](https://buymeacoffee.com)