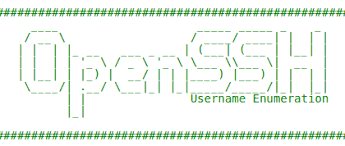


Systems and Network Programming(C/Python)

(IE2012)

Linux Exploitation Project



OpenSSH 2.3 >7.7 - Username Enumeration

CVE 2018-15473

**Introduction**

What is Openssh?

Openssh also known as OpenBSD secure shell is a suite of secure networking facilities based on the protocol SSH (secure shell) and it provides a secure channel over an unsecured network for a client and server architecture. It is a free open source set of tools that is used to provide a secure and encrypted communication over a network using the ssh protocol.

What is User Enumeration?

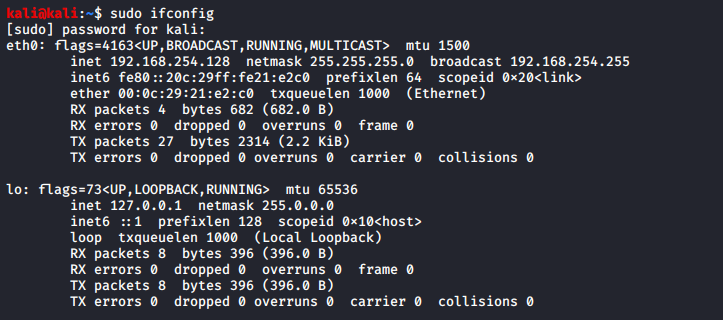
Username Enumeration is when a malicious actor tries to use brute force techniques to try to retrieve valid usernames from a web application. The web applications are mostly vulnerable to these attacks on login pages, registration pages and password logins. If the system is vulnerable to the username enumeration attack, the attacker may be able to obtain a list of existing usernames in the system by submitting input (valid and invalid user names) and analyzing the server response (error messages). The attacker can then run a dictionary attack to further exploit the obtained information. The main goal of Username Enumeration is to gain access to a system. Since most sites use [password authentication](https://guides.codepath.com/websecurity/Password-Authentication), knowing the username is half of the requirement for logging in. Once a set of valid usernames have been identified, attackers can use techniques such as [Brute Force](https://guides.codepath.com/websecurity/Brute-Force) and [Dictionary Attacks](https://guides.codepath.com/websecurity/Dictionary-Attacks) to guess the passwords. Many of the passwords will be strong enough to defend against these attacks, but with a long list of usernames, many of them will certainly use weak passwords and be vulnerable. And then the attacker will easily be able to exploit the system.

**OpenSSH 2.3 <7.7 Username Enumeration**

OpenSSH 2.3 < 7.7 username enumeration is a remote linux vulnerability which was found on the 21st of August in 2018 and the exploit code was written by Justin Gardener. A small defect was found on the OpenSSH server and it was recently exposed by researchers when they were trying to enumerate registered usernames on the server by exploiting the way the server behaves on forged requests. When there is a username that doesn’t exit. It would create an authentication failure. If incase the user exists the outcome would be different. This little misconfiguration leads to username enumeration and all the OpenSSH servers prior to 7.7 are vulnerable. What an attacker can simply do is to create a list and perform a mass-enumeration attack on the server and try to login to a system with the help of enumerated usernames and the same thing could be performed with passwords. This vulnerability is assigned the ID: CVE-2018-15473.

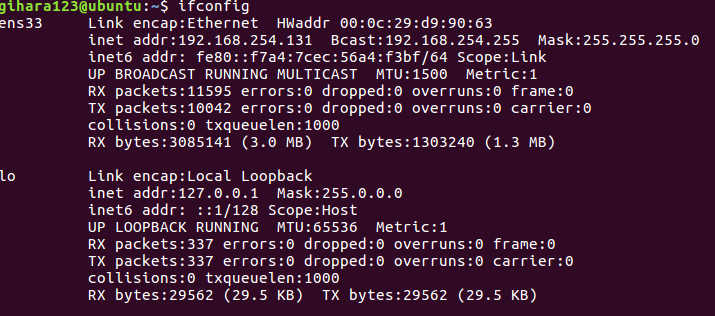
Since this is a remote linux vulnerability, two linux platforms will be needed. For this exploit Vmware will be used and two virtual machines will be created. One virtual machine would be Kali Linux and the other virtual machine would be Ubuntu.

First we have to find the IP addresses of both machines.



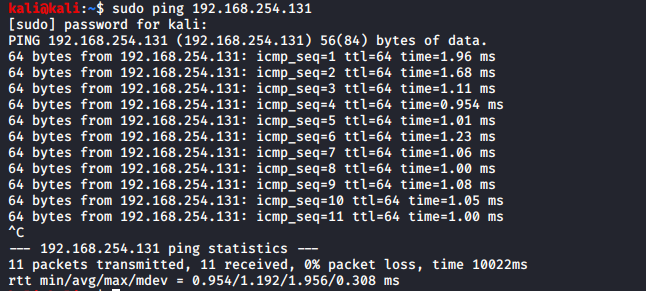
The IP address of the Kali Linux machine : 192.168.254.128

IP address of the Ubuntu machine : 192. 168.254.131

****

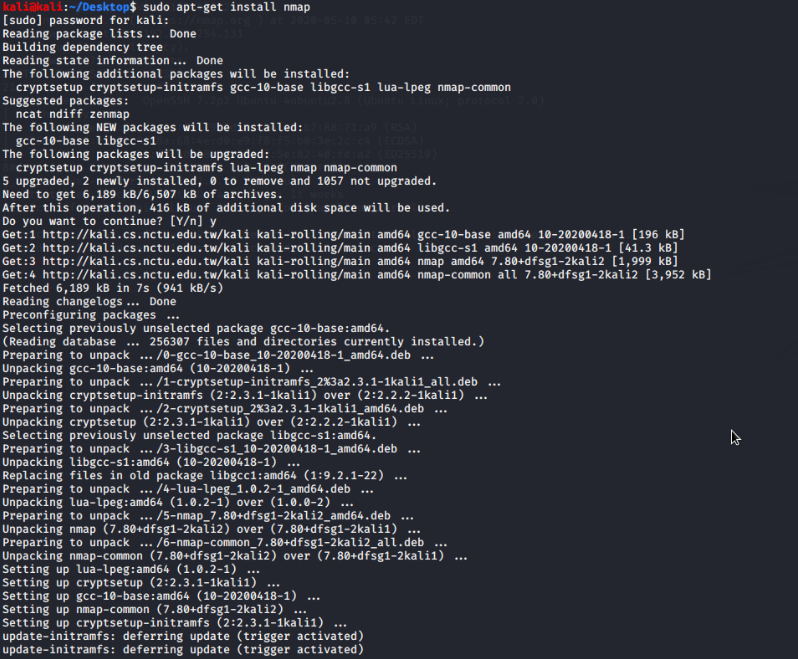
So now we can see that both the IP addresses are in the same range. The kali Linux machine can communicate with Ubuntu.The attacker machine is the Kali Linux machine and the Victim machine is Ubuntu. Now the Kali machine must be pinged to the Ubuntu machine.

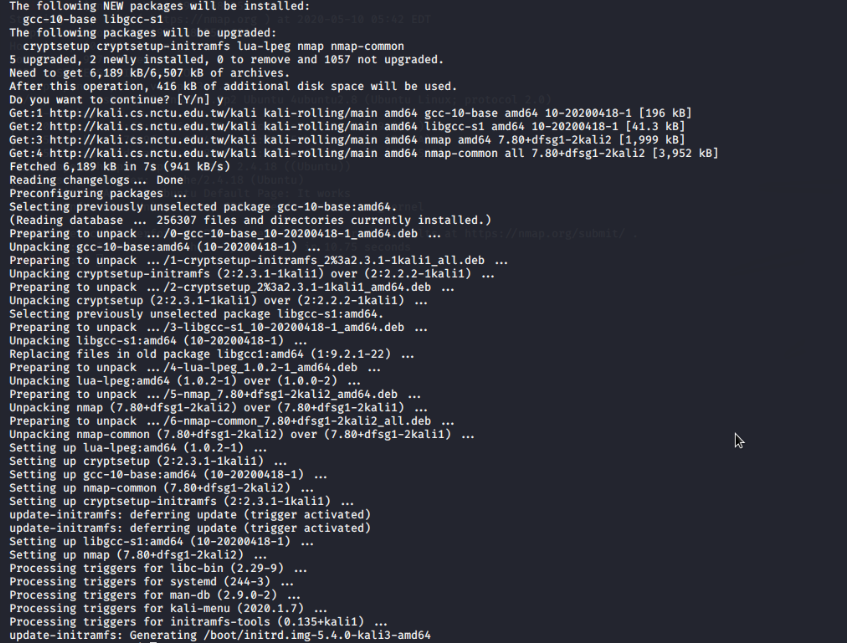
Pinging from kali to Ubuntu. The attacker machine is having a connection with the victim machine.



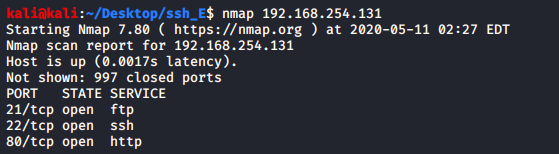
Next we run a nmap scan on the victim’s machine using the IP address. Nmap is a powerful security tool which is used to discover information regarding machines in a network. It can detect everything from running services and open ports. Nmap also helps in securing your network and ensures that the servers are properly configured and there are no unsecure ports.

To run nmap first we need to install nmap to the kali machine.

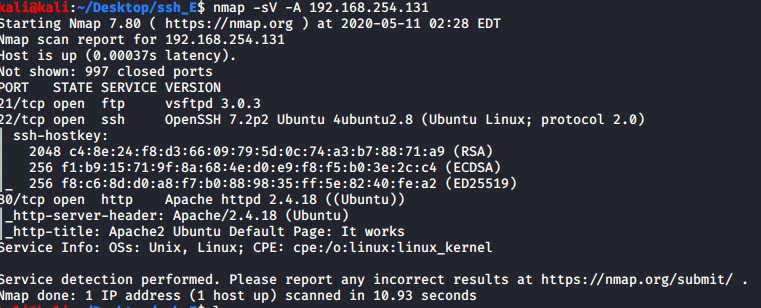




Then we run a nmap scan for the IP address of the Ubuntu machine.

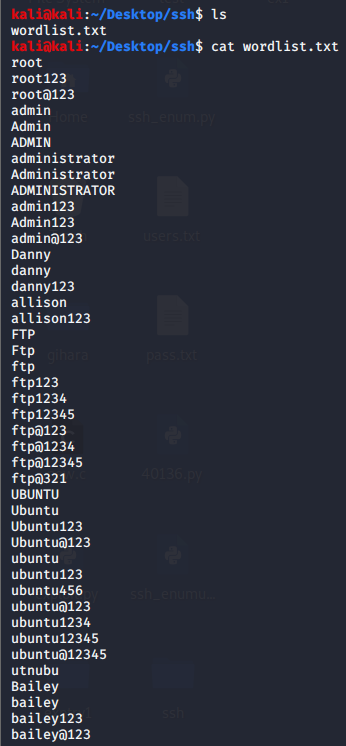


If we want to check more info about the ports, the versions and the os we can run a custom nmap scan



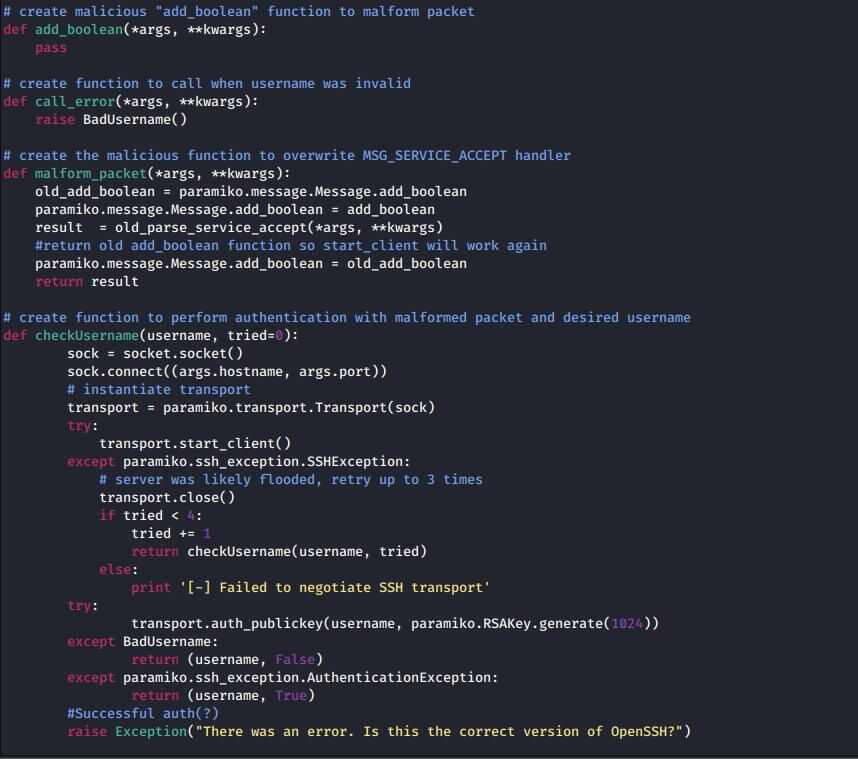
Now we can see the service version on the victim’s machine and it seems to be OpenSSH 7.2p2 running in the 22 port and we are going to try the Username Enumeration for that range.

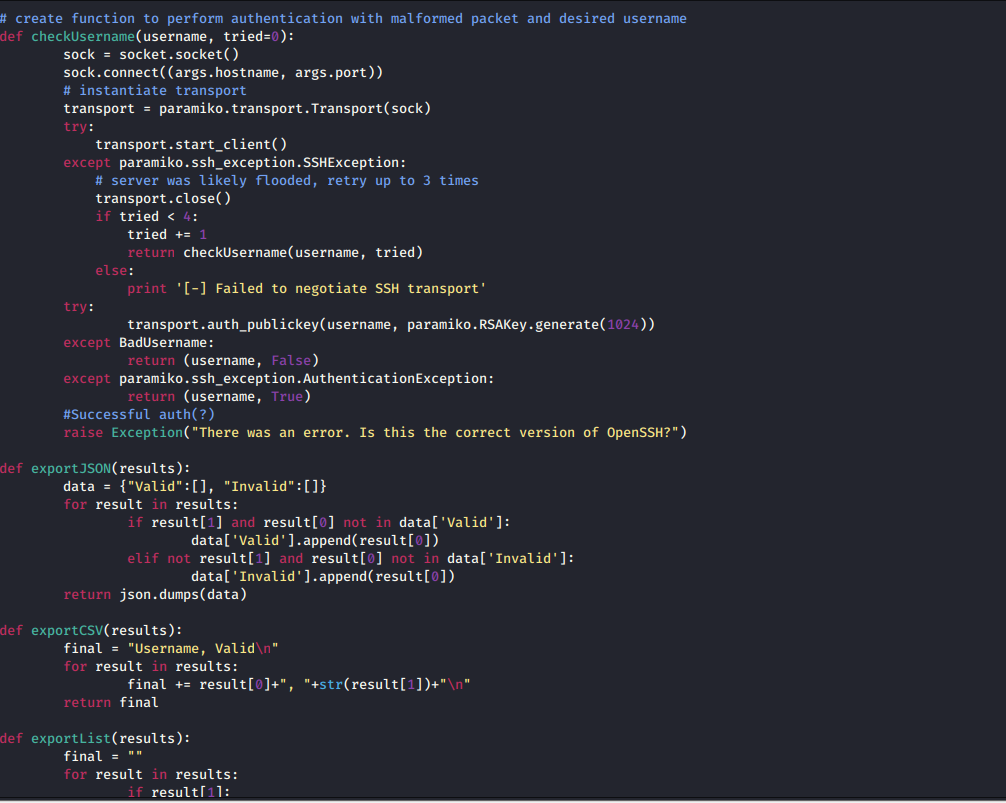
To do the Username Enumeration we need a wordlist. This is the wordlist that we are going to use.

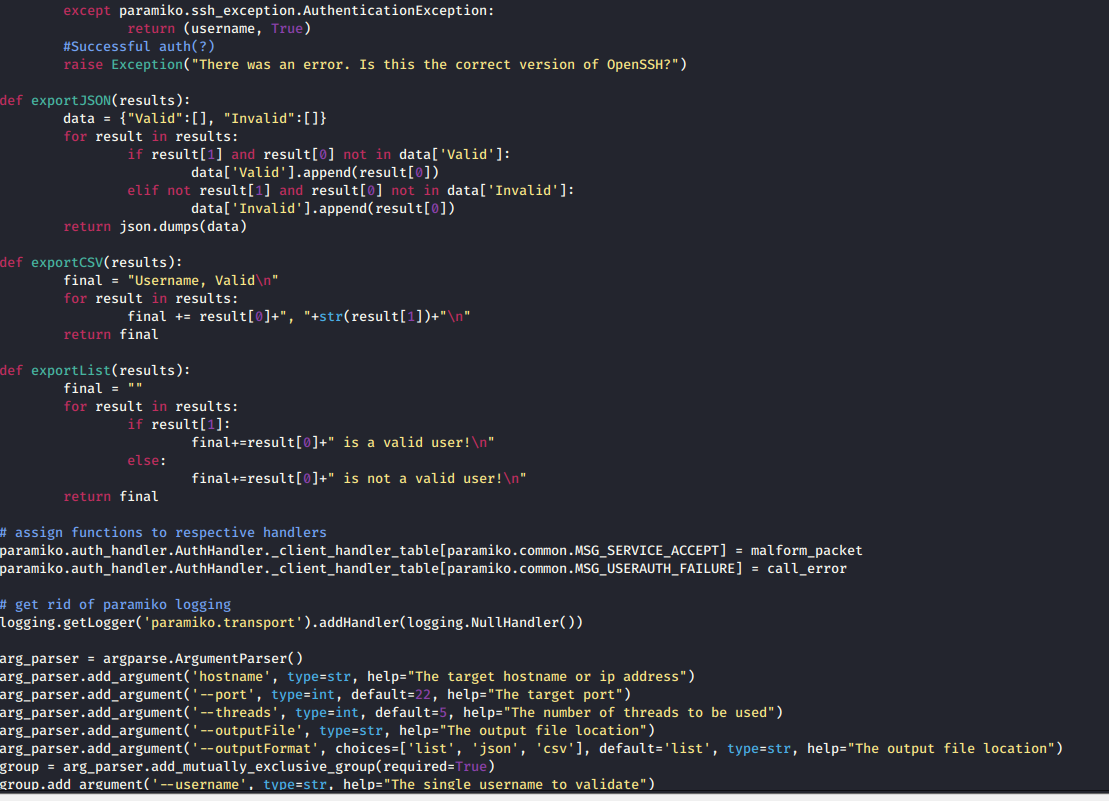


Given below is the python code for OpenSHH 2.3 < 7.7 Username Enumeration





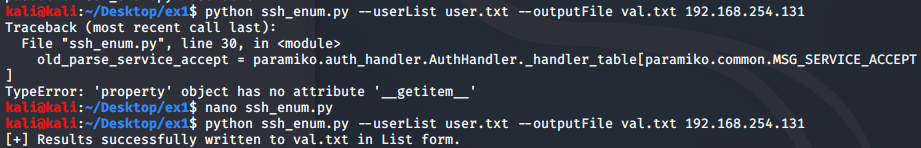








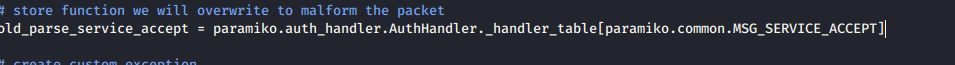
Then we have downloaded the python code for the exploit and saved it as ssh\_enum.py. and then we run it

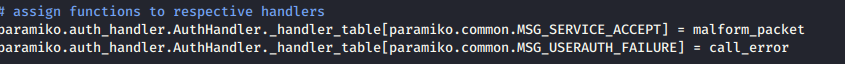


Then we would be able to see an error. To fix the error we have to change the python code.

Paramiko is a python implementation of ssh providing both client and server functionality. It is a pure python interface that works around the ssh functionality.

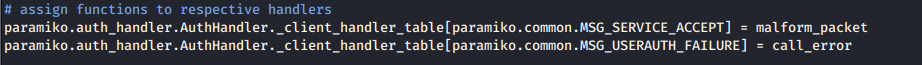
This is the fault in the code.





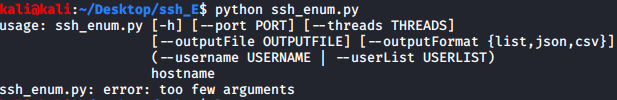
In order to find a solution to the error we have to change the code in this method.

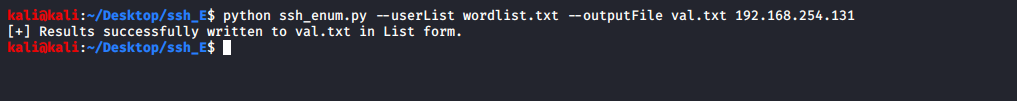
C:\Users\acer\Desktop\Screenshots for assignment snp\paramiko2.PNG



We have specified a client server.

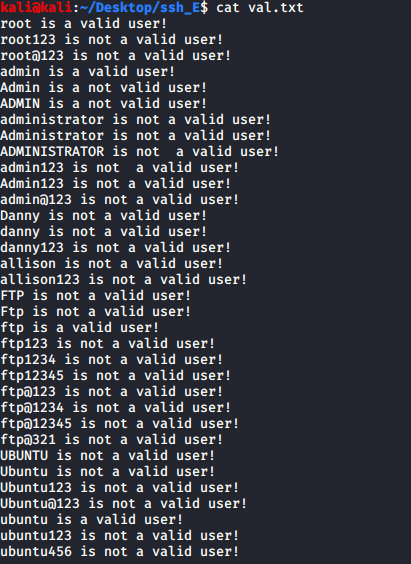
Now as we run the python ssh\_enum.py command we would get a different output



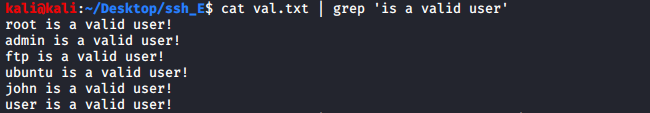


Now we can see that the results have been successfully written to a text file named val.txt.

We could also check the names that are included in val.txt using the cat command



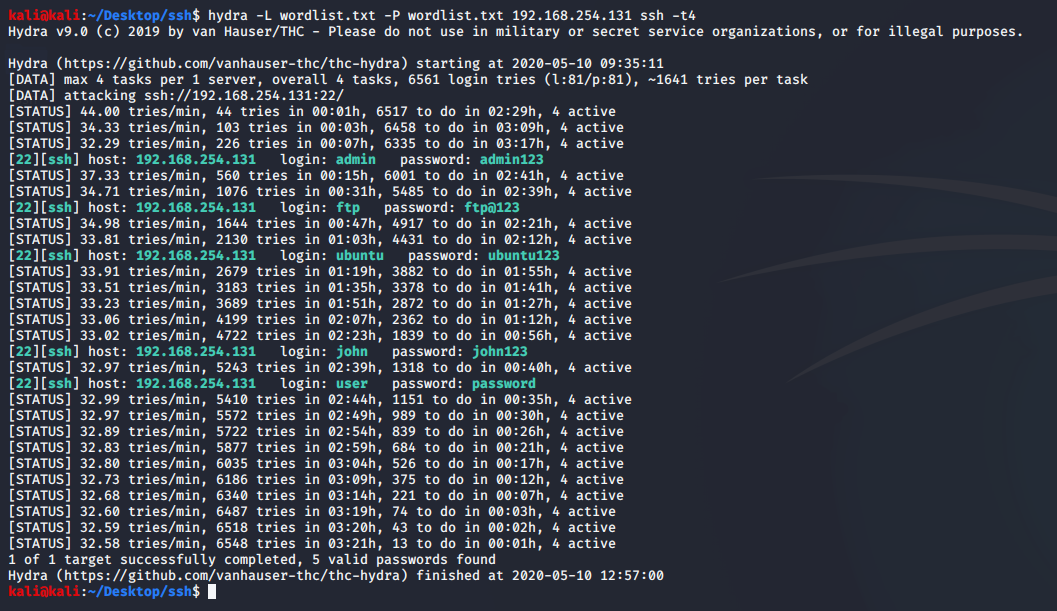
Now if we only want to select the users who are valid. We could use the grep command. The grep command selects the sentences which are selected inside the command.



Next we are going to use a tool named hydra in kali linux to check this wordlist against the victim’s ssh users.

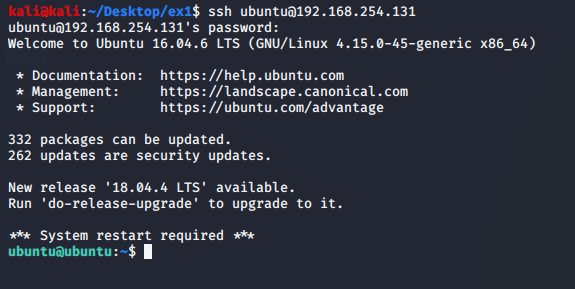
Hydra is a pre installed tool in kali linux which is used to brute force attacks and passwords in different services such as ssh,ftp, telnet and more.





Hydra tool selects the usernames and passwords which can be used to login to a system through ssh users. But as we can see all these usernames and passwords are weak encoded and easily guessable. Using these usernames and passwords we can now try to login to the Ubuntu machine.

To enter to the Ubuntu machine I am going to use the Ubuntu username and password.

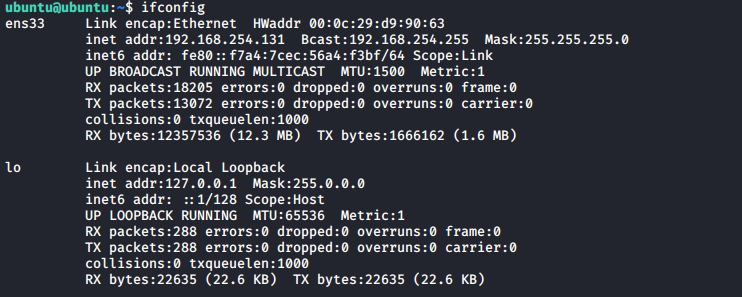


As we can see I was able to login to the Ubuntu machine using a simple weak encoded password and username such as Ubuntu. It shows that through username enumeration the attacker will be able to use their own list of usernames and try out different guessable usernames also using brute force and dictionary attacks.

When we try to run the who am I command it will display the username Ubuntu.

C:\Users\acer\Desktop\Screenshots for assignment snp\ubuntu1.PNG

Running the who am I command helps to identify the user in the Ubuntu machine. But to clearly identify that we are in the Ubuntu machine through Kali Linux is to run the ifconfig command.



From this we can clearly come to a clarification that the user is in the Ubuntu machine because the IP address is the same as the Ubuntu Machine.

Conclusion

An OPenSSH Username Enumeration does not provide a valid list of usernames but it does allow guessing of usernames. Depending on the use of OpenSSH this vulnerability can be mitigated. The vulnerable authentication mechanism can be mitigated using patching and it can be disabled once a patch is available. By disabling public key authentication the Poc script will no longer work and malformed authentication requests would be rejected. Checking logins for signs of exploitation in this vulnerability will differ according to different versions of Openssh but there would be plenty of ways a malformed message could be generated for even fatal outcomes. Since this is not a remote code vulnerability but an information vulnerability it is best to disable public key authentication.

**References**

<https://www.tecmint.com/install-openssh-server-in-linux/>

<https://www.exploit-db.com/exploits/45233>

<https://en.wikipedia.org/wiki/OpenSSH>

<https://guides.codepath.com/websecurity/Username-Enumeration>

<https://www.shellvoide.com/hacks/enumerate-usernames-ssh-servers-77-cve-2018-15473-vulnerability/>

<https://linuxconfig.org/introduction-to-nmap-on-kali-linux>

<https://geek-university.com/nmap/install-nmap-on-linux/>

<https://github.com/paramiko/paramiko/issues/1314>

<https://blog.nviso.eu/2018/08/21/openssh-user-enumeration-vulnerability-a-close-look/>