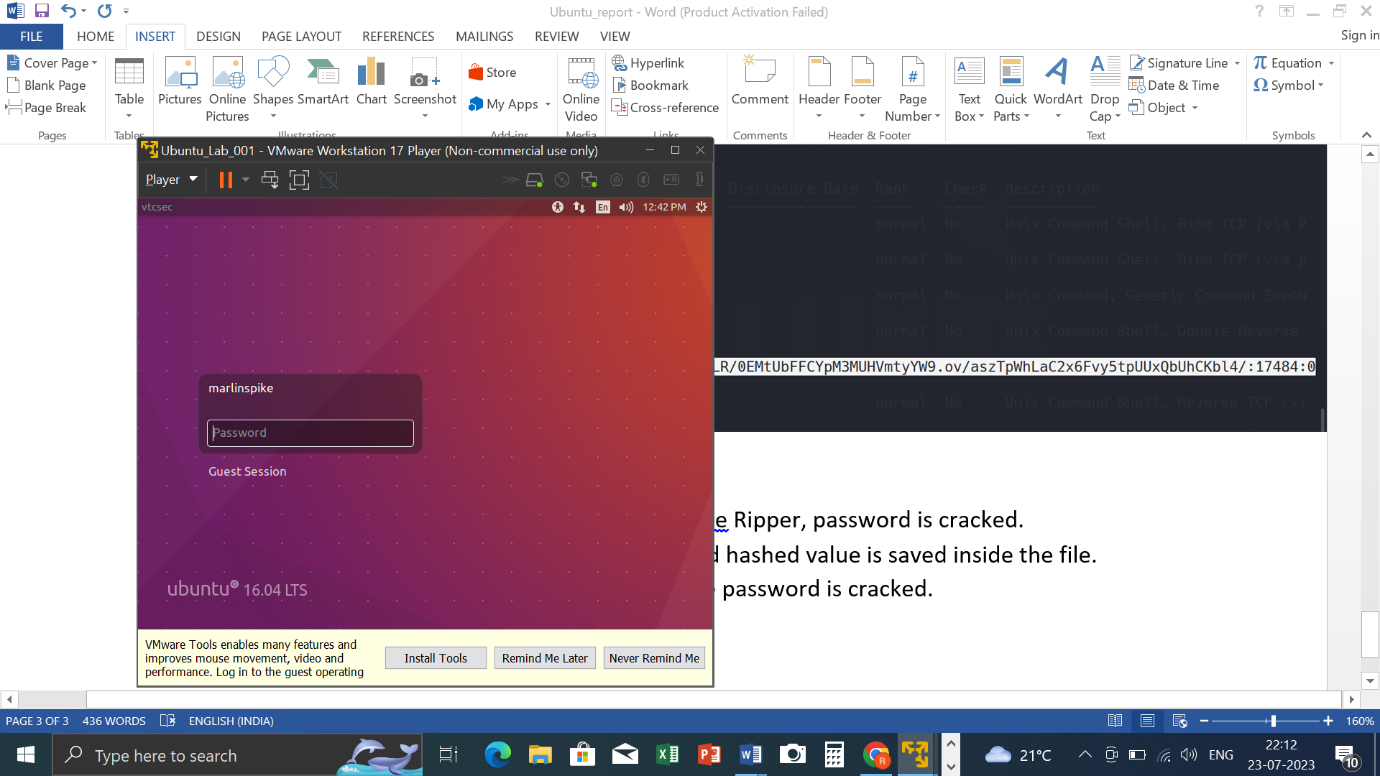
******

**VAPT REPORT ON UBUNTU**

**Varun Hegde | Cybersecurity -June 23 | 24/07/2023**

## VULNERABILITY ASSESSMENT REPORT (Linux)

* Executive Summary:

The purpose of this report to give an overview of the penetration testing conducted on Ubuntu machine. The penetration testing was performed with intention of identifying the vulnerabilities and weakness within Linux based Operating System (Ubuntu), assessing the potential impact of these vulnerabilities, and providing recommendations for remediation.

* Introduction:

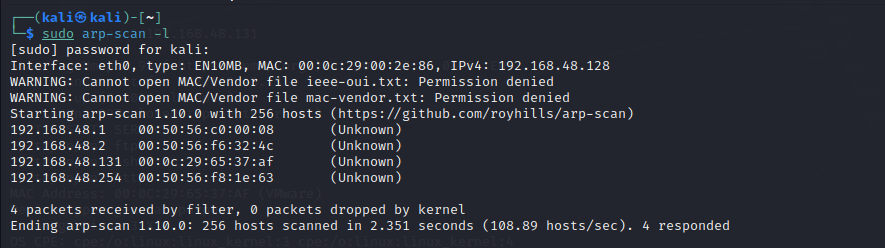
The penetration testing followed a systematic and controlled approach of industry best practices and ethical guidelines. The primary objective was to stimulate real-world attack and replicating the techniques and methodologies to find the vulnerabilities that could be exploited by us. By conducting the penetration test, we aimed to identify the weakness in Linux based Operating System (Ubuntu), vulnerabilities and potential avenues for unauthorized access. This report will provide detailed information on the methodologies; tools and techniques are used during the testing process

* Tool Used:
  + Arp-Scan: The command is used to perform an ARP (Address Resolution Protocol) scan on local network. It allows you to scan to discover the and display all the IP addresses and corresponding MAC (Media Access control) Addresses of connected to the same network. The ARP protocol is used to map IP Addresses to MAC Addresses, which is crucial for data transmission within a local network
  + Nmap: Nmap (Network mapper) is a powerful and widely used network scanning tool that has legitimate and ethical applications in network security, system administration and penetration testing. It design to discover hosts on a network, perform service and version detection and provide the valuable information about the devices and version detection, and provide valuable information about the devices and services and services running on those hosts.
  + Metasploit: Metasploit is widely-used penetration testing and exploitation framework that provides a collection of tools and resources for identify, validate and exploit vulnerabilities in various system and applications including Ubuntu.

**PENTESTING:**

1. ***Information Gathering:***

* Initially **arp-scan** was performed to send arp request in order to map IP address and MAC ID in the network.



* Now, nmap scanning is been done. Nmap (Network Mapper) is a powerful and popular open-source network scanning tool used for network exploration and security auditing. It is designed to discover hosts and services on a computer network, thus creating a map of the network's structure. Nmap uses various scanning techniques to gather information about open ports, operating systems, and other valuable details that help administrators and security professionals assess the security posture of their networks. It is widely used for network inventory, vulnerability assessment, and penetration testing purposes.

Nmap scanning is been done using the option –O(OS detection) in order to find which IP address discovered in arp-scan belongs to Ubuntu lab.



This shows that the IP address 192.168.48.131 belong to Ubuntu Linux.

1. ***Enumeration:***

* ***nmap -sV 192.168.48.131 -oN ubuntu.txt:***

The above nmap scan is been done and the options/ parameters used are:

-sV: Probe open ports to determine service/version info

-oN:this option specifies the output format and filename for the scan result.

OUTPUT:



* + - after the nmap scan we found that there are some open port on which we can find the vulnerability:

OPEN PORTS:

21/tcp open ftp

22/tcp open ssh

OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

80/tcp open http

Apache httpd 2.4.18 ( (Ubuntu))

Http-server-header: Apache/2.4.18 (Ubuntu)

OS details: Linux 3.2 - 4.9

proFTPD 1.3.3c

ProFTPD 1.3.3c is vulnerable to a backdoor that was added to the ProFTPD download archive. This backdoor was present in the proftpd-1.3.3c.tar.[bz2|gz] archive between November 28th 2010 and 2nd December 2010.

The backdoor allows an attacker to execute arbitrary commands on the vulnerable system by sending a specially crafted FTP command. The backdoor is triggered by the "SITE CPFR" command, which is used to copy files from the server to the client.

The backdoor was discovered by security researcher Tavis Ormandy and was patched in ProFTPD version 1.3.3d.

To fix the vulnerability, you need to upgrade your ProFTPD installation to version 1.3.3d or later.

Here are the steps on how to upgrade ProFTPD:

Download the latest version of ProFTPD from the official website.

Unpack the downloaded archive.

Rename the old ProFTPD directory to something else, such as "proftpd.old".

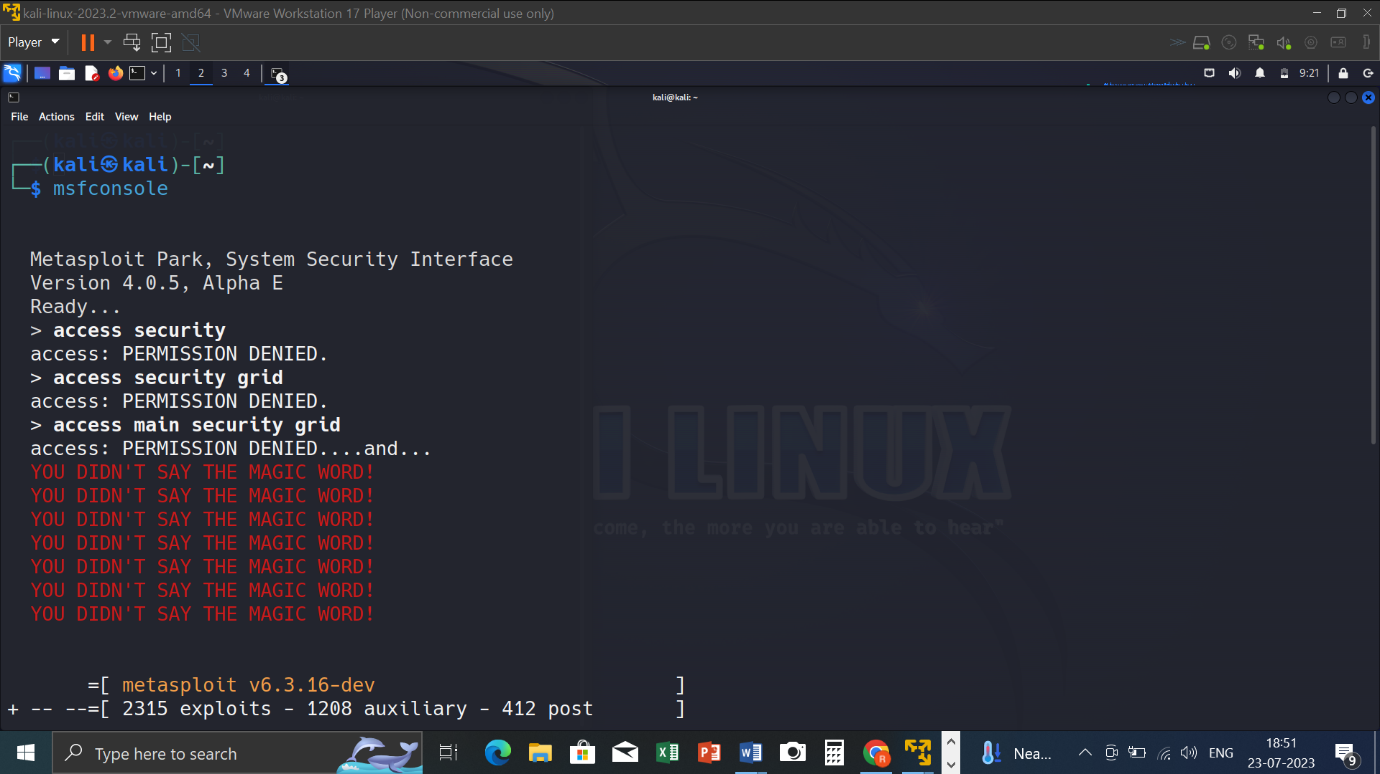
Rename the new ProFTPD directory to "proftpd".

Restart the ProFTPD service.

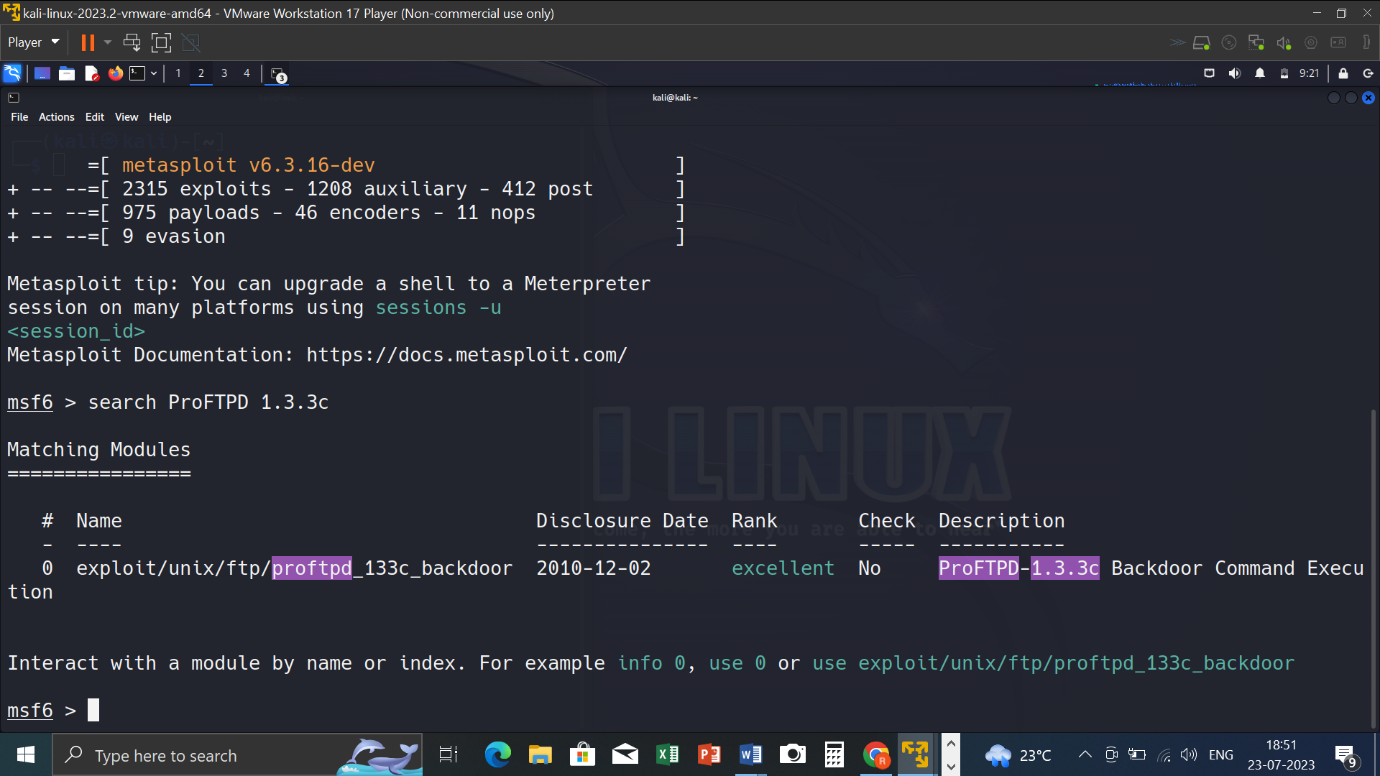
Once you have upgraded ProFTPD, your system will no longer be vulnerable to the backdoor

1. ***Metasploit:***

* To start metasploit use the command “msfconsole”.

******

* Since the 21/tcp port was backdoored, scanning using the command “search ProFTPD 1.3.3c” ( ProFTPD 1.3.3c is the version of 21 port)

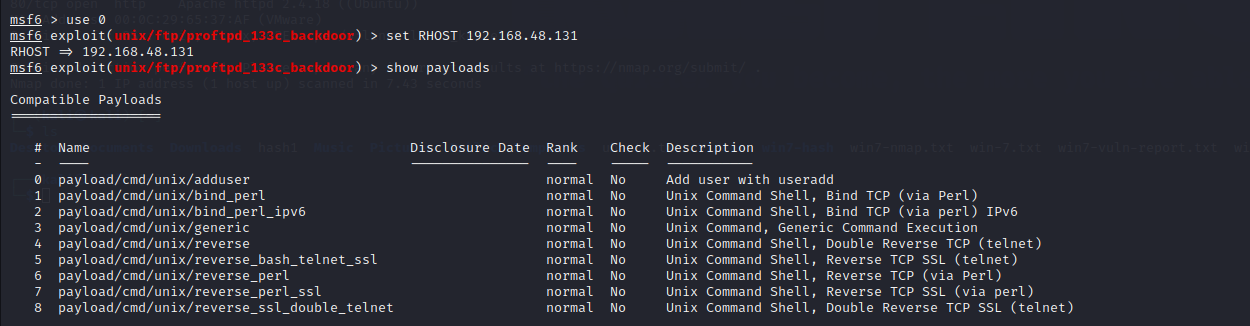
******

* “use 0 “ command in order to enter into unix/ftp/proftpd\_133c\_backdoor.
* Set the RHOST and PAYLOAD

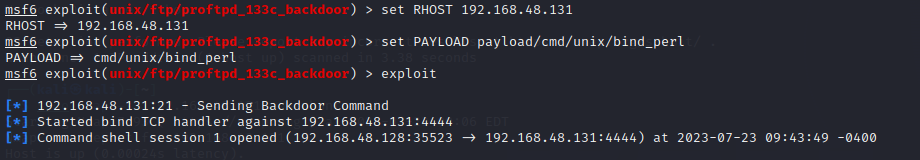
RHOST is set as the victim IP address.

PAYLOAD is set by using the command “show payloads” in order to view the compatible payloads.

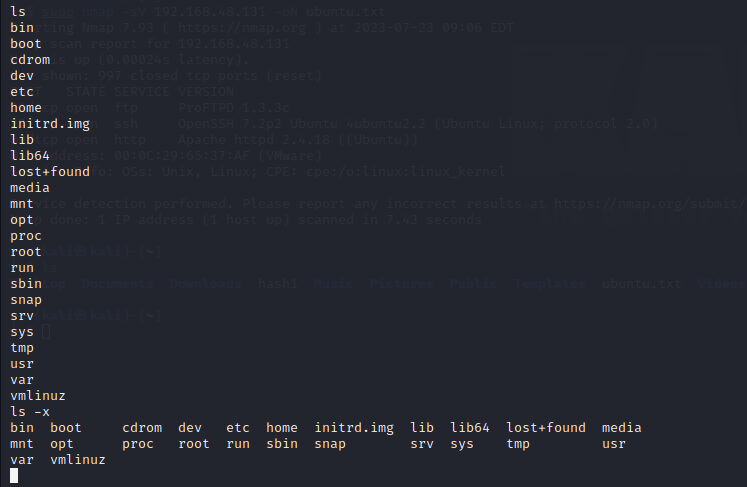
Here, payload with index 0 is been set.



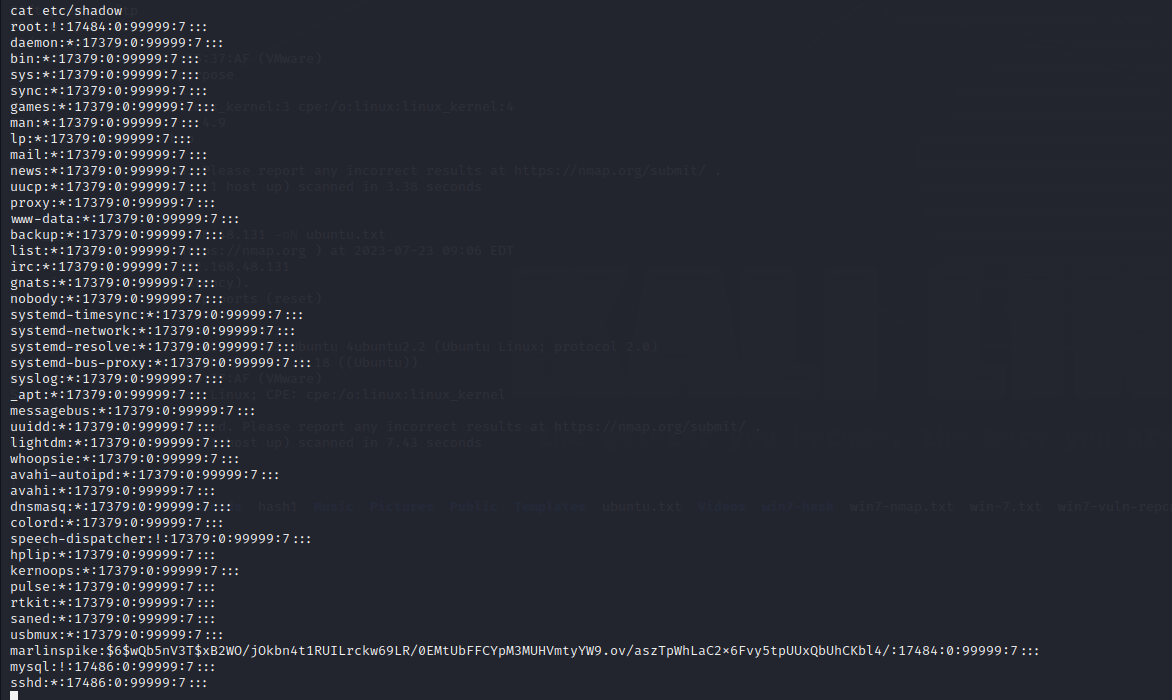
* Exploit.

******

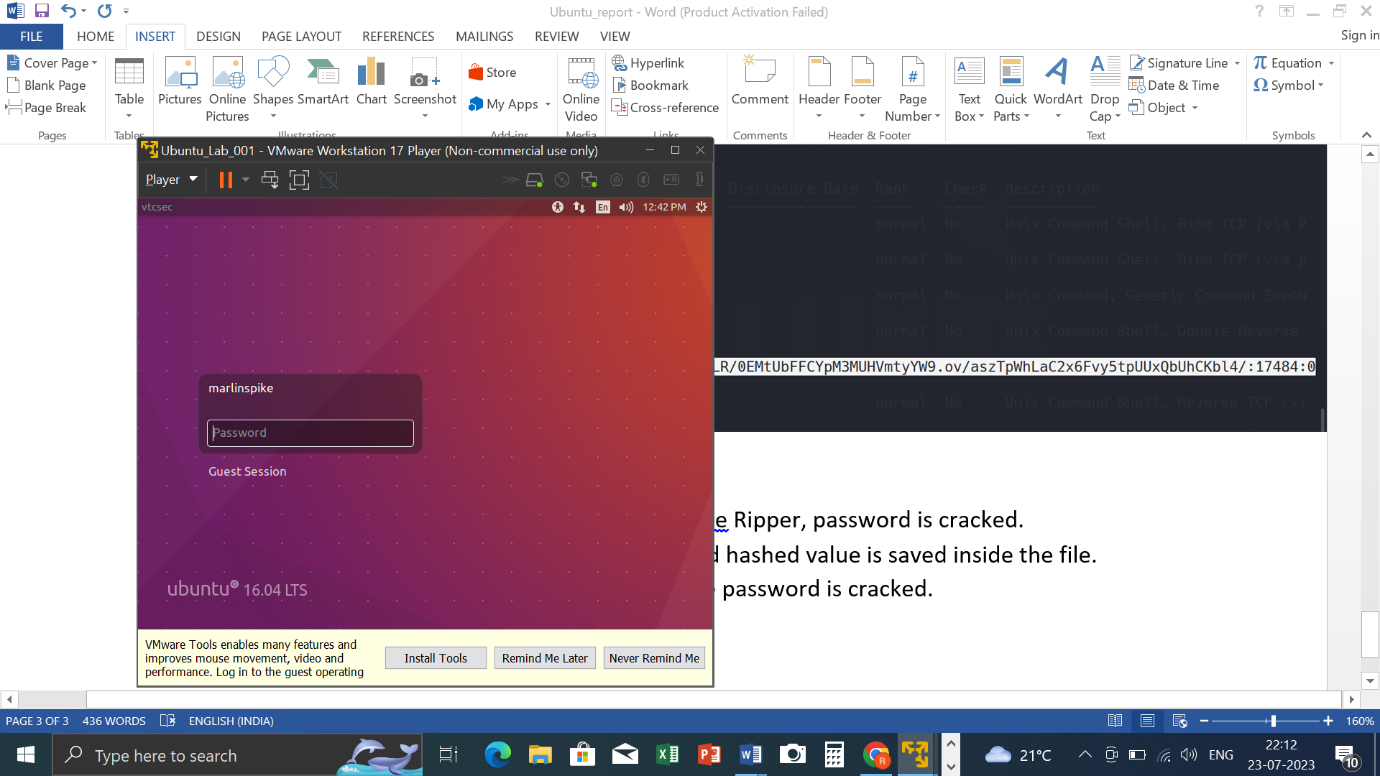
* We know that in ubuntu passwords are stored in etc/shawdow.Use the command “ls” to list out the directory/files.

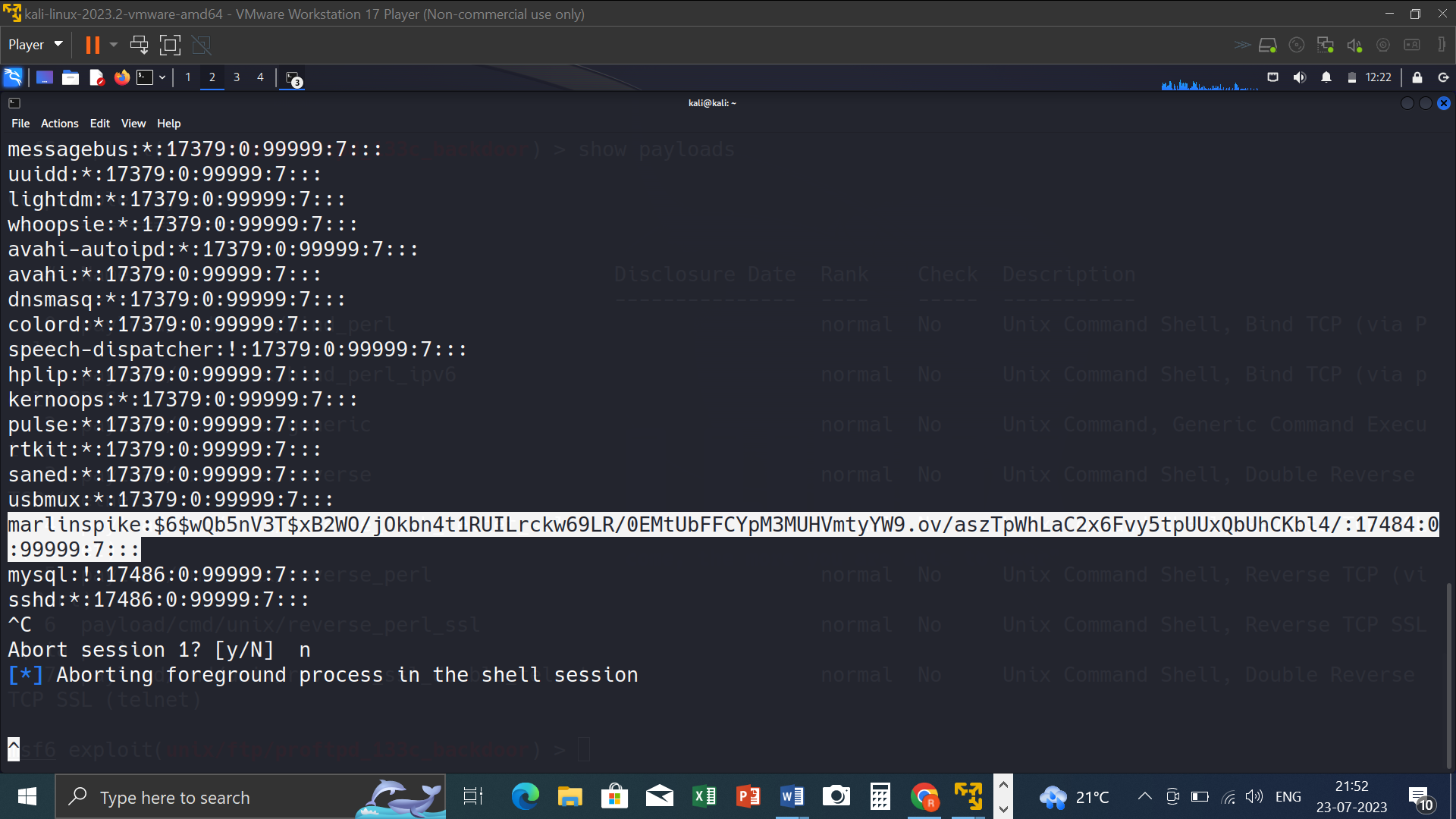
******

* We use cat etc/shadow to see the password hashes.

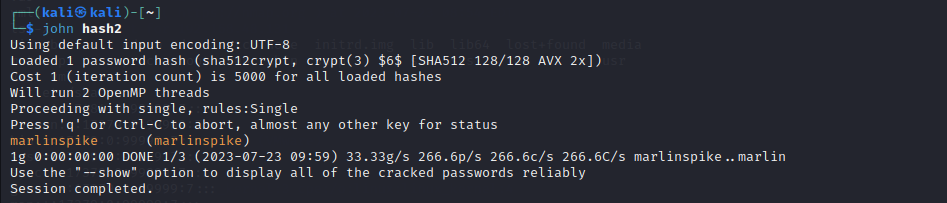
******

* Since the username of target is marlinspike, copy the cracked hashed password.

******



* Using the password cracking tool John The Ripper, password is cracked.
* A file is created using nano command and hashed value is saved inside the file.
* Using the command john <filename>, the password is cracked.



**THE CRACKED PASSWORD OF UBUNTU LAB IS : marlinspike**



**Conclusion:**

**Apply the latest security patches: The vulnerabilities have all been patched by Ubuntu. Users should apply the latest security patches to their systems to mitigate the risk of exploitation.**

**Use a firewall: A firewall can help to block unauthorized access to the system.**

**Use strong passwords: Users should use strong passwords to protect their accounts.**

**Be aware of phishing attacks: Phishing attacks are a common way to exploit vulnerabilities. Users should be aware of phishing attacks and be careful about clicking on links or opening attachments from unknown senders.**

**Conclusion**

**The vulnerabilities found in Ubuntu 16.04 LTS are serious and could be exploited by attackers. Users should apply the latest security patches to their systems to mitigate the risk of exploitation**

**THANK YOU**