Assignment 3

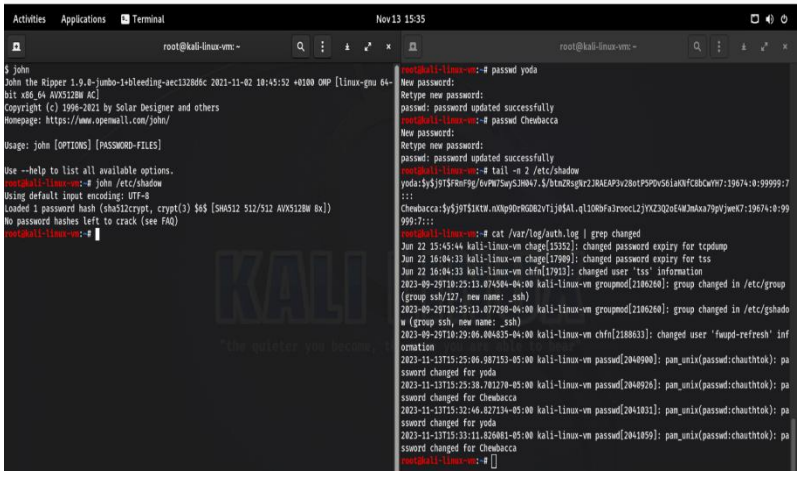
1. **a. Describe at least 2 tools related to System Hacking (Chapter 7) with relevant screenshots, that demonstrates its working.**

Ans: Burp suite: Burp Suite is a potent cybersecurity tool used for investigation and testing of online application security. Finding and taking advantage of vulnerabilities in online applications is the main function of this tool. Users can intercept, examine, and change HTTP and HTTPS communication between their browser and the intended web application by using Burp Suite, which functions as a proxy server. Security experts may examine the security posture of web applications thanks to the proxy feature, which is essential for modifying requests and answers.

Several modules, such as the Proxy, Scanner, Spider, Repeater, Intruder, and more, are available on the tool's user-friendly interface. The essential element that makes it easier to intercept web traffic is the proxy module. To find security vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and other issues, security analysts utilize the Proxy to examine and alter requests and answers.

The process of finding and taking advantage of security flaws is automated by the Scanner module. By examining online applications for common vulnerabilities, it does dynamic application security testing, or DAST. The Spider module automatically finds and navigates across connections to assist in mapping the structure of web applications.

John the Ripper: John the Ripper is a popular open-source password cracking application that uses a variety of attack techniques to find weak passwords. Originally created for Unix-based systems, it now supports a variety of platforms. John the Ripper is a flexible tool for cracking password hashes collected from a variety of sources since it uses tactics including dictionary assaults, brute-force attacks, and hybrid attacks. It can effectively handle password files from many operating systems and supports a variety of cryptographic hash techniques. Because of John the Ripper's speed and versatility as a command-line tool, security experts and penetration testers frequently use it to evaluate the security of passwords in a variety of settings. Its architecture is expandable and modular, and the community continues to maintain it, which adds to its efficacy in cases including penetration testing and password auditing.



b. Describe at least 2 tools related to Malware (Chapter 8) with relevant screenshots, that demonstrates its working.

Ans:

Malwarebytes Anti-malware:

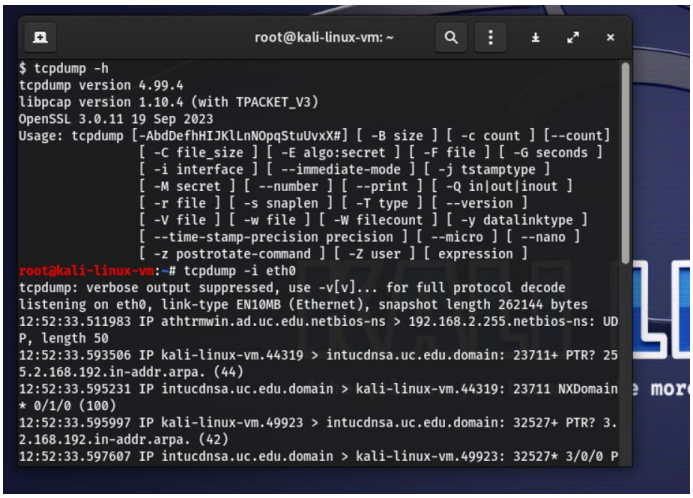
A trustworthy cybersecurity tool called Malwarebytes Anti-Malware is made to identify and get rid of different kinds of malware, such as viruses, spyware, adware, and other harmful programs. Prominent for its intuitive interface and potent scanning skills, Malwarebytes use sophisticated heuristic analysis and behavior-based detection to promptly discover and eliminate any threats. Comprehensive security is offered across many devices with the program, which is compatible with Windows, macOS, and Android. Additionally, Malwarebytes Anti-Malware has a proactive prevention engine designed to thwart malware infestations before they start. Software effectiveness against developing cyber threats is ensured by regular upgrades. Known for its dependability and effectiveness, Malwarebytes Anti-Malware is a useful tool for people and businesses looking for strong defense against malware threats.

Cuckoo sandbox:

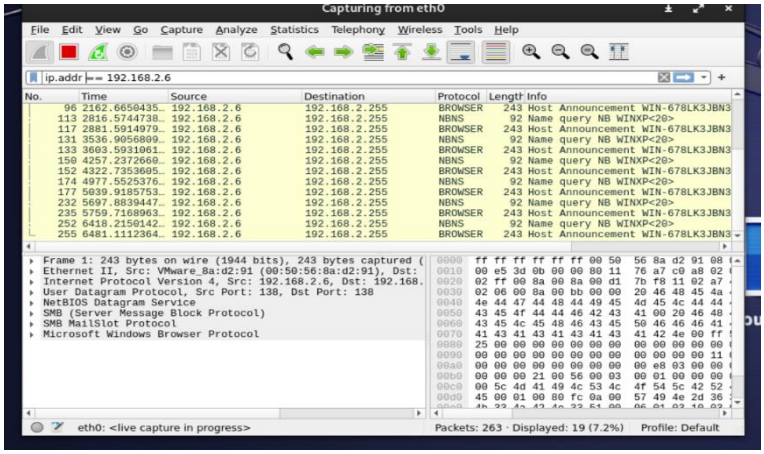
An automated and dynamic environment for examining and comprehending the behavior of dangerous software is what Cuckoo Sandbox, an open-source malware analysis tool, is meant to offer. Cuckoo serves as a sandboxing solution that enables researchers and security experts to run questionable files in a safe setting and watch how they interact and behave. It makes use of a variety of analysis methods, such as system calls, network traffic analysis, and API call monitoring, to produce comprehensive reports on the malware's operations. Cuckoo Sandbox is a flexible tool for dynamic malware analysis because of its extensible and modular design, which supports a range of virtualization systems and analysis engines. By analyzing and comprehending the strategies, methods, and procedures used by cybercriminals, security experts utilize Cuckoo Sandbox to improve incident response, boost threat intelligence, and keep updated about new cyberthreats.

c. Describe at least 2 tools related to Sniffing (Chapter 9) with relevant screenshots, that demonstrates its working.

Ans: Tcpdump: Network packets can be captured, shown, and analyzed using the command-line packet analyzer tcpdump, which is popular in Unix-like operating systems. The features of tcpdump make it an effective tool for monitoring and debugging networks. It allows for the real-time collection of packets from either a subset of the available interfaces or all of them, and it displays the detailed information in a legible style regarding protocols, flags, source and destination addresses, port numbers, and payload data. Filtering collected packets according to several parameters, including IP addresses or protocol kinds, is one of its noteworthy features that makes targeted analysis easier. For thorough network analysis, the tool's promiscuous mode of operation, which enables the collection of every network packet, makes it useful. It is also possible to examine network traffic offline using tcpdump by reading packets from files that have already been collected. Captured packets can be saved in common formats like pcap for further analysis as part of its flexible output. For network managers, security experts, and anybody else interested in learning more about network traffic and seeing possible problems, tcpdump is still a vital tool despite the fact that its command-line interface can be intimidating to certain users.



Command : tcpdump –i eth0



Wireshark:

Data packets moving via a network may be captured, examined, and analyzed with the help of Wireshark, a popular and multifunctional network protocol analyzer that is essential to network sniffing. A full picture of network traffic may be obtained from pre-captured files or in real time using Wireshark's robust command-line features and user-friendly graphical interface. Utilizing Wireshark to diagnose network problems, find security flaws, and comprehend network communication patterns is common practice for network administrators, security experts, and developers. Selection of certain traffic kinds, including packets linked to certain IP addresses, protocols, or application-layer data, may be viewed thanks to its display filters. For troubleshooting, network activity monitoring, and, in the context of ethical hacking, networked system security assessment, Wireshark's capacity to

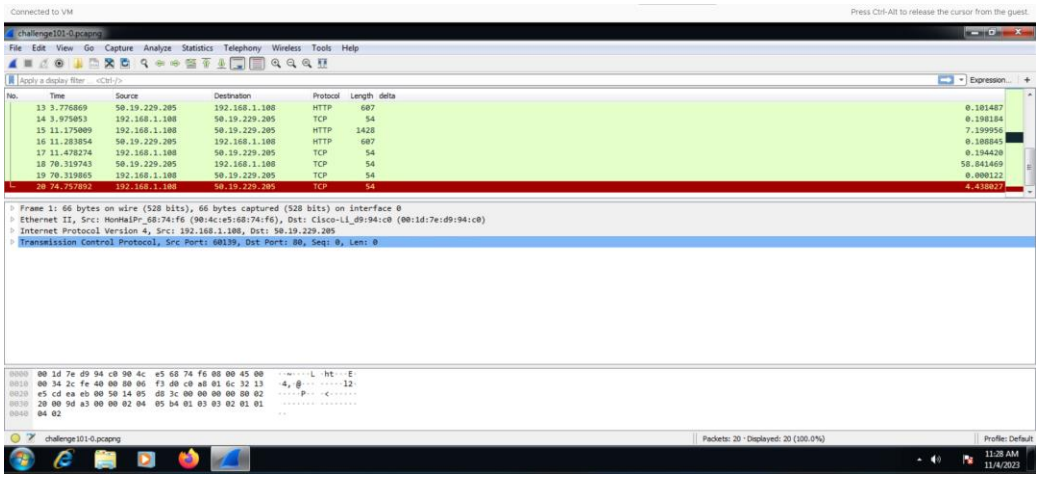
record unencrypted data—including HTTP requests and responses—makes it an invaluable instrument. It is essential to stress, nonetheless, that Wireshark should be used responsibly, that network sniffing operations adhere to moral and legal obligations, and that getting the necessary permissions is a must before recording or deciphering network signals.

Part one: Pack Analysis

File: Challenge 101-0.pcapng

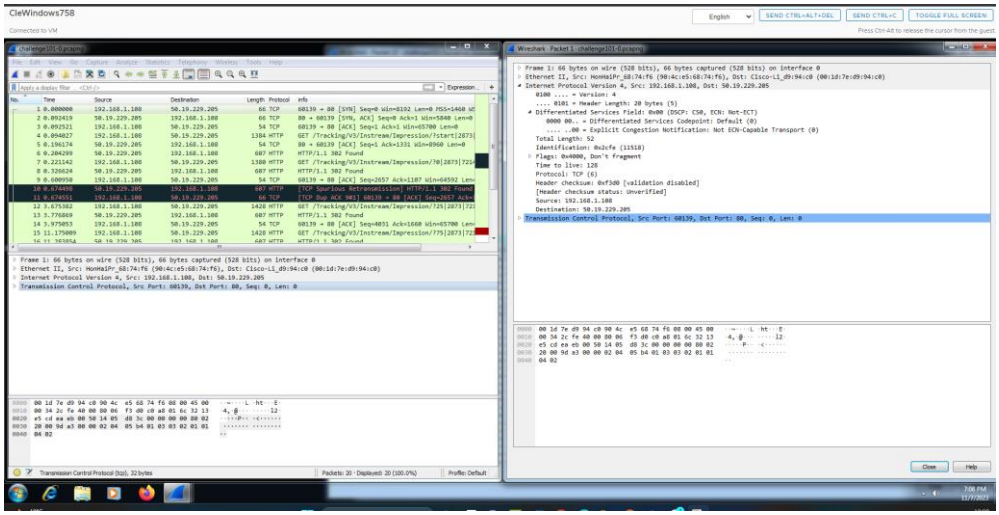
1. **How many packets are in this trace file?**

Ans: There are 20 packets in the trace file.

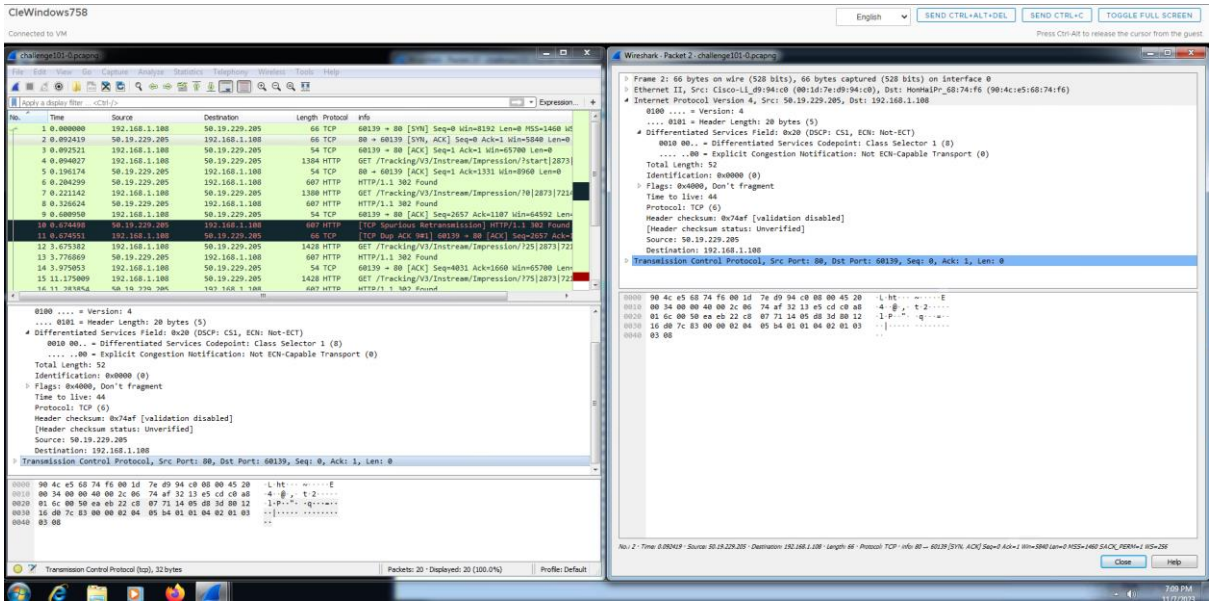


2. **What IP hosts are making a TCP connection in frames 1,2 and 3?**

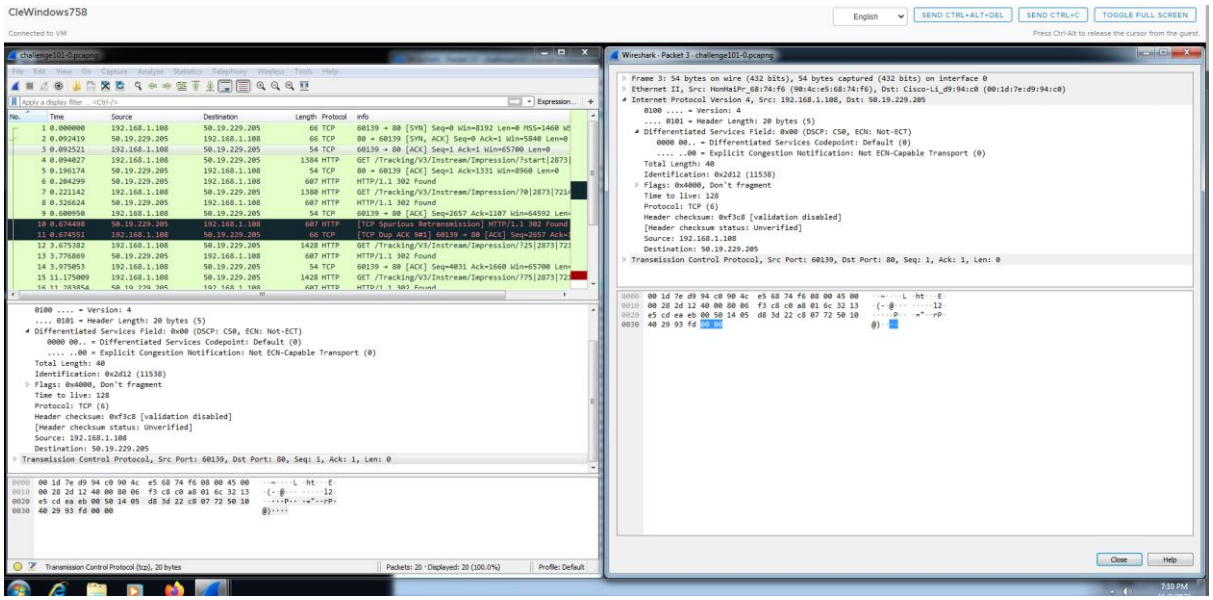
Ans: IP host for TCP connection in frame 1 is:



IP host for TCP connection in frame 2 is:

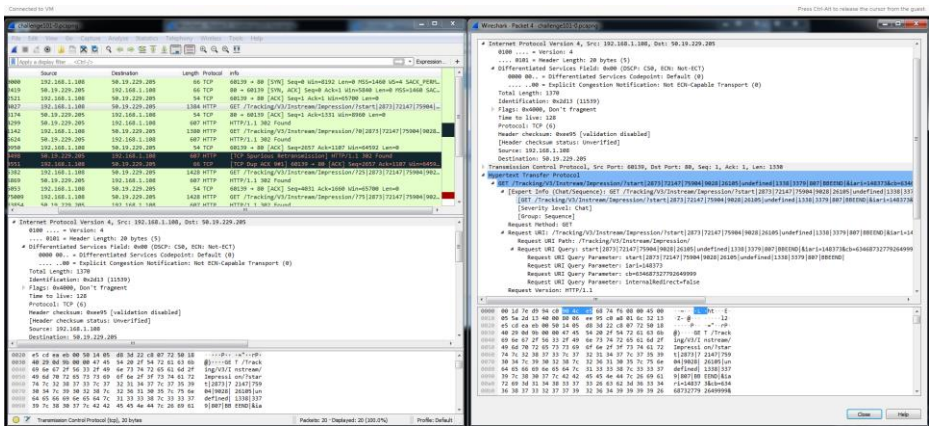


IP host for TCP connection in frame 3 is:



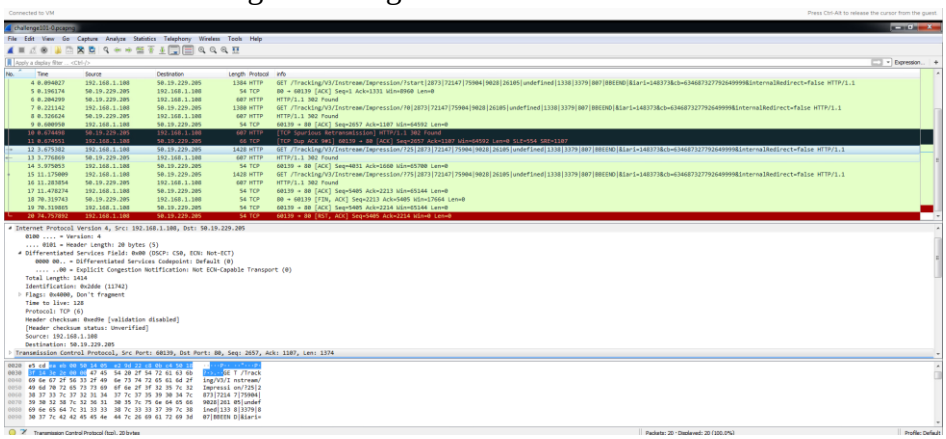
3. **What HTTP command is sent in frame 4?**

Ans: GET command



4. **What is the length of the largest frame in this trace file?**

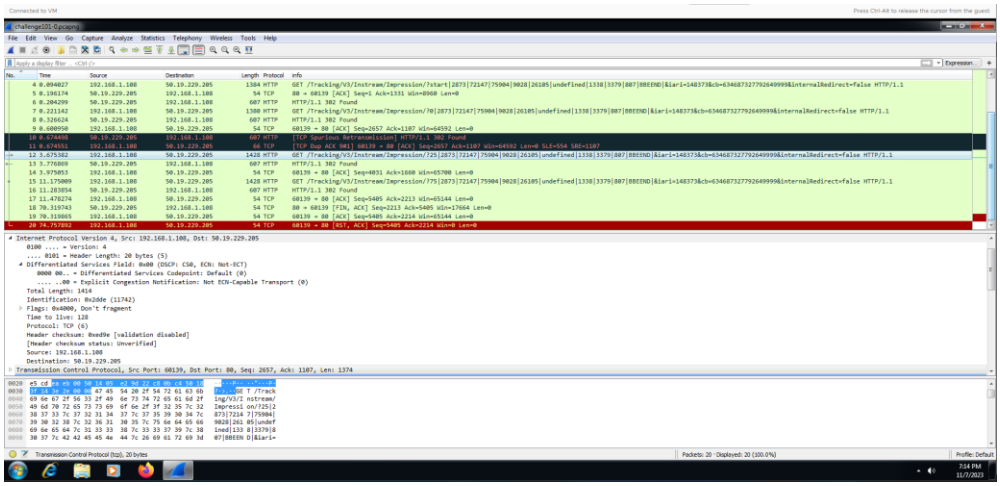
Ans: The largest length is 1428 and the frame number is 15



5. **What protocols are seen in protocol column?**

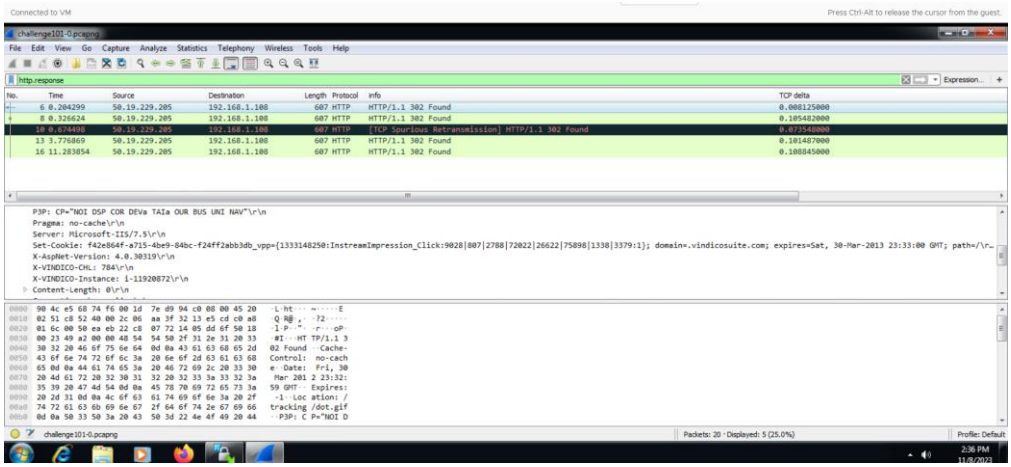
Ans: There are two protocols in this trace file

TCP and HTTP protocol



6. **What responses are sent by the HTTP server?**

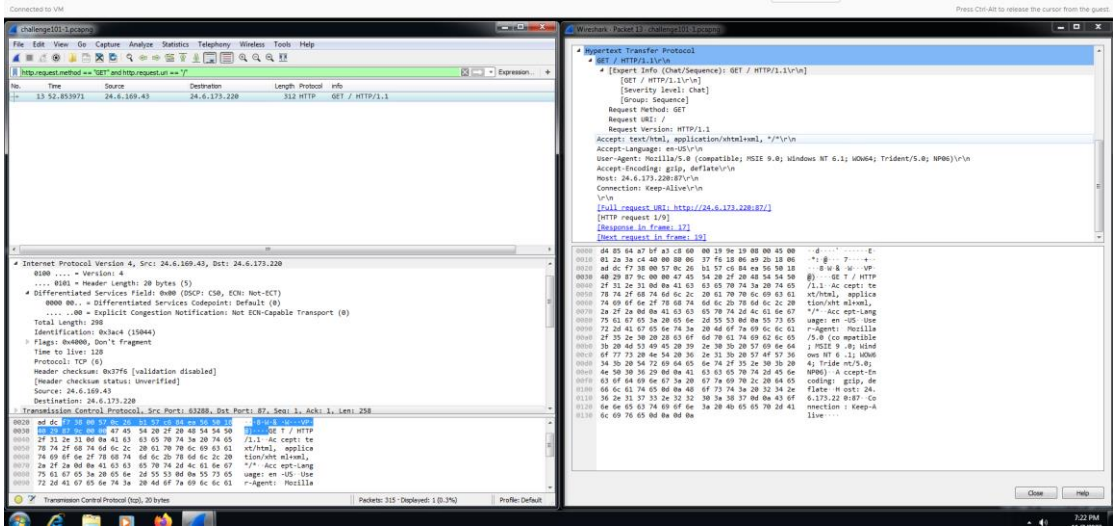
Ans:



File: Challenge 101-1.pcapng

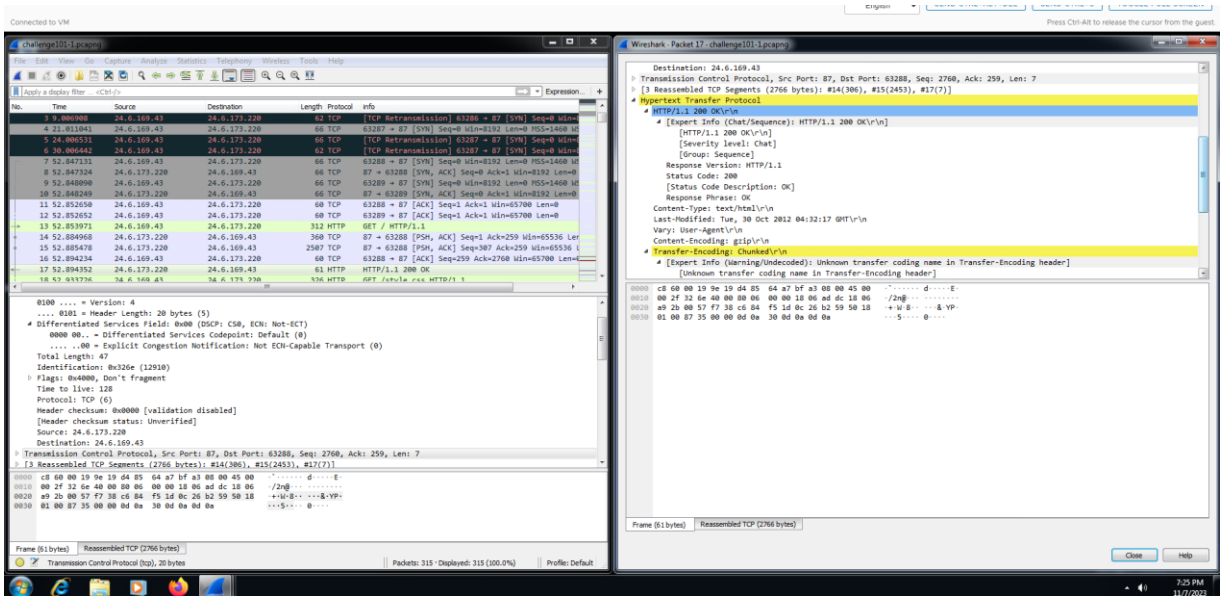
7. **What frame number does the client request the default root web page (“/”)?**

Ans: Frame number 13 does the client request the default root web page(“/”)



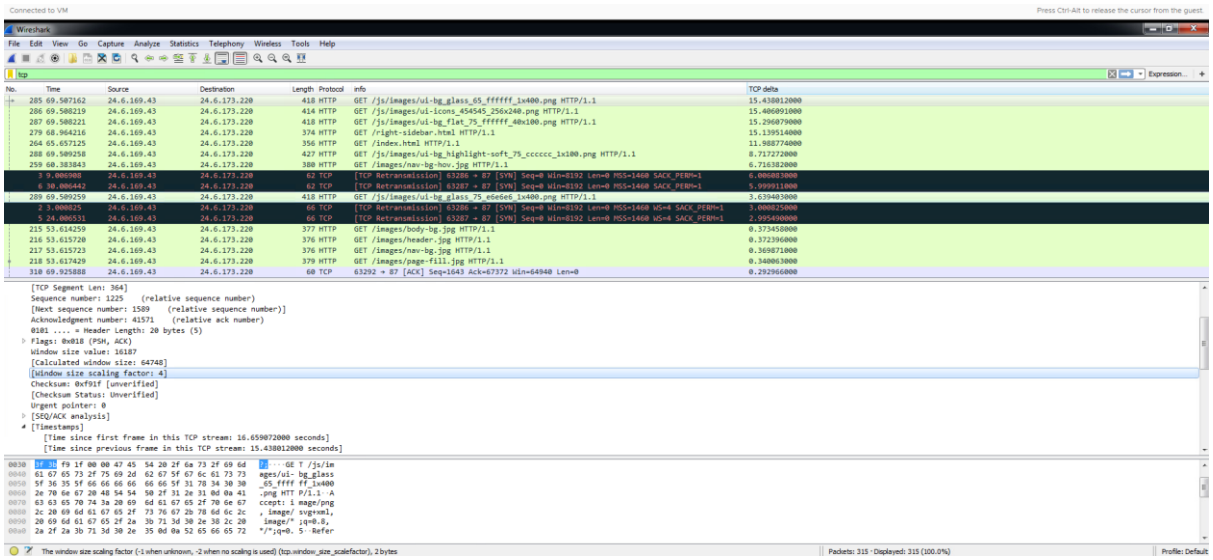
8. **What response does the server send in frame 17?**

Ans:



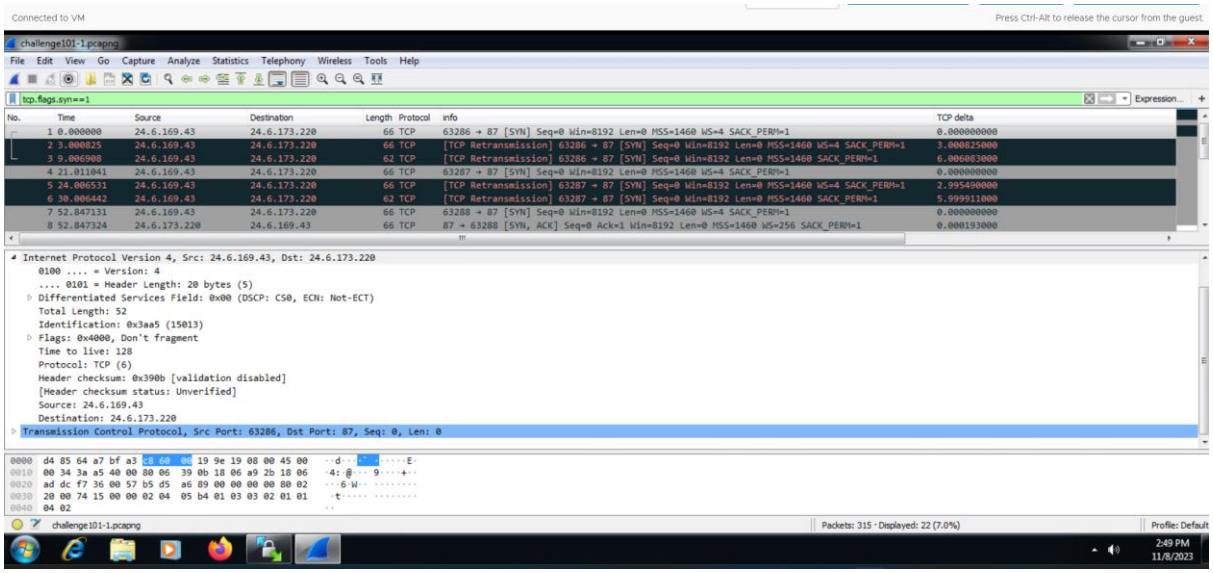
9. **What is the largest TCP delta (delay) value seen in this trace file?**

Ans:



10. How many SYN packets arrived after at least 1 second delay?

Ans:

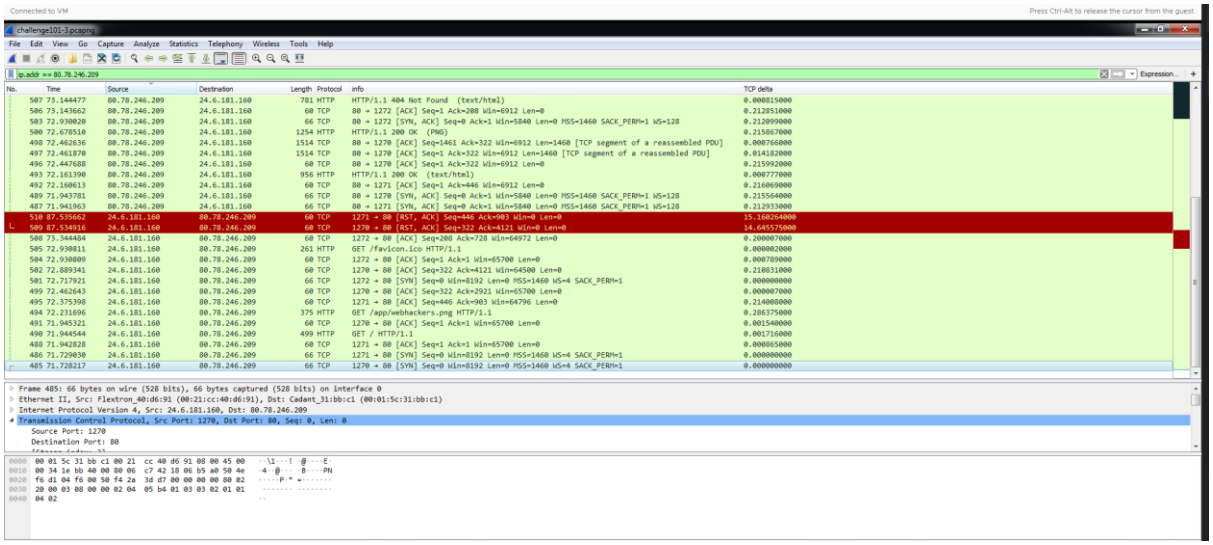


Again apply frame.time_delta>=1

File: challenge 101-3.pcapng

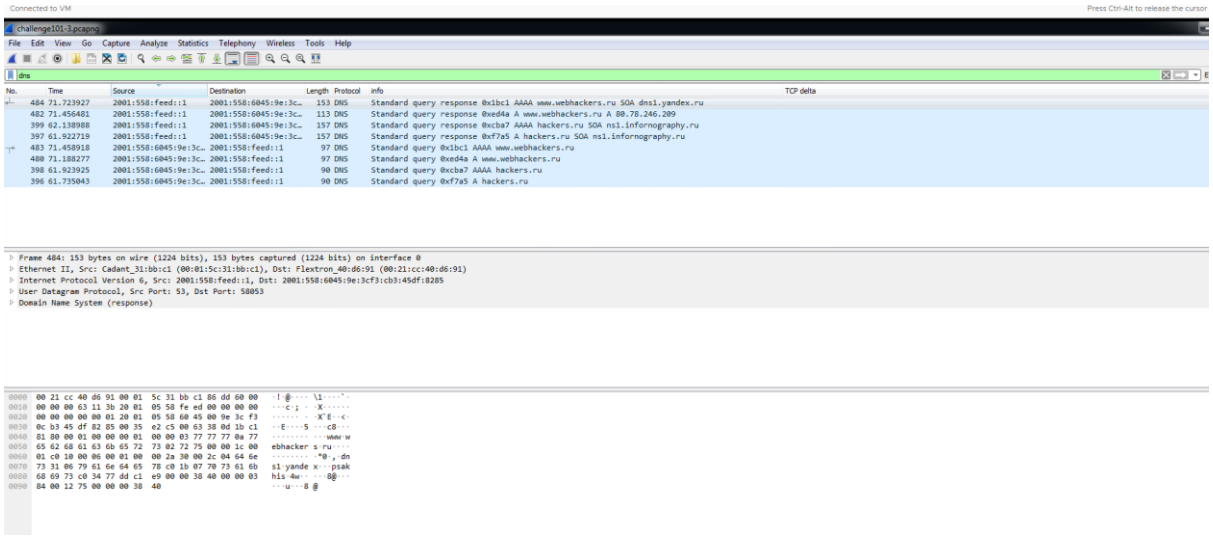
11. How many frames travel to or from 80.78.246.209?

Ans:



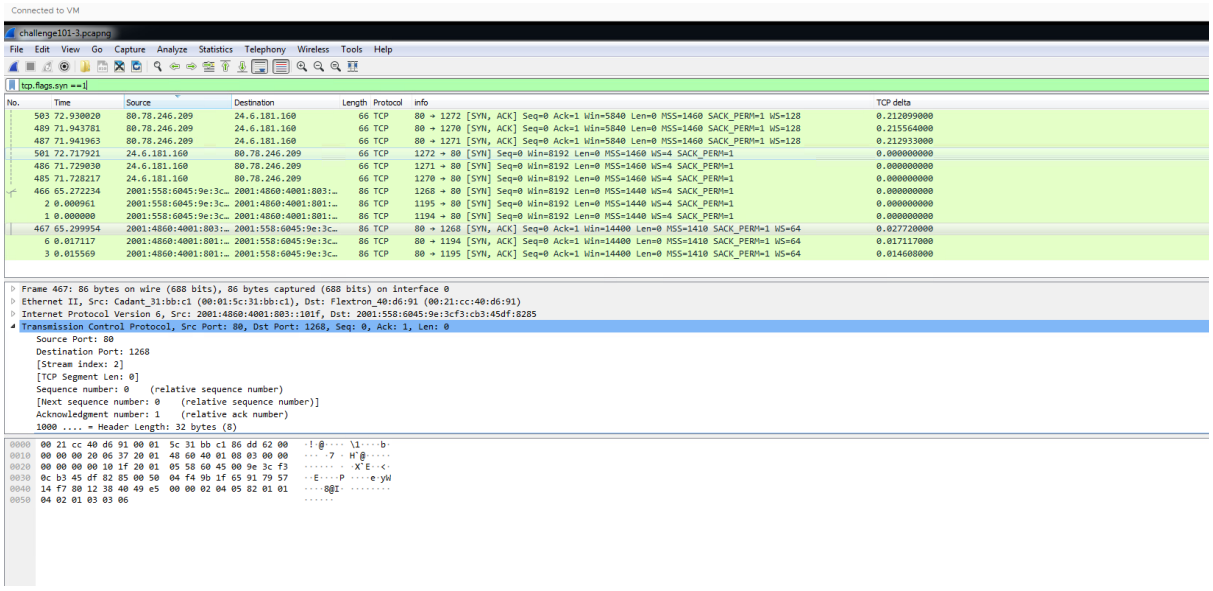
12. How many DNS packets are in the trace file?

Ans:



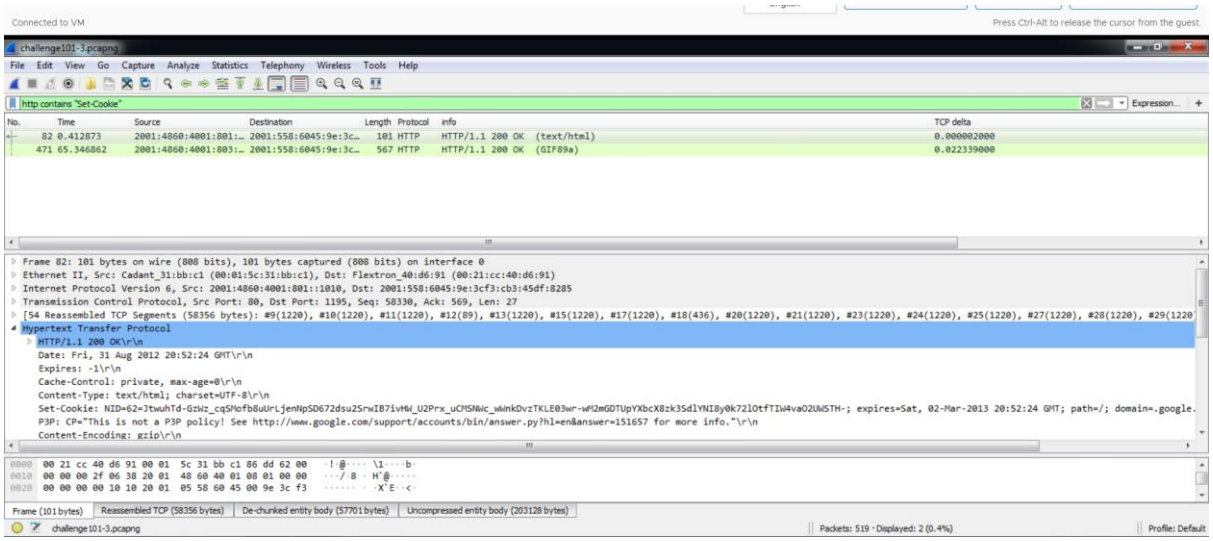
13. How many frames have the TCP SYN bit set to 1?

Ans:



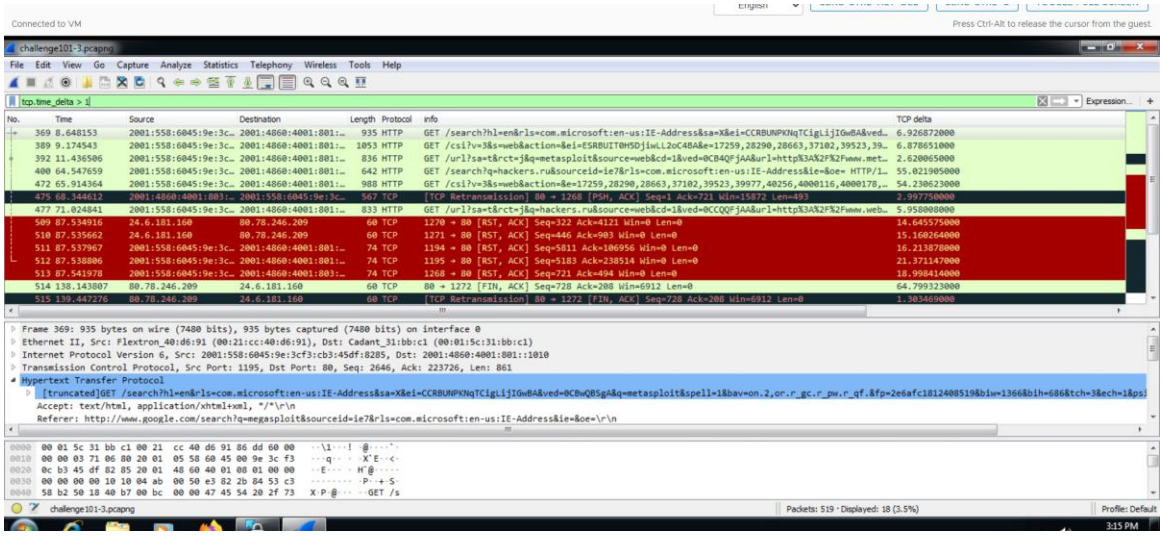
14. How many frames contain the string “set-cookie” in upper case or lower case?

Ans: In search filter enter http contains “Set-Cookie”, then it will show the number of frames which contains Cookies.



15. How many frames contain a TCP delta time greater than 1 second?

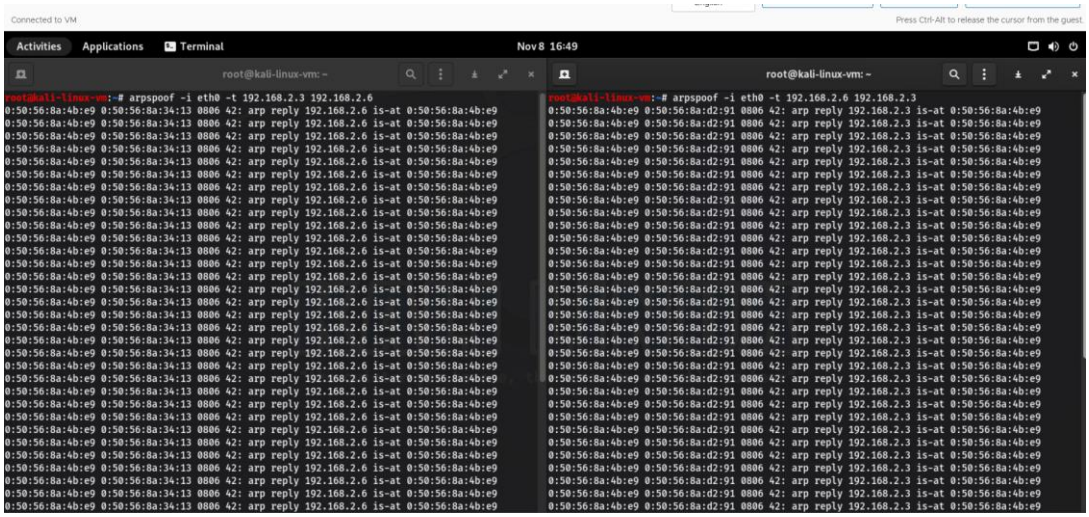
Ans:



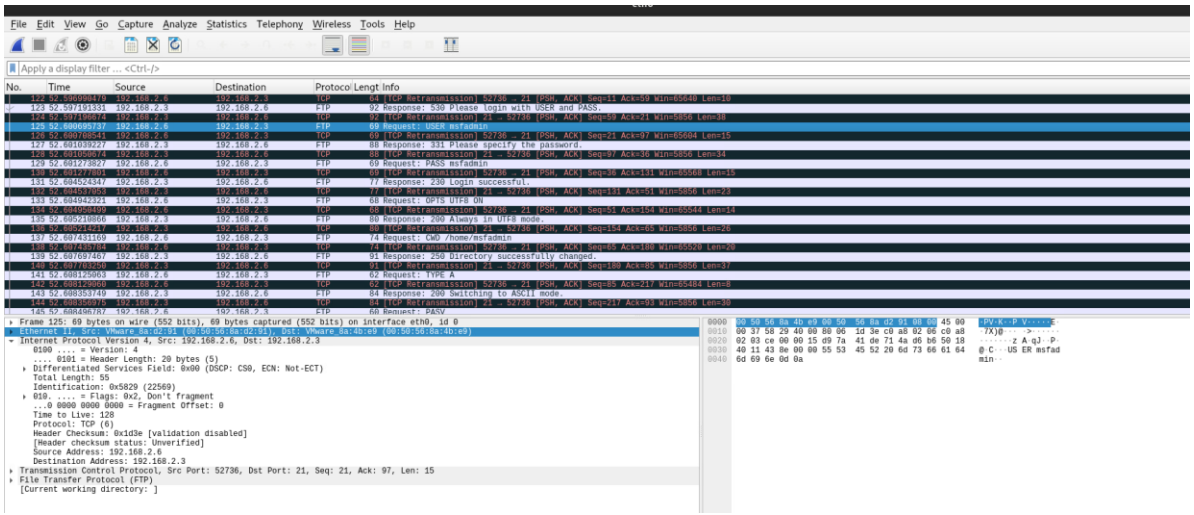
Module Activity Description:

Part two: Capturing packets using ARP poisoning

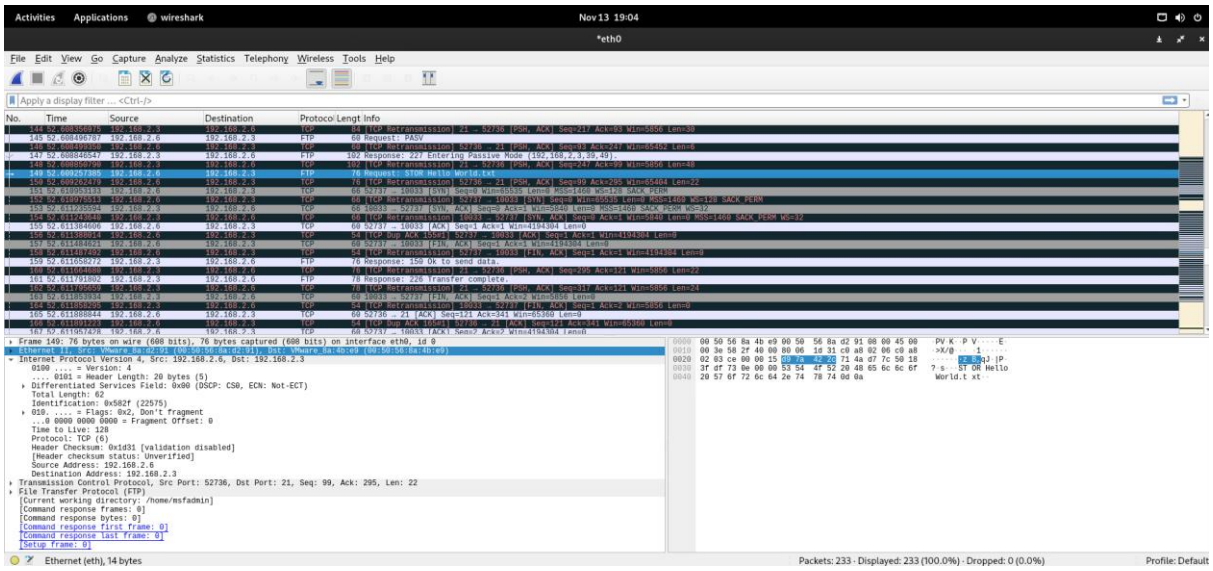
- On your Windows 7 system, install WinSCP, Filezilla, or your favorite FTP client.
- On you Kali Linux system, start a packet capture with Wireshark on the eth0 interface
- Turn on packet forwarding with the following command:
  echo 1 > /proc/sys/net/ipv4/ip_forward
- Start ARP poisoning your Windows 7 and metaploitable2 systems:
  arpspoof –i eth0 –t <IP of windows7><IP of metasploitable2>
- In a new terminal run the same command, but rearrange the IP addresses so you are capturing both sides of the conversation
- On you Windows 7 system, connect to FTP on your metaploitable2 system using port 21.
- Login with user: msfadmin password: msfadmin
- Create a text file on your Windows 7 system with the words “Hello World” in the text
- Transfer this file to the metasploitable2 system using ftp
- Stop the packet capture and hit ctrl-c in both terminal windows to stop the ARP poisoning.
- Analyze the packet capture and answer the following questions/paste screen shots.
- Find the packets that contain the username and password for the ftp server



16. Paste a screen shot showing each of these packets.

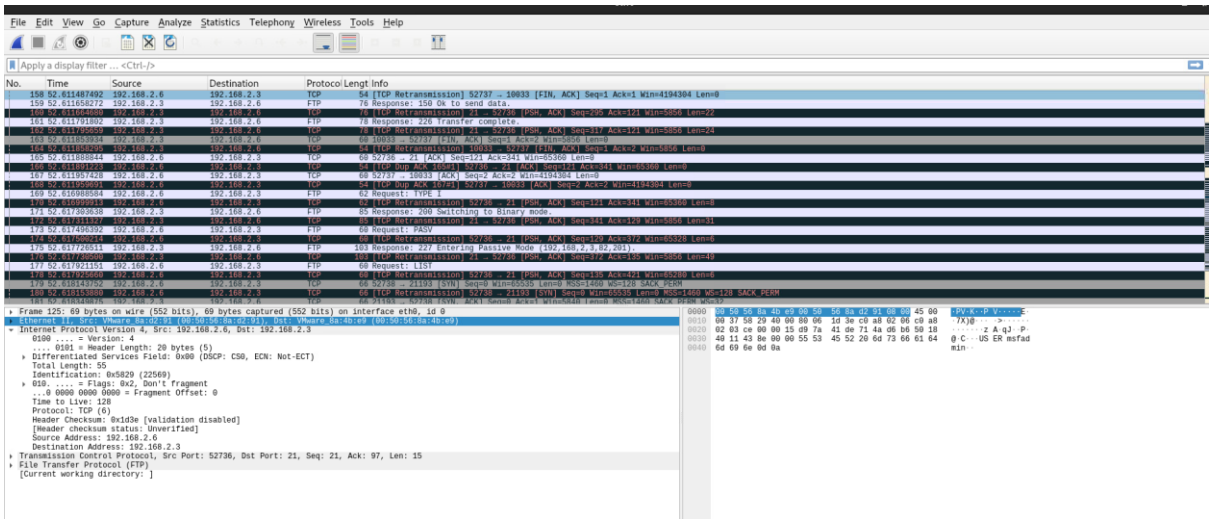


Find the packet that contains the text file you transferred.



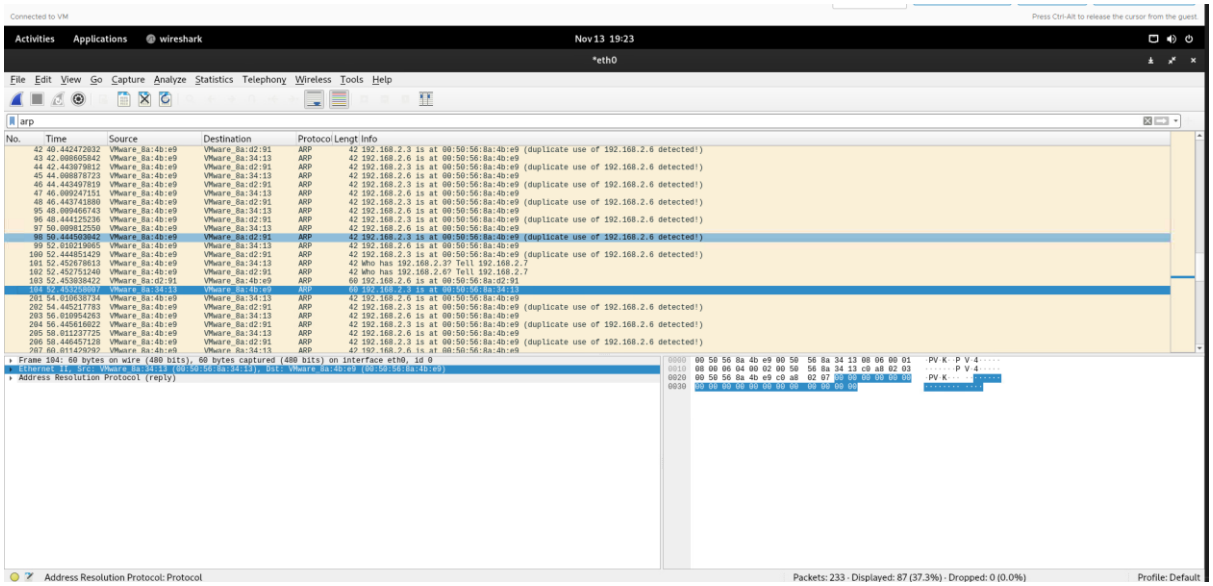
17. Paste a screen shot showing the FTP data for this file.

Ans:



18. Are there any packets that might send up a red flag that an ARP poisoning attack is occurring?

Ans:



19. In this example, are attack focused on two systems on the same network. If you were trying to capture traffic coming and going from two systems on different networks, what IPs would you want to poison?

Ans: Traffic between two systems on the same network is usually intended to be redirected in an ARP poisoning attack. Traffic is redirected via the attacker as a result of ARP poisoning, which entails sending fictitious ARP answers in order to link the attacker's MAC address to the victim system's IP address.

ARP poisoning would not be enough by itself if you were attempting to intercept communication between two systems on separate networks. The local assault known as ARP

poisoning takes place inside the same broadcast domain. Generally, routers divide networks apart, and ARP queries don't traverse router borders.

Other methods, such as Man-in-the-Middle (MitM) assaults, which target the routers or gateways connecting the networks, may be of use to collect communication between devices on separate networks. Attackers may use DNS spoofing, routing protocol flaws, or other techniques to intercept and modify communications.

You might wish to target the IP addresses of the routers or gateways that connect the two networks in these kinds of situations. An attacker may intercept and alter communications flowing through the router by breaking into it.

Remember that carrying out network attacks should only be done in a controlled setting with the appropriate authorization and ethical standards followed, not even when done for testing or instructional purposes. It is against the law and morality to manipulate or intercept network communication without authorization. Before doing any action that involves intercepting or altering network communication, make sure you have the proper authorization.

20. What could likely occur alerting security to an attack in the last question?

Ans: When an attacker uses ARP poisoning to try and intercept communication between two systems on separate networks, a number of security warnings could go out. An unusual volume of ARP traffic or irregularities in ARP answers might be picked up by network monitoring tools and Intrusion Detection Systems (IDS), which would indicate a possible ARP poisoning assault. Unusual patterns might raise suspicions, such as repeated MAC address changes or mismatched IP-MAC combinations.

Moreover, anomalous activity at the routers or network gateways may set off alarms. Security systems may identify any effort to tamper with DNS spoofing, modify routing tables, or make unwanted modifications to network configurations.

Moreover, the assault may cause hiccups or performance problems for the targeted systems. Connectivity issues, strange network activity, or security software alerts are among the things that users may report.

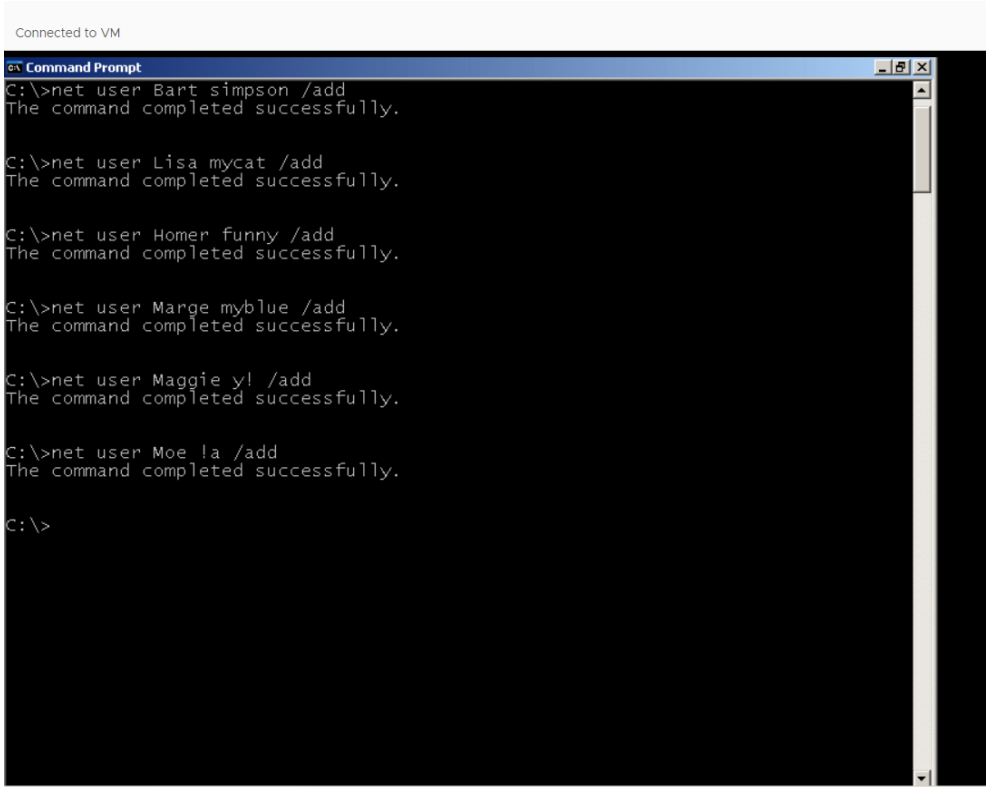
Firewalls and intrusion detection systems, among other security appliances, may provide warnings or notifications to network administrators and security teams that are watching over network traffic, pointing out questionable activity. ARP requests and answers log entries and anomalies, particularly those impacting vital network infrastructure, may be logged for additional analysis.

Lab 5: Password Cracking

- Create the following users and passwords on your Windows XP system.
- Hint: You can use the GUI user management or the net user command:

net user <username><password> /add

Username	Password
Bart	simpson
Lisa	Mycat
Homer	Funny
Marge	Myblue
Maggie	y!
Moe	!a

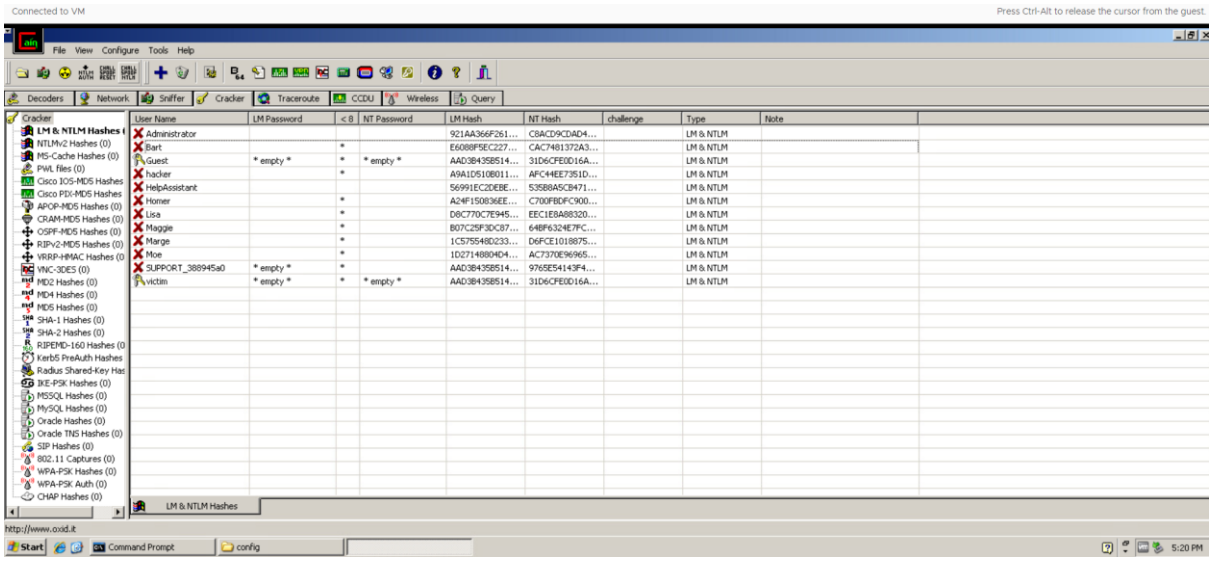


Users' passwords are not stored in the Microsoft Windows registry. Instead, their password hashes are stored in the SAM file in C:\Windows\System32\Config. There are programs, such as Cain, pwdump, and fgdump, which can dump these hashes. Cain is a GUI based program while pwdump and fgdump are command line tools. Cain can be downloaded from the following link: http://www.oxid.it/downloads/ca_setup.exe

- Log into the Windows XP system using the hacker user account. (Password : toor)
- Click the shortcut to Cain on the Desktop
- Click the Cracker tab(key icon) in the middle of the Cain program.
- Right-click in the white space and select Add to list

Verify that Import Hashes from local system is selected and click Next.

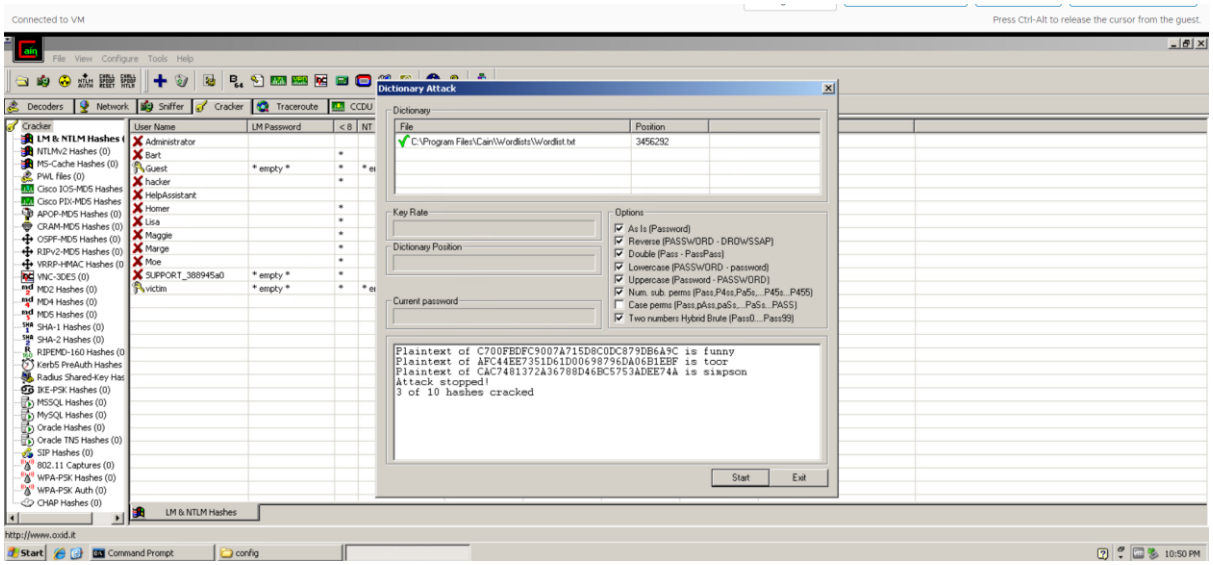
1. **Paste a Screen shot of the list of local windows accounts and their corresponding hashes.**



INFO: The two types of hashes extracted from the SAM file are the LM and NTLM hashes. The LAN Manager, or LM hash, dates back to the days of MSDOS. It is the default hash used for systems running DOS, Windows 3.11, Windows, 95, Windows ME, Windows NT, Windows 2000, Windows XP, and Windows 2003. Some of the newer operating systems in the list can have their security settings adjusted so that the LM hash will not be used. However, their default operating system setting is to use the LM hash, not NTLM. The NTLM, or New Technology LAN Manager hash, has been around for a while but it was not until the release of Windows Vista that it became the default hash used. Windows Vista, Server 2008, Windows 7, Server 2012, and Windows 8 all are set to use the NTLM hash by default. However, their security settings can be scaled back to use the older, less secure, LM hash. It is more secure for the OS to use the NTLM hash.

- Right-click in the white space and click on **Select All** to select all accounts.
- Right-click and then select **Dictionary Attack**, and then select the **NTLM Hashes** choice from the list
- Right-click in the top pane under the word dictionary and select **Add to list**
- First, double-click on the **Wordlists** folder. Now, double-click on **wordlist.txt**
- Click the **start** button in the bottom right corner to start the dictionary attack.

2. **Paste a Screen shot showing the password hashes that revealed.**

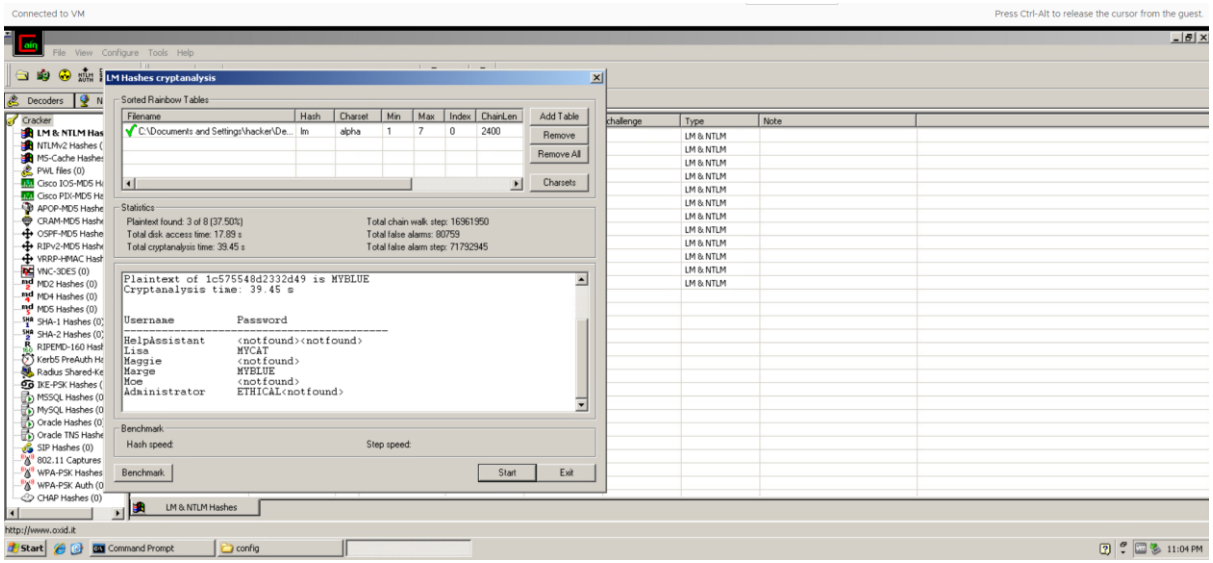


INFO: The wordlist.txt dictionary file that comes with Cain is located in the following directory: C:\Program Files\Cain\Wordlists. If the plain text passwords are not located within the dictionary file, the plaintext passwords will not be revealed. Another method, such as a brute force attack or Cryptanalysis Attack (Rainbow Table) will have to be utilized. In order to perform a Cryptanalysis Attack with a Rainbow Table, you will need one or more Rainbow Tables. Rainbow Tables can be created with a program like Winrtgen, which is located in the C:\Program Files\Cain\Winrtgen folder. This program is placed in this folder when Cain is installed on the system. Double-clicking on the Winrtgen.exe file will open up a Rainbow Table generator for Windows. By clicking the add Table button, LM or NTLM rainbow tables can be generated. The time to generate the Rainbow Table will depend on the character set used and the maximum password length. Rainbow Tables can take a few hours or a number of years to generate, depending on the options selected.

- *Hold down the **CTRL** key and select the accounts without revealed passwords. Right-click, select **Cryptanalysis Attack > LM Hashes via RainbowTables (RainbowCrack)***
- *Click the **Add Table** button in the right hand pane of the LM hashes cryptanalysis window.*
- *Browse to the desktop, and choose the LM rainbow table with the name **lm_alpha#1-7_0_2400*40000000_oxid#000.rt**. Double-click on it, then click **Start** to begin the Cryptanalysis Attack.*

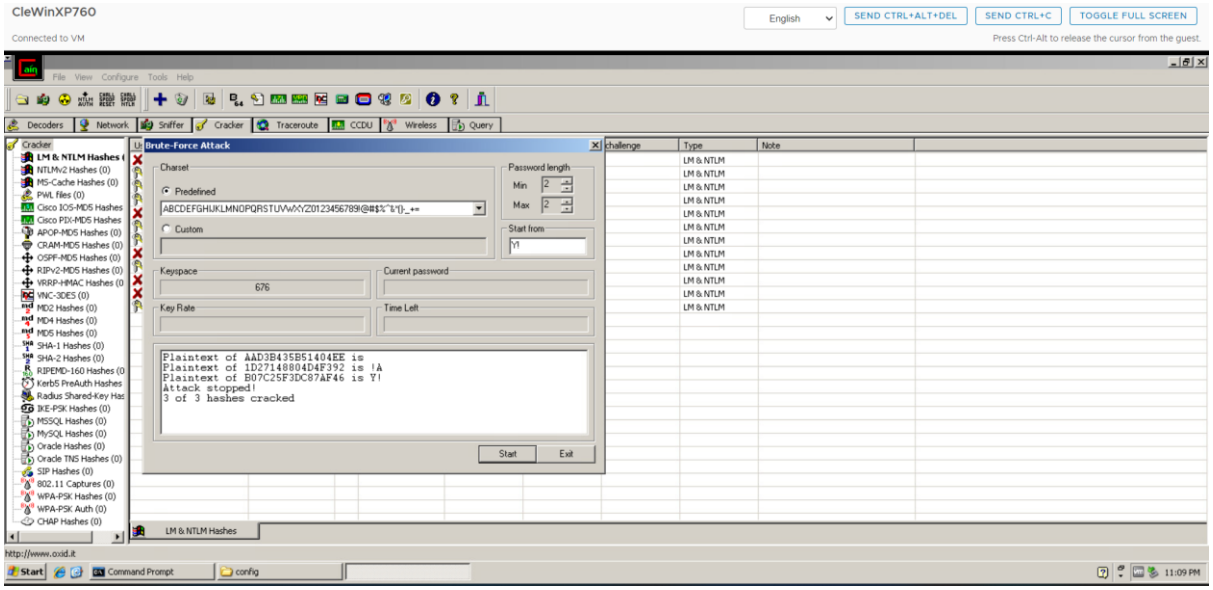
3. **Paste a screenshot showing the additional passwords that are now revealed.**

Ans:



- *Hold down **CTRL** and select **Maggie** and **Moe**. (Don't include Help Assistant or support) right-click, select **Brute Force Attack**, and then select **LM Hashes**.*
- *Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length(Max) to 2 by using your mouse to reduce the max from the default. Click **start**.*

4. **Paste a screen shot showing the revealed passwords.**



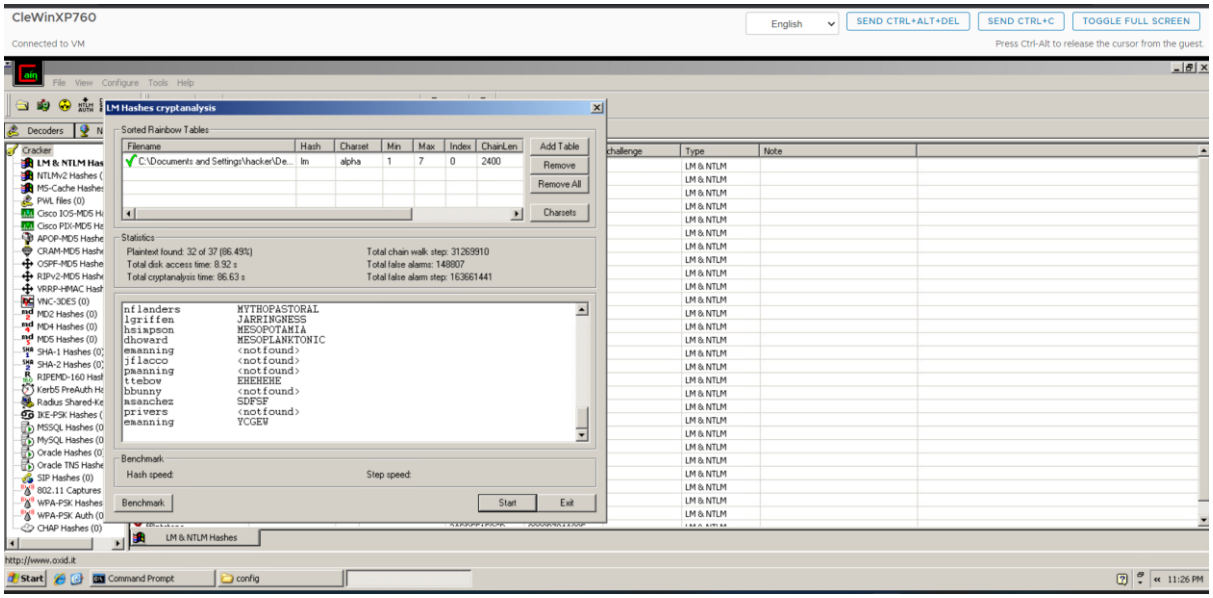
INFO: All of the passwords you assigned to the users in this exercise were cracked. The HelpAssistant and Support Accounts were not cracked. These accounts are disabled on the system anyway by default, so it is not really necessary to crack their passwords.

Although Brute Force could be used to crack these accounts, it is likely to take a long time. The administrator password will be attacked later using a different technique

- *Right-click in the white space and select Remove all to remove the accounts.*
- *Right-click in the white space of the Cracker tab and select Add to list*
- *Click the radio button to Import Hashes from a text file.*
- *Click the Browse square on the right. Click Desktop and click accounts.txt*
- *Click Next. You should see a large list of users, starting with pmanning.*
- *In order to crack the passwords for all the users, we can use one of three methods:*
  - *Cryptanalysis Attack(Rainbow Table)*
  - *Dictionary Attack*
  - *Brute Force Attack*
- *First, let's try to crack as many passwords from the list by using the Rainbow Table.*
- *To crack the user's passwords listed, right-click and choose Select All.*
- *The usernames in the list will be highlighted blue. To crack passwords, right- click and select Cryptanalysis Attack LM hashes via RainbowTables(RainbowCrack).You should receive the message that 37 hashes of type NTLM loaded…*
- *Click the Start button to begin the Cryptanalysis Attack on the hashes.*
- *After the Cryptanalysis Attack is over, 32 or 37 plaintext passwords will be revealed.*

5. **Paste a screen shot showing the passwords that were revealed.**

Ans:

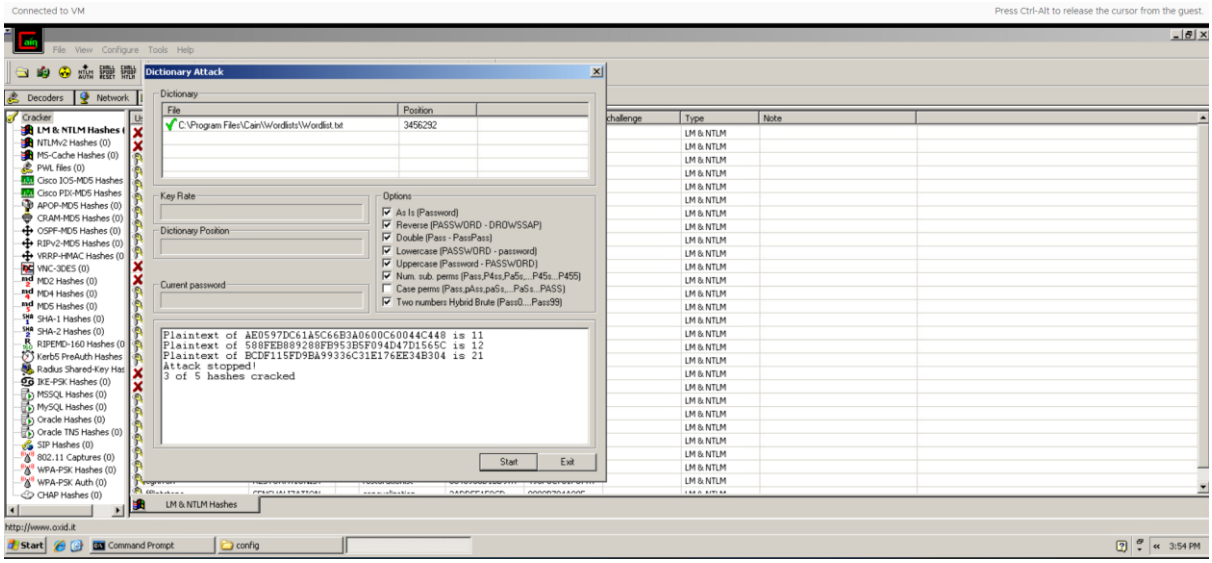


- *Click **Exit** to leave the Cryptanalysis Attack screen to return to the user list.*
- *Notice that all but six of the users' passwords have been cracked. Hold down **CTRL** and select the remaining six accounts without revealed passwords. Right-click, select **Dictionary Attack**, and then select the choice for **NTLM Hashes**.*
- *Before starting the Dictionary Attack, we need to reset the initial file position of the dictionary. If this is not done, the dictionary attack will start from where the attack last left off. It is always a good idea to reset the initial file position of the Dictionary file.*

- *Right-click on **Wordlist.txt** dictionary file and select **Reset Initial File Position**.*
- *Click the **Start** button to attack the 5 loaded hashes of type NTLM*

6. Paste a screen shot showing the cracked hashes.

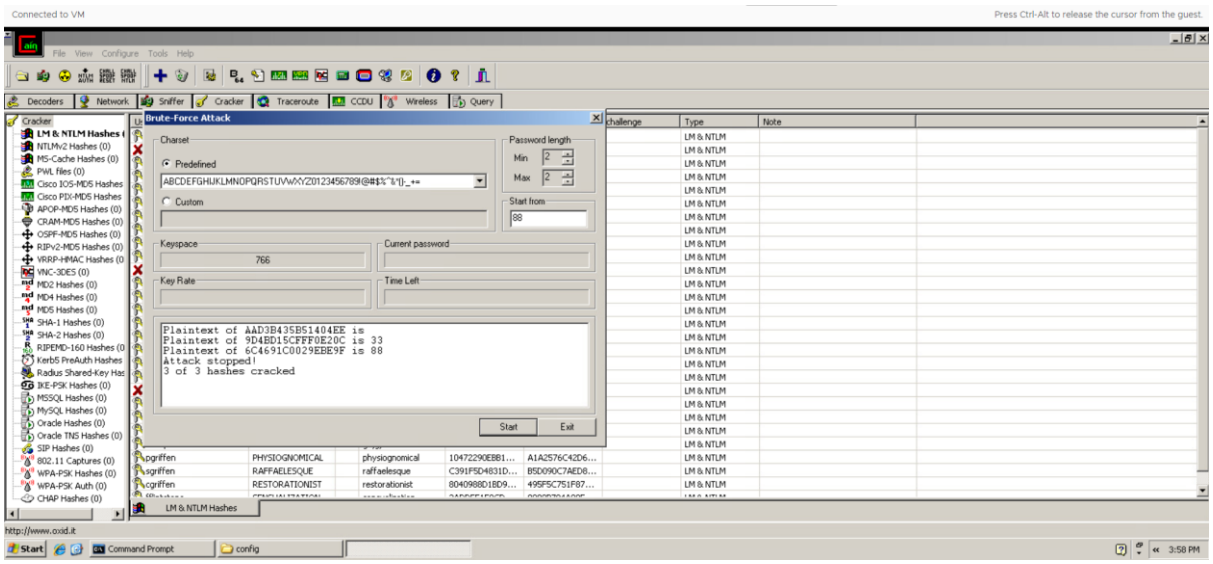
Ans:



- *Notice that all of the users' passwords have been cracked except six of them. Hold down **CTRL** and select the accounts without revealed passwords. Right-click, select **Brute Force**, and then select the choice for **LM Hashes.***
- *Click the arrow for the dropdown box for the character set. Pick the second character set in the list. For the password length, change the maximum length **(Max) to 2** by using your mouse to reduce the max from the default. Click **Start** You will receive the message, 3 hashes of type LM loaded. Click **Start***

7. Paste a screen shot showing the hashes that were cracked.

Ans:



Questions:

8. **What file can be used to generate a Rainbow Table?**

Ans: Usually used for password cracking, a rainbow table is a precomputed table for reversing cryptographic hash algorithms. Oftentimes, the file that is utilized to create a Rainbow Table is called the "rainbow table file." This file includes a large collection of precomputed hash values for a range of potential plaintext inputs, together with the original inputs that correspond to those values. The method of creating rainbow tables is hashing a beginning plaintext, decreasing the hash using a number of reduction functions to a new form, and then repeating this process to produce chains of hash values. In order to draw attention to the weaknesses of using weak or widely used passwords, rainbow tables are mostly used in security assessments. This highlights the need of using strong, unique passwords and cryptographic mechanisms that fend against such assaults. Note that adding further difficulty to passwords through the use of salt, a random value exclusive to each password, lessens the impact of Rainbow Table assaults.

9. **Why would you want to change the character set before you attempt a Brute Force Attack?**

Ans: When undertaking a Brute Force Attack, changing the character set beforehand is a tactic used to boost the attack's efficacy and efficiency, particularly when trying to crack cryptographic keys or passwords. When we talk about the character set, we mean the range of characters—uppercase, lowercase, digits, and special symbols—that may be used in a password or key. An attacker can adjust the character set to better fit the target password's expected composition and so better target the brute force assault.To speed up the assault and reduce the total number of possibilities to try, an attacker may decide to concentrate the brute force attack on a particular character set, such as lowercase letters and numerals, provided they have information indicating that these are the most probable characters to be included in the password. By utilizing this method, the brute force process may be made much more efficient, increasing the likelihood of breaking weak passwords in a fair amount of time. To counter brute force assaults, it's vital to remember that employing strong encryption methods, enforcing account lockout procedures, and improving password restrictions are essential.

10. **Where is the dictionary file located that comes with the Installation of Cain?**

Ans: The dictionary file can be located in C:\Program Files\Files\wordlists

11. **Which Microsoft operating systems are unlikely to have LM hashes present?**

Ans: An early version of Microsoft operating systems employed a password hash type called LM (LAN Manager) hashes. Because to LM hashes' well-known flaws, security concerns have led contemporary Windows operating systems to stop utilizing them. Microsoft operating systems released after Windows Vista have a lower likelihood of having LM hashes present, as of my knowledge cutoff in January 2022. Microsoft moved to more secure password hashing techniques, such NTLM (New Technology LAN Manager) and Kerberos, starting with Windows Vista and later versions (like Windows 7, Windows 8, and Windows 10).

Passwords are therefore unlikely to be stored in the susceptible LM hash format on Windows operating systems produced after Windows Vista. Strong password regulations, multi-factor authentication, and frequent security upgrades are necessary for upholding a safe environment; it's crucial to remember that utilizing more secure hashing techniques does not render a system

impervious to password attacks. Furthermore, after my previous knowledge update in January 2022, Microsoft could have released new operating systems or upgrades.

Module Activity Description:

Part Three: Dumping Windows Passwords in clear Text

- Open the shortcut to the command prompt on the Windows XP Pro desktop
- Drag the wce.exe file into the Command Prompt window.
- Add a space and a question mark to the command to see the available switches:

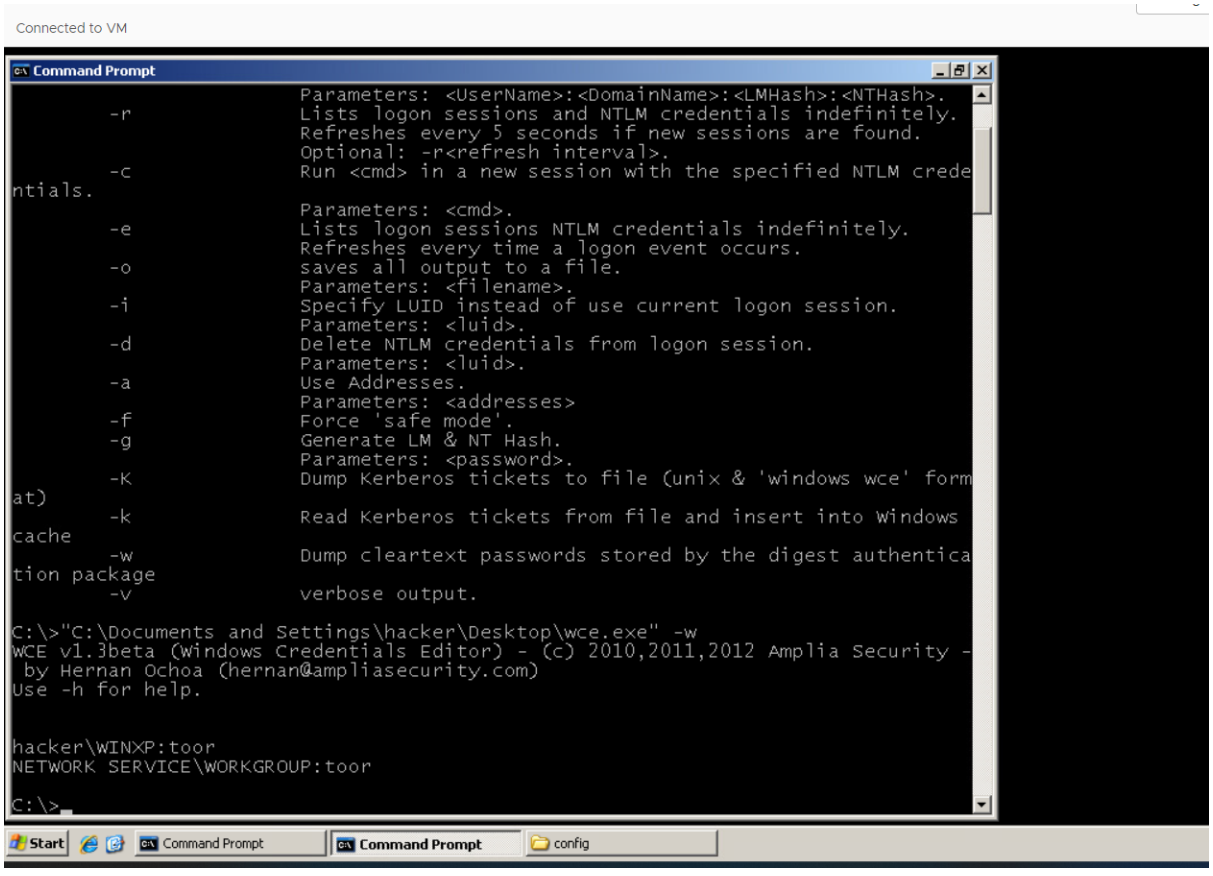
C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" ?

- Add a space and a -w to the command to dump the clear text passwords:

C:\>"C:\Documents and Settings\hacker\Desktop\wce.exe" –w

12. Paste a screen shot of the results for this command?

Ans:



Info: The mimikatz tool can also dump the passwords of other users that have logged on.

- Log off as hacker by clicking on the Start button and selecting Log Off.
- Then, click Log off a second time when an additional log off box appears.
- Log on as Administrator with the password of Ethicalhackin&

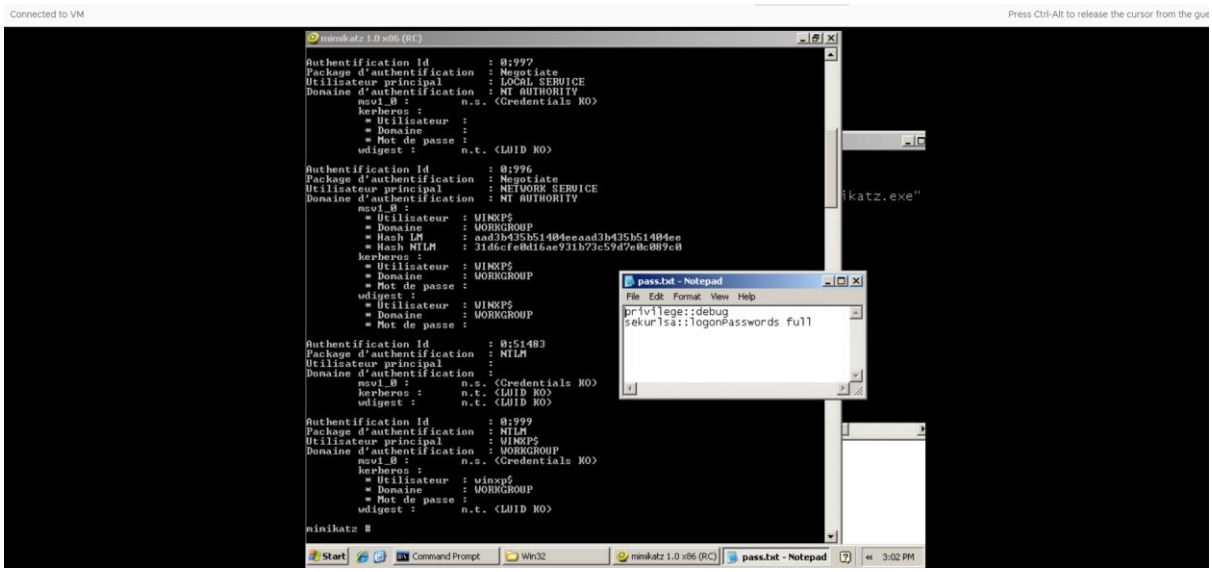
- Log off as administrator by clicking on the Start button and selecting Log Off
- Do NOT LOG OFF, Select Switch Users instead, which will leave Administrator logged Into the system.
- Log back into the XP system using the hacker account with the password of toor.
- Open the shortcut to the command prompt on the Windows XP Pro desktop.
- Double-click on the Win32 folder on the Desktop of the hacker account. Drag the mimikatz file from the Win32 folder into the command prompt Window.
  C:\>"C:\Documents and Settings\hacker\Desktop\Win32\mimikatz.exe"
- Double-click on the pass.txt file in the Win32 folder. Copy the first line, privilege::debug and paste it into the mimikatz terminal

mimikatz # privilege::debug

- If successful, you will receive the following message back from the mimikatz prompt: Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK
- Paste the second line from the pass.txt file into the mimikatz terminal:
  mimikatz # sekurlsa::logonPasswords full

13. Paste a screen shot showing the Administrator password. Note: You may need to go back and redo steps 5-12 if you do not see the administrator's password dumped in clear text. These steps should be done in a timely fashion.

Ans:



Questions:

14. What switch allows you to dump plain text passwords with WCE?

Ans: Add a space and a –w switch allows to dump plain text passwords with WCE.

15. How does the WCE tool differ from the mimikatz tools?

Ans: Although they both concentrate on extracting and modifying credentials in Windows systems, the Windows Credential Editor (WCE) program and Mimikatz have different methodologies and features. Plaintext password and hash password extraction from memory is WCE's primary area of expertise. It is intended to specifically target and take advantage of holes in the way Windows runstime stored credentials. WCE is particularly useful against services like Remote Desktop Protocol (RDP) and Windows authentication protocols. It may be used to extract credentials from processes, including those associated with login sessions.

Contrarily, Benjamin Delpy's Mimikatz is a more complete post-exploitation utility. Password hashes, plaintext passwords, and Kerberos tickets may all be extracted from memory using Mimikatz, among its many extended features. It's also well-known for its capacity to carry out pass-the-hash attacks, in which a hacker doesn't need to know the real password in order to authenticate by using a hashes of the password they've got.

16. What must a user do in order for mimikatz to retrieve a password from RAM?

Ans: The Target system must be logged on in order for mimikatz to retrieve password from RAM.

Module Activity Description:

Part Four: Hacking Linux passwords with jack the Ripper

Complete the following section on your Kali Linux system

INFO: First, we will examine the passwd file, which contains the list of all of the user accounts on the Linux system. The passwd file is located within the /etc directory.

- To view the contents of the passwd file, type:
  cat /etc/passwd
- View the permissions on the /etc/passwd file by typing the following command:
  ls -l /etc/passwd
  INFO: Notice that all users have at least read permissions. Only root has write permissions. At one time, the password was stored in the passwd file. However, due to the fact that that the passwd file does not have very restrictive permissions, the password is no longer stored there. Instead, there is an X present, which designates that it is stored in the shadow file
- To view the contents of the shadow file, type:
  cat /etc/shadow
- To create a new user named yoda, type the following command in the terminal:
  useradd yoda
- To create a new user named chewbacca, type the following command in the terminal:

useradd Chewbacca

- Now, view the changes made to the passwd file by typing the following:
  tail /etc/passwd
- Next, examine the alterations to the shadow file by typing the following:
  tail /etc/shadow
  INFO: The "!" symbol (often called a bang) represents that fact the password has not been set.
- Examine the entries in the auth.log related to account changes by typing:
  tail /var/log/auth.log

Next, we will give each user a password. We will use simple passwords for the exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. Retype the password and it will be accepted. For security reasons, the password will not be displayed.

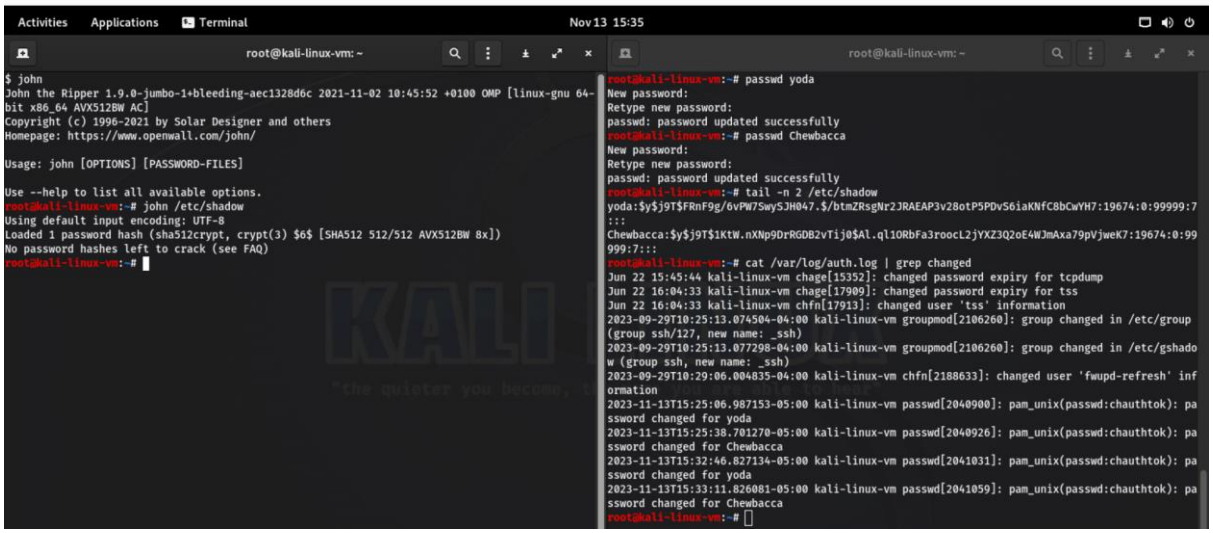
- Set chewbacca's password to green by typing "green" twice after typing: passwd Chewbacca
- Next, examine the alterations to the shadow file by typing the following:
  tail –n 2 /etc/shadow

INFO: The password hashes are salted, which means if you give two users the same exact password, a different hash will be displayed. When salting is done, you will be unable to perform a rainbow table attack. Instead, you will need to perform a dictionary or brute force attack. You cannot use a rainbow table attack against a hash that has been salted. Both user's passwords were set to "green" but are different because they were salted Changes to accounts, such as setting a password, will be logged in the auth.log.

- To look for specific information about password changes within auth.log, type: cat /var/log/auth.log | grep changed
- Start John the Ripper by going to Applications>Password Attacks>John
- This will open a new terminal window
- Type the following command to attempt to crack the passwords with john: john /etc/shadow

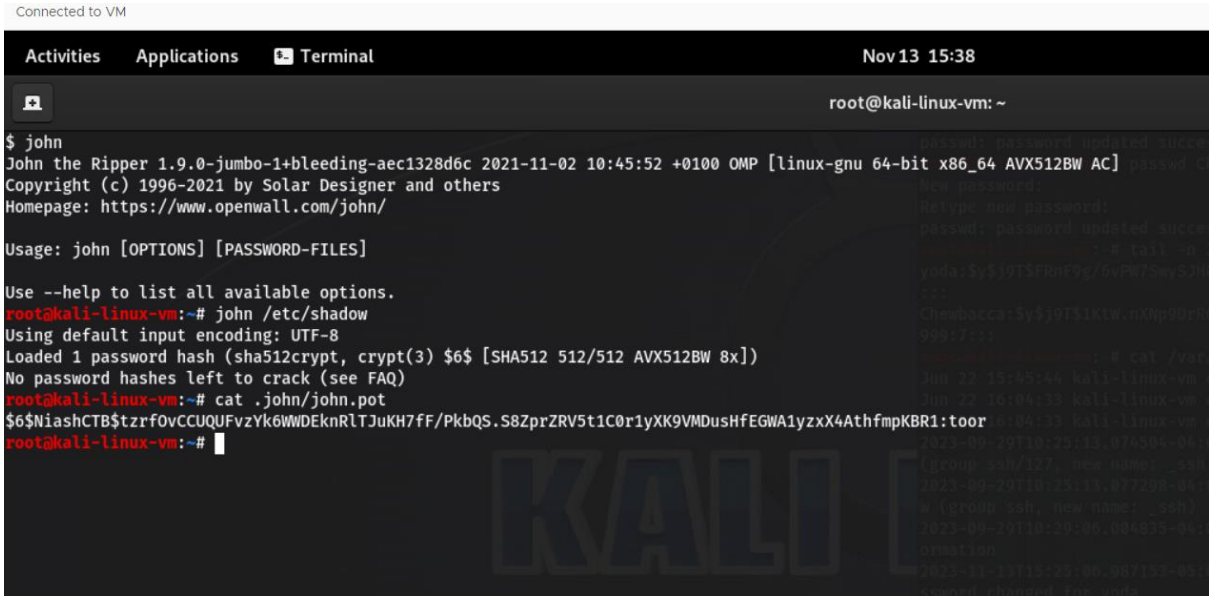
17. Paste a Screen shot of the cracked password.

Ans:



Notice that even though there were only 2 different passwords in the list, the messages from john indicated that it loaded 3 password hashes with 3 different salts. If you need to view the password hashes and the corresponding revealed passwords at future time, you can always retrieve them from the john.pot file where they are stored.

- To view the password hashes and corresponding passwords, type the following: cat .john/john.pot



18. What is stored within the shadow file?

Ans: The User account information and encrypted passwords are stored within the shadow file.

19. What a user is created on linux system, which file has a record of it?

Ans: When a user is created on Linux system, password file will be created has a record of it.

For example, a line in the "/etc/passwd"

20. What is the command to change a user's password on a Linux system?

Ans: The command to change a user's password on a Linux system is "passwd" command.

21. Where does the John the Ripper store the passwords after they cracked?

Ans: The John the Ripper stores the file in John.pot file after they are cracked.

Module Activity Description:

Part Five: Creating an Additional Account with root Level Permission

Info: On Microsoft Windows operating systems, you can create multiple accounts with administrative rights. On a Linux system, there is usually only one root account. However, if another account is created with a UID of 0, that account will have root level permissions. We will modify the /etc/passwd and /etc/shadow to create an account that is 'equivalent' to root. In order to do this, you would need the password for the root account, physical access, or a local exploit that would elevate your permissions to root.

- Type the following command to open the passwd file located in the /etc folder:
  gedit /etc/passwd
- Copy the first line of the file. Go down in front of the "d" in daemon and hit enter. Go up one line to the blank line and paste the root account info into the 2nd line.
- Change the name on the second line from root to vader. Save and close the file.
- Type the following command to open the passwd file located in the /etc folder.
  gedit /etc/shadow
- Put your cursor in front of the "d" in daemon. Right-click on the first two lines of the file and click copy. Go down in front of d in daemon, right-click and paste
- Change the name on the third line from root to vader. Save and close the file.

INFO: When we utilized the useradd and passwd commands during the first task, the commands triggered events in auth.log. In this task, however, a user named vader was created with the password of toor, by editing the passwd and shadow files.

- Type the following to see if there is evidence of the vader account in auth.log.
  tail /var/log/auth.log

INFO: The reason that there is no evidence of the vader account being created or given a password is because the /etc/passwd and /etc/shadow files were manually edited. Another trick we used was the placement of the account. When the yoda and chewbacca accounts were created, they were added to the bottom of the /etc/passwd and /etc/shadow files. When new accounts are added, that is the location they are placed.

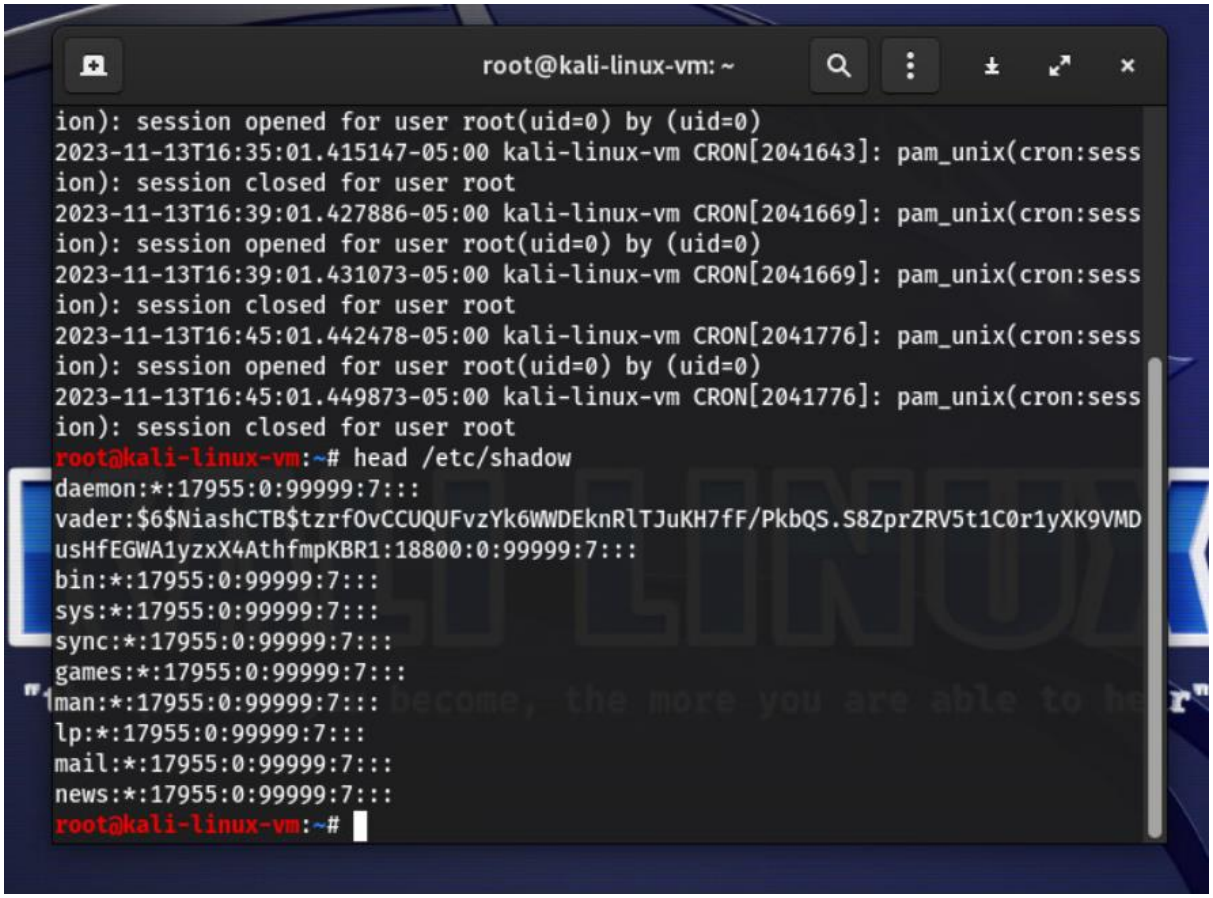
- Test the new account by logging out of your system and logging back in with the vader account. The password should be the same as your root account**.**

We were able to log in as our account with root level permissions, but we need to verify that we can perform tasks that only the root account is allowed to do on the system.

- To prove that you actually do have root level access, type the following:
  head /etc/shadow

22. Paste a screenshot showing the /etc/shadow file.

Ans:



23. When the useradd command is utilized, which file has a record of the event?

Ans: Auth.log file has a record of the event when the useradd command is utilized.

24. When the passwd command is utilized, which file has a record of the event?

Ans: There will be no record of the event will be recorded when the passwd command is utilized.

Part Six: Enumerating users

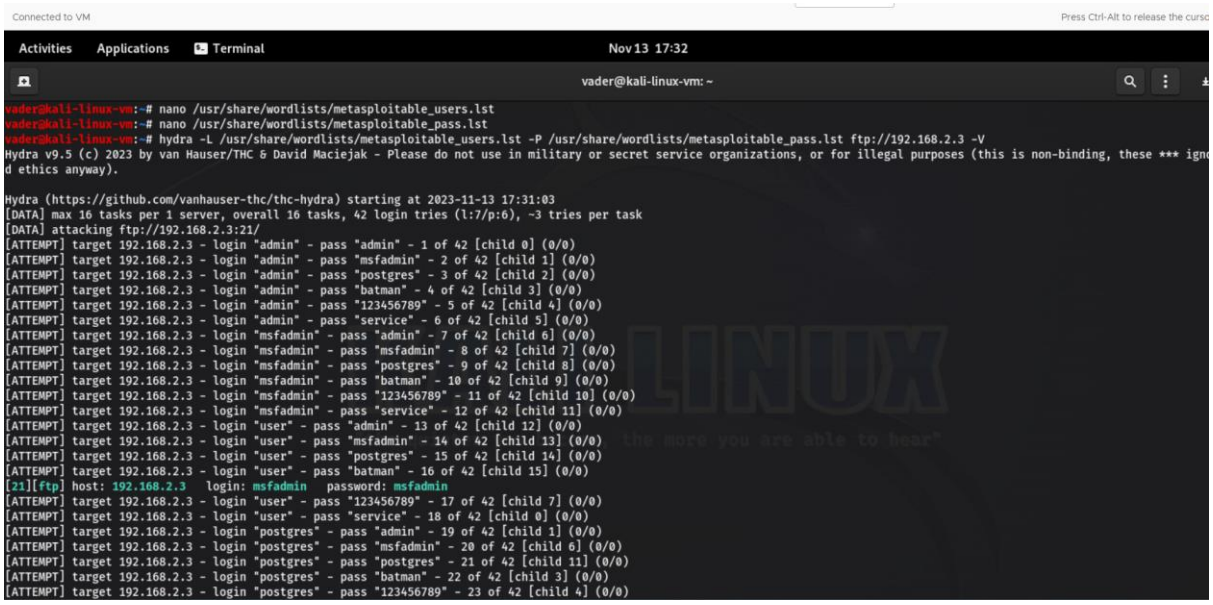
In the previous sections of this lab, we ran password attacks on systems we were already logged into and/or had access to the user and password hash files. Therefore, it was quite simple to run various attacks knowing the usernames and hashes. These were all examples of offline attacks. Often we may not know the usernames ahead of time, so we have to determine those. This is a process known as enumerating users. There are many different tools we can use.

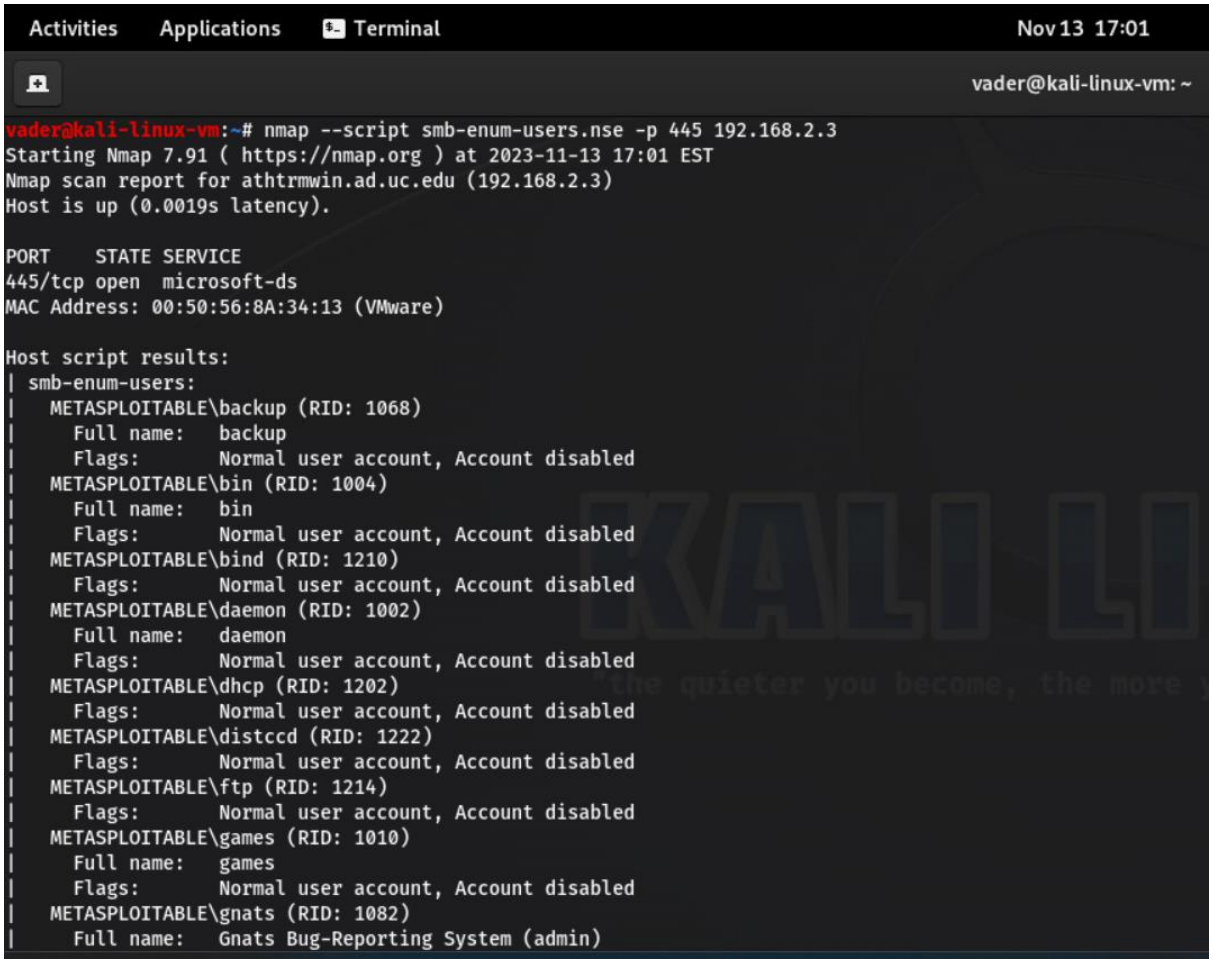
Part 5.1: Enumerating user with nmap

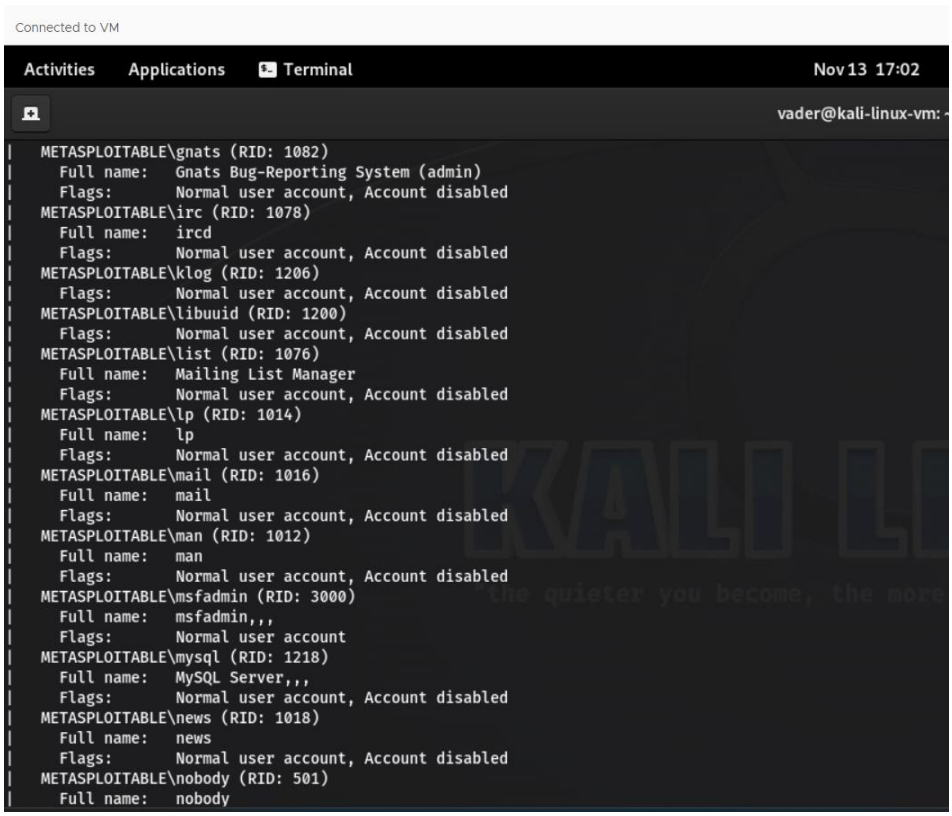
- *In order to enumerate the user accounts available on the target machine we will be using the following Nmap script: smb-enum-users. We can run the NMap script by using the following command:*
  nmap --script smb-enum-users.nse –p 445 [IP of Metasploitable2]

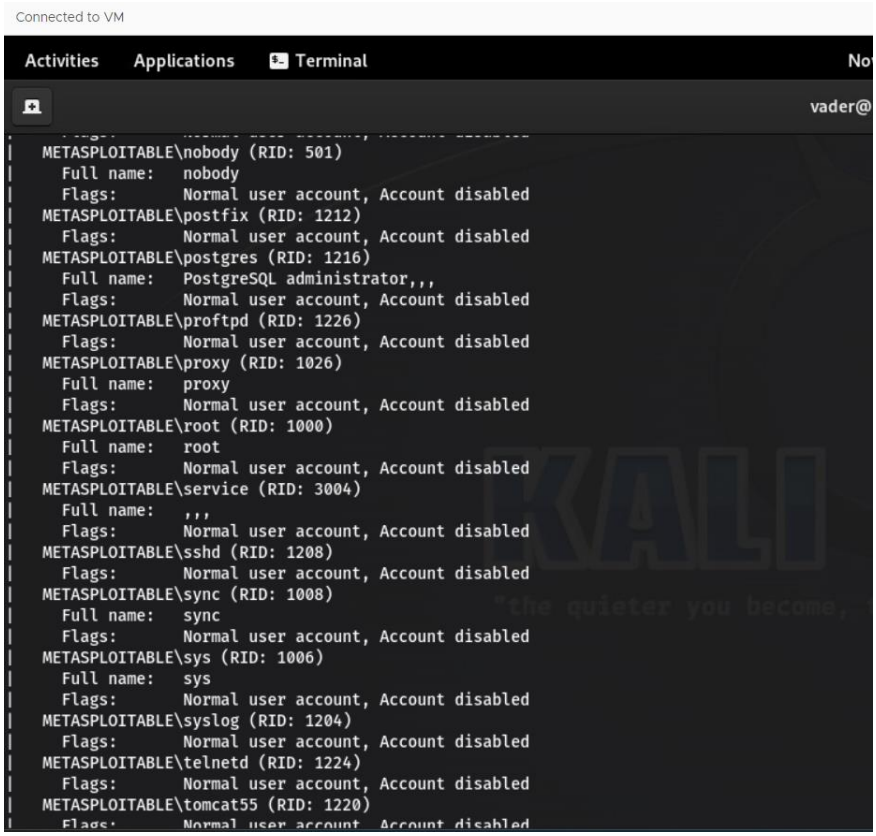
25. Paste a screen shot of the all the user accounts that you found.

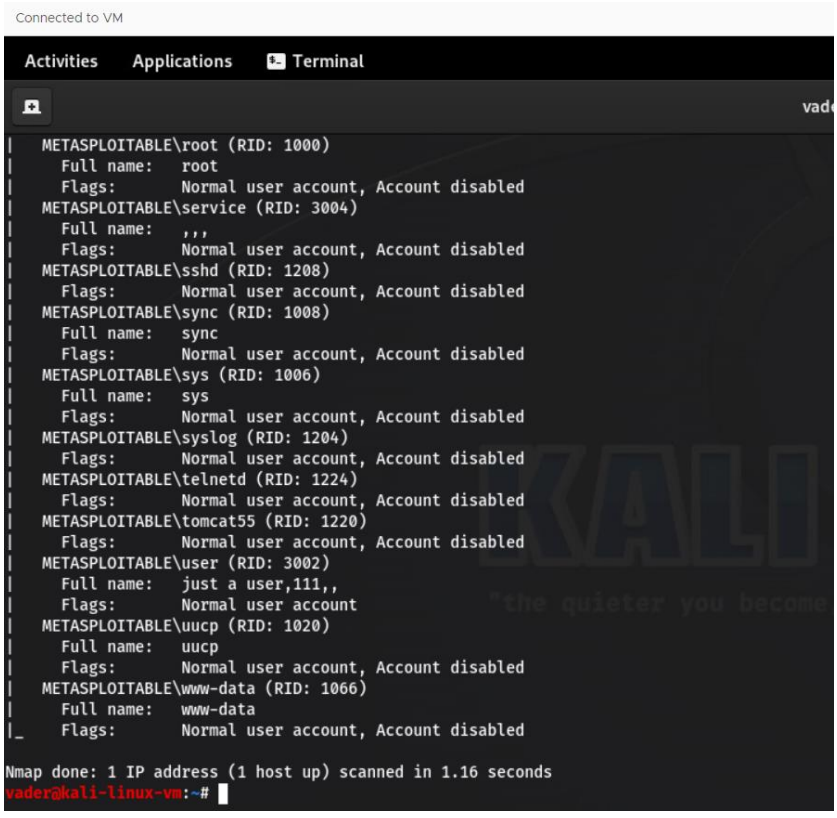
Ans:




Activities
Applications
Terminal
Nov 13 17:01
vader@kali-linux-vm: ~
vader@kali-linux-vm:~# nmap --script smb-enum-users.nse -p 445 192.168.2.3
Starting Nmap 7.91 (https://nmap.org) at 2023-11-13 17:01 EST
Nmap scan report for athtrmwin.ad.uc.edu (192.168.2.3)
Host is up (0.0019s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:50:56:8A:34:13 (VMware)
Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
| Full name: backup
| Flags: Normal user account, Account disabled
| METASPLOITABLE\bin (RID: 1004)
| Full name: bin
| Flags: Normal user account, Account disabled
| METASPLOITABLE\bind (RID: 1210)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\daemon (RID: 1002)
| Full name: daemon
| Flags: Normal user account, Account disabled
| METASPLOITABLE\dhcp (RID: 1202)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\distccd (RID: 1222)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\ftp (RID: 1214)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\games (RID: 1010)
| Full name: games
| Flags: Normal user account, Account disabled
| METASPLOITABLE\gnats (RID: 1082)
| Full name: Gnats Bug-Reporting System (admin)


Connected to VM
Activities
Applications
Terminal
Nov 13 17:02
vader@kali-linux-vm:
| METASPLOITABLE\gnats (RID: 1082)
| Full name: Gnats Bug-Reporting System (admin)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\irc (RID: 1078)
| Full name: ircd
| Flags: Normal user account, Account disabled
| METASPLOITABLE\klog (RID: 1206)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\libuuid (RID: 1200)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\list (RID: 1076)
| Full name: Mailing List Manager
| Flags: Normal user account, Account disabled
| METASPLOITABLE\lp (RID: 1014)
| Full name: lp
| Flags: Normal user account, Account disabled
| METASPLOITABLE\mail (RID: 1016)
| Full name: mail
| Flags: Normal user account, Account disabled
| METASPLOITABLE\man (RID: 1012)
| Full name: man
| Flags: Normal user account, Account disabled
| METASPLOITABLE\msfadmin (RID: 3000)
| Full name: msfadmin,,,
| Flags: Normal user account
| METASPLOITABLE\mysql (RID: 1218)
| Full name: MySQL Server,,,
| Flags: Normal user account, Account disabled
| METASPLOITABLE\news (RID: 1018)
| Full name: news
| Flags: Normal user account, Account disabled
| METASPLOITABLE\nobody (RID: 501)
| Full name: nobody


Connected to VM
Activities
Applications
Terminal
vader@
| METASPLOITABLE\nobody (RID: 501)
| Full name: nobody
| Flags: Normal user account, Account disabled
| METASPLOITABLE\postfix (RID: 1212)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\postgres (RID: 1216)
| Full name: PostgreSQL administrator,,,
| Flags: Normal user account, Account disabled
| METASPLOITABLE\proftpd (RID: 1226)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\proxy (RID: 1026)
| Full name: proxy
| Flags: Normal user account, Account disabled
| METASPLOITABLE\root (RID: 1000)
| Full name: root
| Flags: Normal user account, Account disabled
| METASPLOITABLE\service (RID: 3004)
| Full name: ,,,
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sshd (RID: 1208)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sync (RID: 1008)
| Full name: sync
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sys (RID: 1006)
| Full name: sys
| Flags: Normal user account, Account disabled
| METASPLOITABLE\syslog (RID: 1204)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\telnetd (RID: 1224)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\tomcat55 (RID: 1220)


Connected to VM
Activities
Applications
Terminal
| METASPLOITABLE\root (RID: 1000)
| Full name: root
| Flags: Normal user account, Account disabled
| METASPLOITABLE\service (RID: 3004)
| Full name: ,,,
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sshd (RID: 1208)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sync (RID: 1008)
| Full name: sync
| Flags: Normal user account, Account disabled
| METASPLOITABLE\sys (RID: 1006)
| Full name: sys
| Flags: Normal user account, Account disabled
| METASPLOITABLE\syslog (RID: 1204)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\telnetd (RID: 1224)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\tomcat55 (RID: 1220)
| Flags: Normal user account, Account disabled
| METASPLOITABLE\user (RID: 3002)
| Full name: just a user,111,,
| Flags: Normal user account
| METASPLOITABLE\uucp (RID: 1020)
| Full name: uucp
| Flags: Normal user account, Account disabled
| METASPLOITABLE\www-data (RID: 1066)
| Full name: www-data
|_ Flags: Normal user account, Account disabled
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
vader@kali-linux-vm:~#

Part 5.2: Enumerating user accounts through null sessions with rpcclient

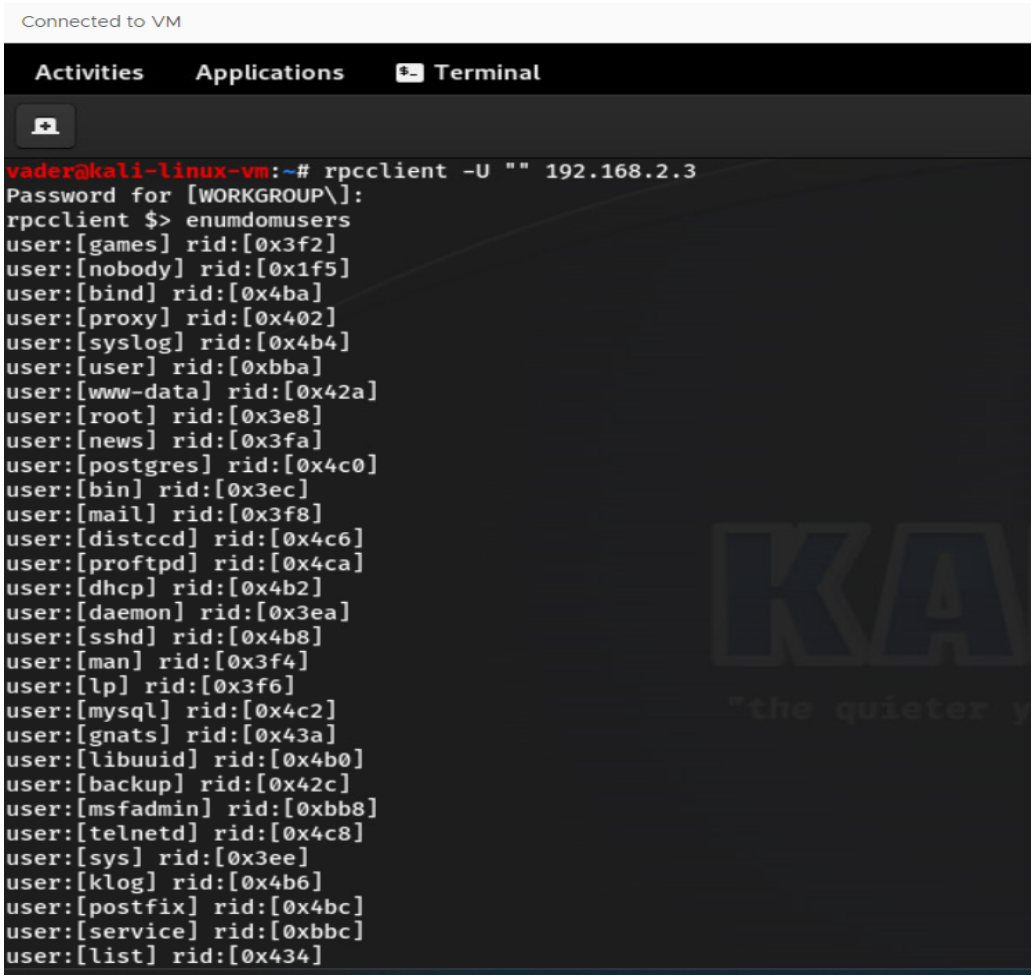
Rpcclient is a Linux tool used for executing client side MS-RPC functions. A null session is a connection with a samba or SMB server that does not require authentication with a password. No username or password is needed to set-up the connection and therefore it is called a null session. The allowance of null sessions was enabled by default on legacy systems but has been disabled from Windows XP SP2 and Windows Server 2003. The connection uses port 445 which is an open port on out target host as we've seen in the results of the port scan.

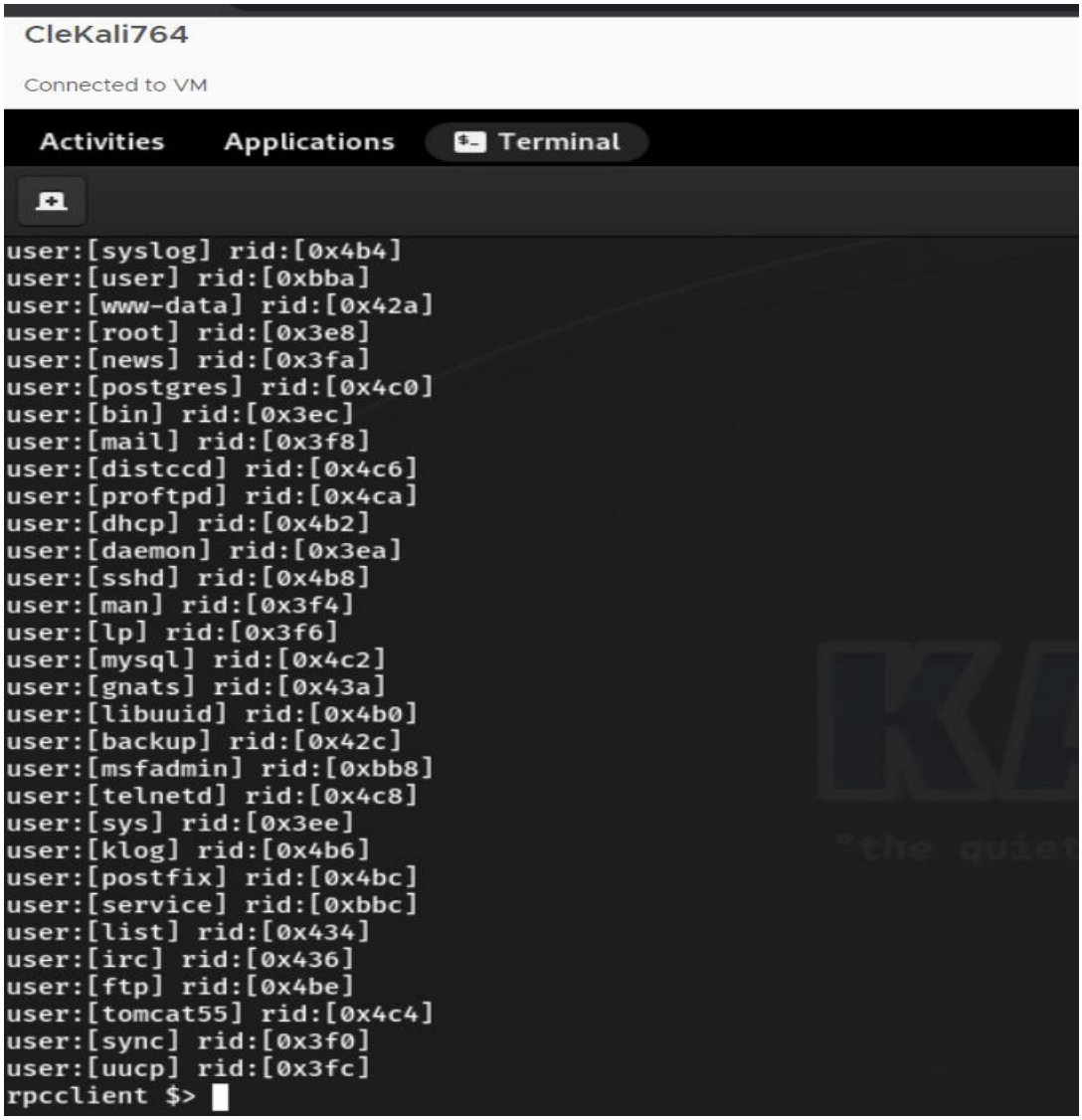
- Set up a null session with metasploitable 2 samba server using the following command: rpcclient –U "" <IP address of Metasploitable 2>
- Hit enter when promted for a password
- In the rpclient prompt run:

Enumdomusers

26. Paste a screen shot of the user list this generated.

Ans:





Module Activity Description:

Part seven: Online Dictionary Password Attacks

Once we have collected potential usernames from either enumeration or through OSINT, we can attempt to crack the passwords with either a dictionary or brute force attack. Either of which will likely take quite a bit of time. In this example, we will create a shortened user list and dictionary for demonstration purposes. Kali Linux does come with some pre-defined lists for dictionary attacks as well as common usernames. They are located in the /usr/share/wordlists directory. A popular dictionary is called "rockyou" and is comes zipped up.

- For our example, we will create our own lists.
- With your favorite text editor, create a file called: /usr/share/wordlists/metasploitable_users.lst
- add the following users (a new line for each.):
  - admin
  - msfadmin

- user
- postgres
- sys
- klog
- service

- Next create a new file called:

  /usr/share/wordlists/metasploitable_pass.lst

- Add the following words (a new line for each):
  - Admin
  - Msfadmin
  - Postgres
  - Batman
  - 123456789
  - Service
- Now we can Hydra to run a dictionary attack against the ftp service on our Metasploitable2 system.
- Run the following command:

hydra –L /usr/share/wordlists/metasploitable_users.lst –P /usr/share/wordlists/metasploitable_pass.lst ftp://<IP_metasploitable2> -V

27. Paste a screen shot showing each of the passwords that were found.

Ans: