|  |  |
| --- | --- |
| **Purple diagram of mountains and sea  Logo text: University of the Highlands and Islands, Executive Office, Ness Walk, INVERNESS IV3 5SQ  Oilthigh na Gàidhealtachd agus nan Eilean, Slighe Nis, Inbhir Nis IV3 5SQ** |  |

**Please attach these pages to the front of your assessment.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student ID &**  **Student Name** | **21010093**  **Calum Lindsay** | **Date submitted** | **13/05/2022** |
| Programme title | HNC Computing | | |
| Unit number | J0HK 34 | | |
| Unit title | Ethical Hacking | | |
| Learning outcome number | **Assessment 2** (covers Outcome 2,3 & 4) | | |
| Learning outcome title | Plan a penetration test.  Use current techniques to undertake a penetration test and exploit system vulnerability.  Implement appropriate countermeasures to mitigate a cyber-attack | | |
| Word count | N/A | | |

|  |  |
| --- | --- |
| **Checklist** | ✔ |
| Citations in the text use the UHI Harvard referencing system | N/A |
| All cited sources are listed alphabetically and in full in the bibliography | N/A |
| Word count is within 10% of the target length | N/A |
| File saved with the filename format ‘Student number\_unit initials\_LO number’ | N/A |

The University of the Highlands and Islands recognises that malpractice, where deliberately engaged in, is unacceptable and is considered a serious academic offence. A full copy of the university’s Malpractice Policy and Procedure can be found here: <https://myuhi.sharepoint.com/Policies/Forms/Public%20view.aspx>

Students are responsible for ensuring the work they submit is their own and complies with the ASQR and Malpractice Policy. If you have any queries you should contact your unit lecturer or Personal Academic Tutor (PAT) before submitting your assessment.

Please note that any case of suspected malpractice will be investigated according to current UHI Academic Standards and Quality Regulations (ASQR).

|  |  |
| --- | --- |
| In submitting this work, I confirm that I have read and understood UHI ASQR and malpractice policy and am aware of the possible penalties. | **🗸** |

|  |  |
| --- | --- |
| **Originality checker (to be completed if Turnitin is used)** | **🗸** |
| I confirm that I received information about the use of Turnitin and was directed to Turnitin training | **N/A** |
| I understand that this assignment will be submitted to Turnitin for originality checking | **N/A** |

|  |
| --- |
| **If you have received feedback/feedforward from coursework or an assignment for this unit/module/course, state the next steps**  You can either cut and paste these from previous assignment / coursework feedback, or pick some elements that you have decided you would like to work on |
|  |
| **If you have received feedback/feedforward from coursework or an assignment for this unit/module/course, state what you have done to address the next steps** |
|  |

**For staff use only**

|  |  |  |  |
| --- | --- | --- | --- |
| Lecturer contact number: [[1]](#footnote-1) | | | |
| Lecturer email: euan.robertson@uhi.ac.uk | | | |
| Feedback/feedforward return date | |  | |
| Feedback |  | | |
| Feedforward |  | | |
| Pass / Fail - to be ratified at Progression Board  (or Grade for HN Graded Units only) | | |  |
| Sampled for Internal Verification | | | Yes / No |
| **Assessment attempt:** 1 or 2 | | |  |
| **Is an application for an additional attempt in exceptional circumstances required? Yes / No** | | | |

Scope Report of Trilogy Europe

Investigation overview:

Trilogy Europe are a multi-national manufacturing company. They wish to tender for military contracts and therefore, wish to ensure their systems are resilient to cyber-attacks. They wish to keep this investigation internal to the company and don’t want anything related to it to leak to the news or general public. They want me to perform an internal penetration test on a portion of their network which is only used by the research and development section of the company as this is where the military work will be carried out. I will collate the results of this testing and produce a report detailing any threats and vulnerabilities found and any countermeasures I would recommend putting in place.

## Scope Report

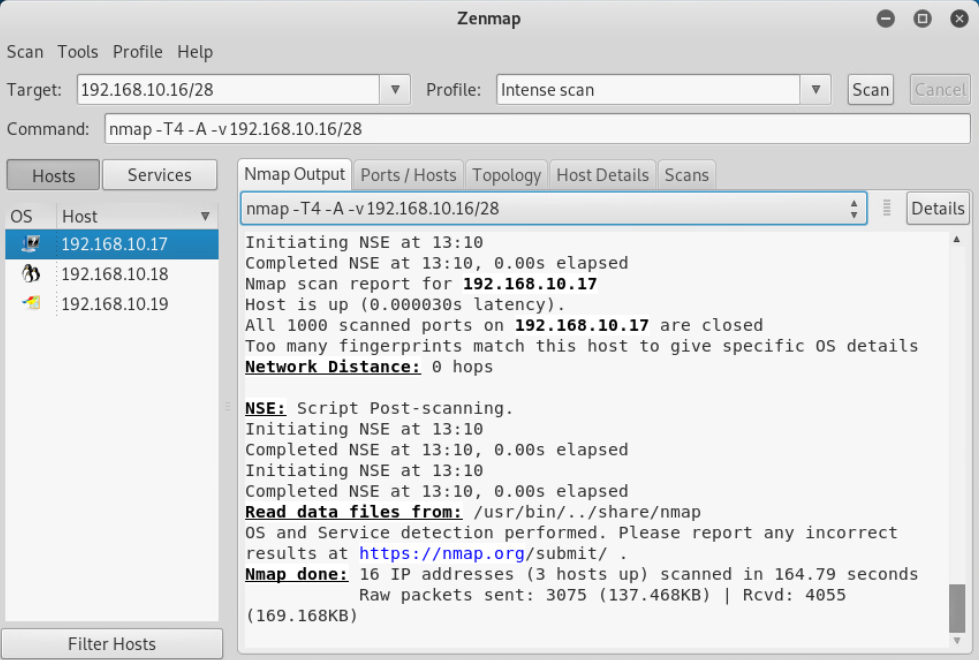
### Planning Stage:

*Pen-test completed and submission date: 13/05/2022*

* An internal investigation of the 192.168.10.16/28 Network is to be performed.
* Full access is allowed to all data within the network which includes creation, viewing or deletion of all files and other data stored on devices within the network.
* Everything within the network can be tested in any way.
* No social engineering will be performed.
* No external testing will be performed.

### Reconnaissance Stage:

First Zenmap was used to detect what devices were connected to the network and retrieve information about them. Zenmap discovered 3 devices one of which is the Kali-Linux computer that we are using to perform the penetration testing.



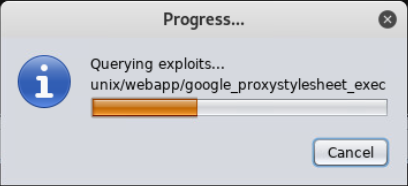
Details discovered about the other 2 devices to be tested are shown below in the following 3 tables:

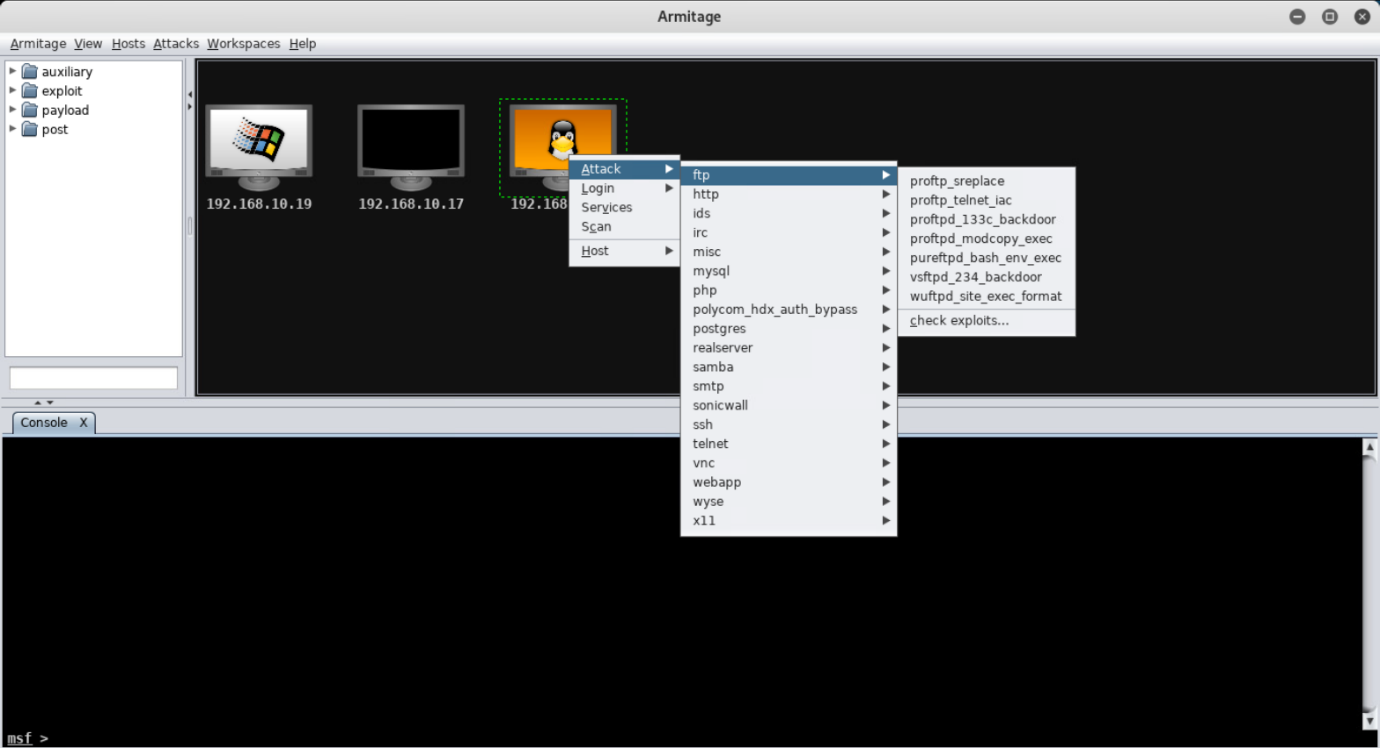
|  |  |  |
| --- | --- | --- |
| **Ip Address** | **Open Ports / Scanned Ports** | **Operating System** |
| 192.168.10.18 | 23/1000 | Linux 2.6.9 – 2.6.33 |
| 192.168.10.19 | 5/1000 | Microsoft Windows XP SP0 - SP1 |

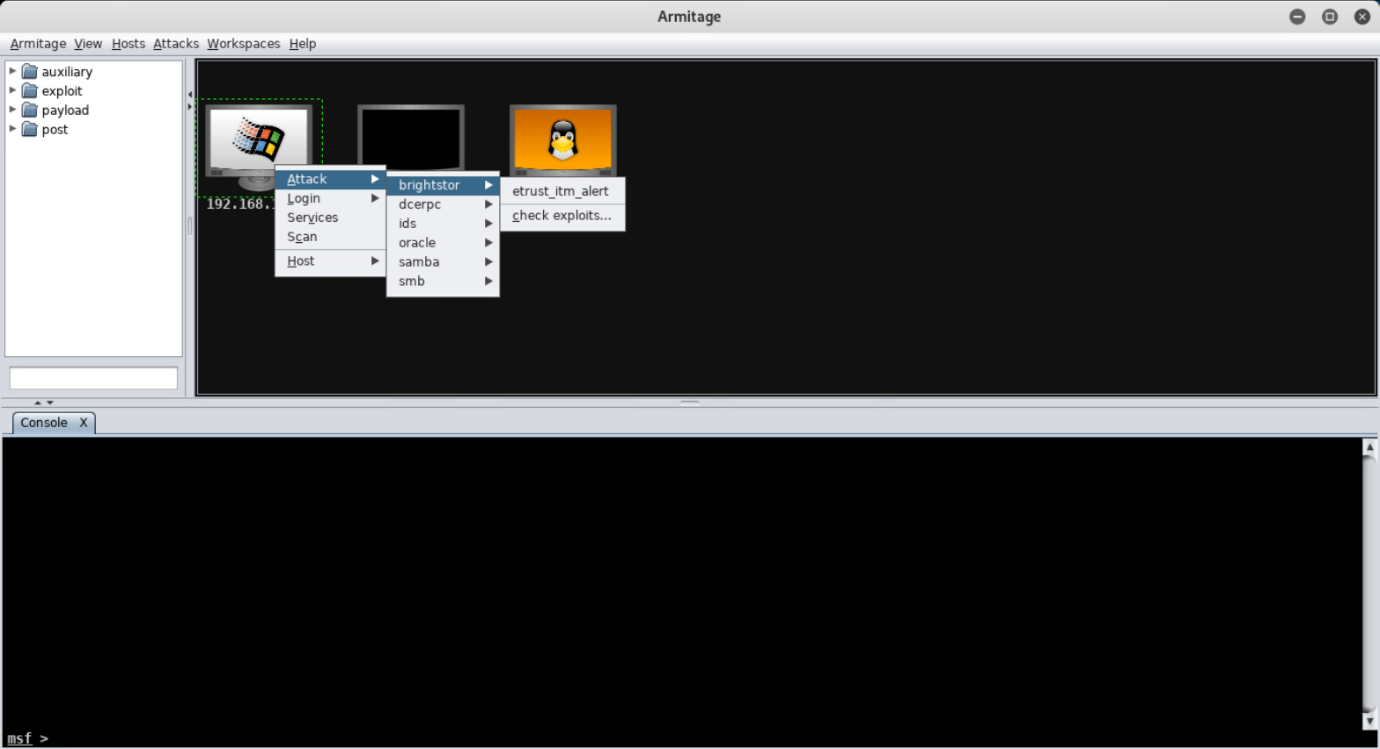
|  |  |  |  |
| --- | --- | --- | --- |
| **192.168.10.18 – Open Ports And Services** | | | |
| **Port** | **Protocol** | **Service** | **Version** |
| 21 | tcp | ftp | vsftpd 2.3.4 |
| 22 | tcp | ssh | OpenSSH 4.7 |
| 23 | tcp | telnet | Linux telnetd |
| 25 | tcp | smtp | Postfix smtpd |
| 53 | tcp | domain | ISC BIND 9.4.2 |
| 80 | tcp | http | Apache httpd 2.2.8 |
| 111 | tcp | rpcbind | 2 (RPC #100000) |
| 139 | tcp | netbios-ssn | Samba smbd 3.X – 4.X |
| 445 | tcp | netbios-ssn | Samba smbd 3.0.20 – Debian |
| 512 | tcp | exec | netkit-rsh rexecd |
| 513 | tcp | login | openBSD or Solaris rlogind |
| 514 | tcp | shell | Netkit rshd |
| 1099 | tcp | java-rmi | Java RMI Registry |
| 1524 | tcp | bindshell | Metasploitable root shell |
| 2049 | tcp | nfs | 2-4(RPC #100003) |
| 2121 | tcp | ftp | ProFTPD 1.3.1 |
| 3306 | tcp | mysql | MySQL 5.0.51a – 3ubuntu5 |
| 5432 | tcp | postgresql | PostgreSQL DB 8.3.0 – 8.3.7 |
| 5900 | tcp | vnc | VNC (protocol 3.3) |
| 6000 | tcp | X11 | Unknown |
| 6667 | tcp | irc | UnreallRCd |
| 8009 | tcp | ajp13 | Apache Jserv (Protocol v1.3) |
| 8180 | tcp | http | Apache Tomcat/Coyote JSP engine 1.1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **192.168.10.19 – Open Ports And Services** | | | |
| **Port** | **Protocol** | **Service** | **Version** |
| 135 | tcp | msrpc | vsftpd 2.3.4 |
| 139 | tcp | netbios-ssn | Microsoft Windows netbios-ssn (Unknown) |
| 445 | tcp | microsoft-ds | Windows XP microsoft-ds (Unknown) |
| 1025 | tcp | msrpc | Microsoft Windows RPC (Unknown) |
| 5000 | tcp | upnp | Unknown |

Another penetration testing tool was used by the name of Armitage to gather information on the 2 computers. Armitage will scan the network similarly to how Zenmap did and then we can make it “Find attacks” which will give us a list of potential attacks that we can use on the systems to attempt to gain access based on the services running on the systems, the operating systems they are using and the versions of these software packages.



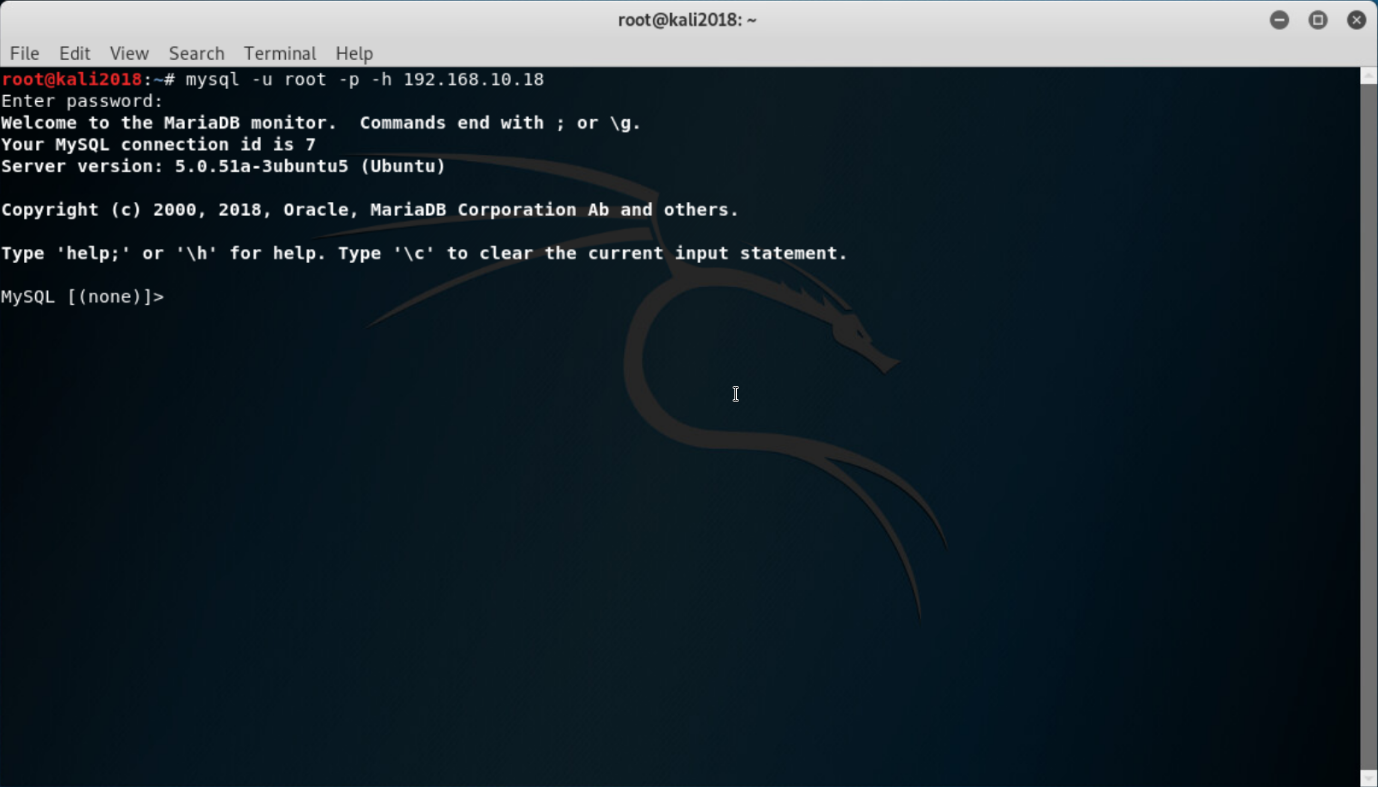




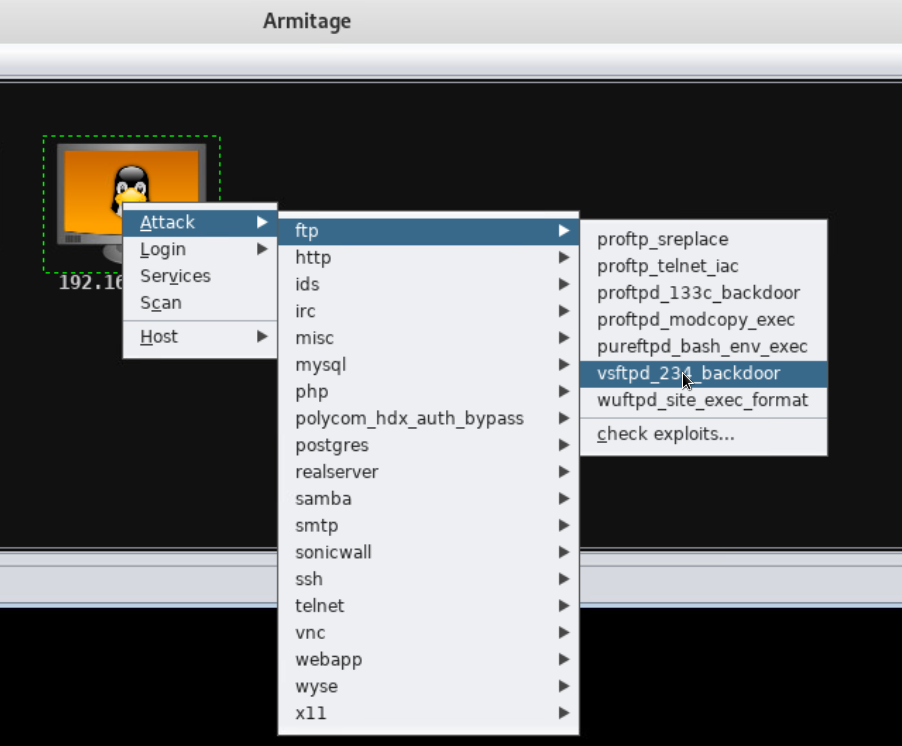
As you can see Armitage has found several attacks worth attempting on the Linux machine and much fewer on the Windows machine. When we attempt to gain access later, we will produce a table detailing which attacks were attempted and which failed or succeeded.

### Gaining access Stage:

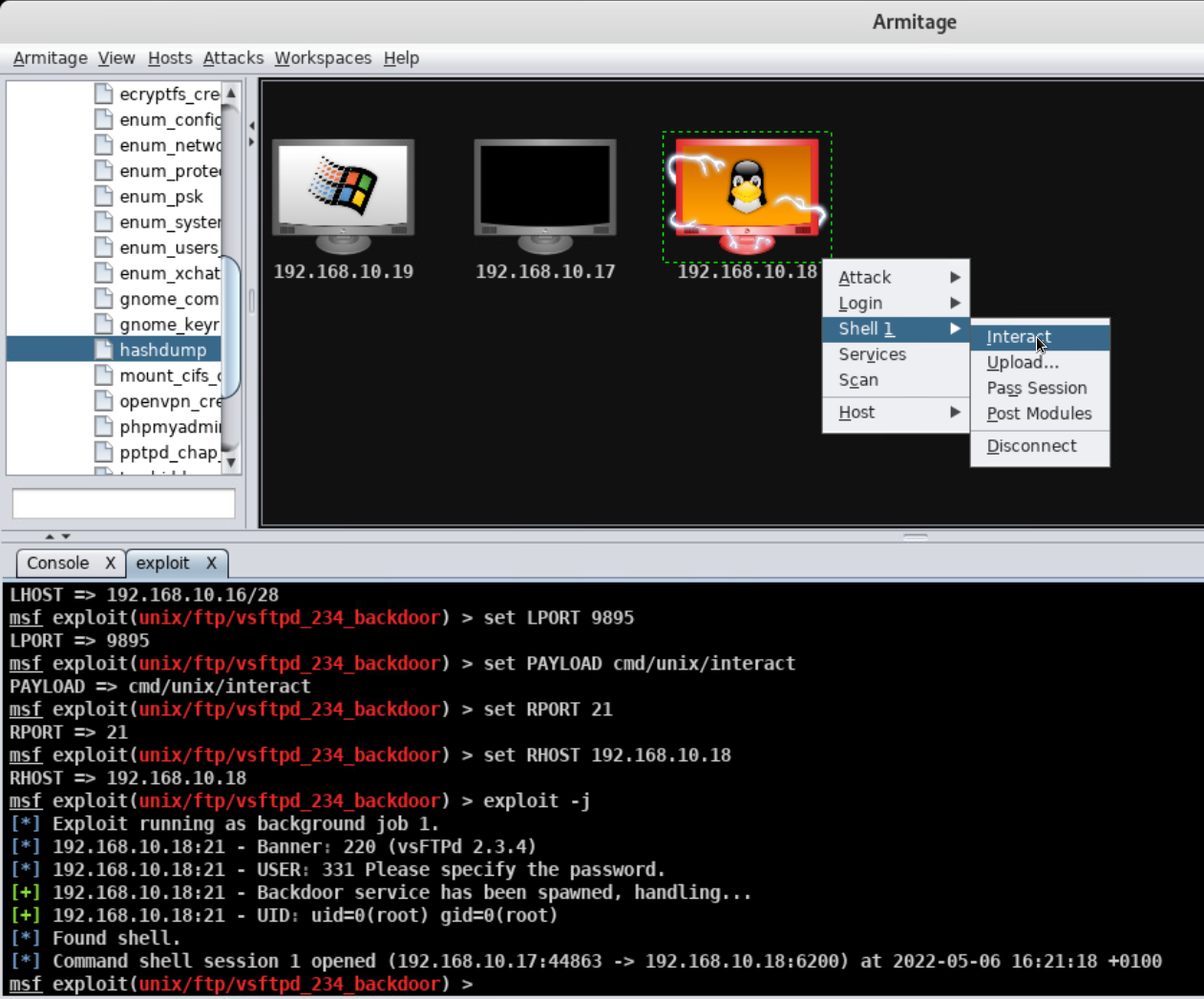
First, we will attempt to gain access to the Linux system (192.168.10.18). As we know there is a MySQL Server running from our Reconnaissance and there is a common mistake made when setting up the server where no password is set for the root user we can attempt to login as root without a password.



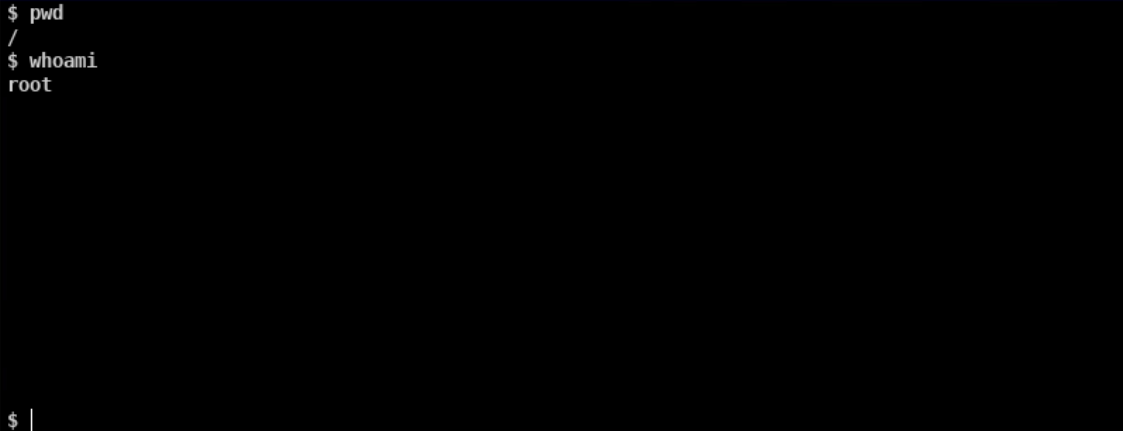
As you can see, we were successfully able to login without any password and as we are the root user, we are able to access, update and delete all records in the database. Moving back to Armitage we will use the ‘vsftpd\_234\_backdoor’ attack.



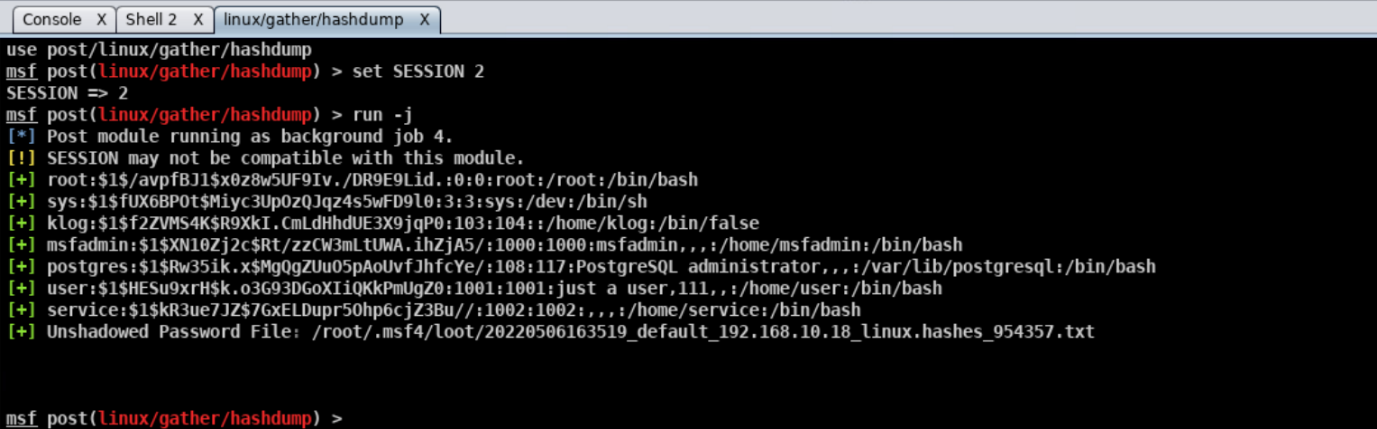
Our attack was successful, and we are now able to get a remote shell running on the target computer! Armitage adds lightning bolts around the target system as shown in the screenshot below to indicate that the exploit you have used has been successful.



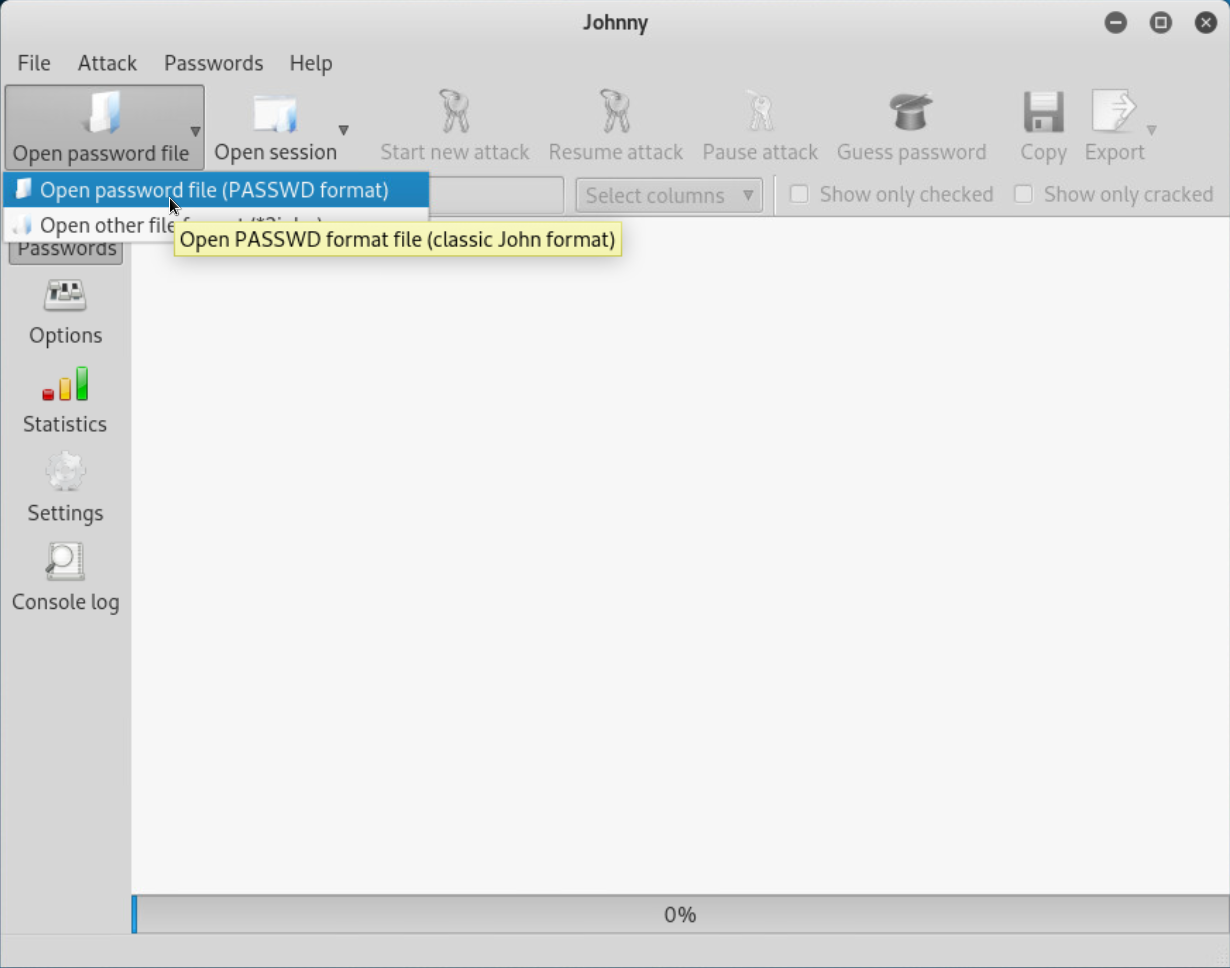
If we interact with the remote shell that was created and run a couple of commands we can easily discover that we are in root and logged in as the root user so have full access to the system.

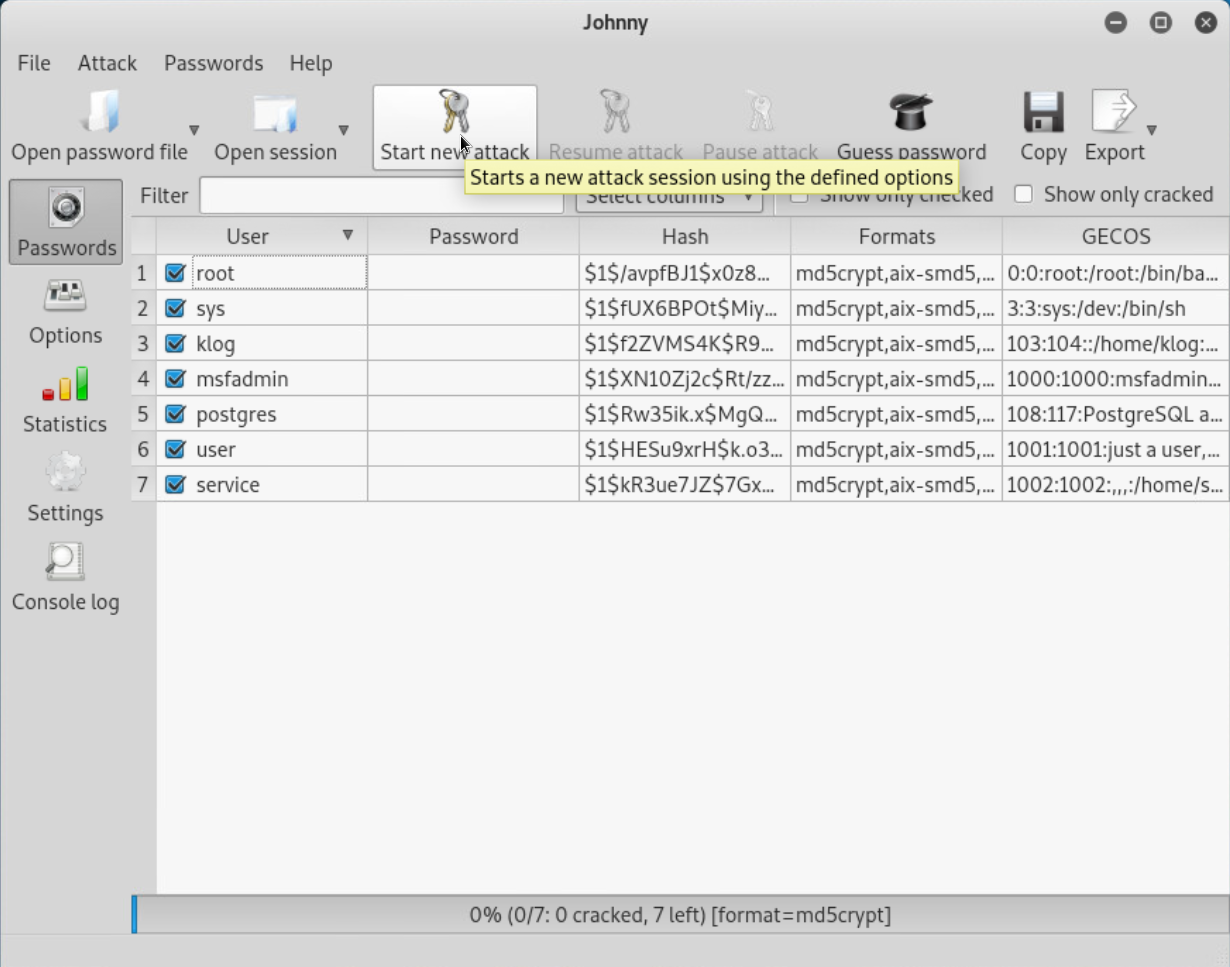


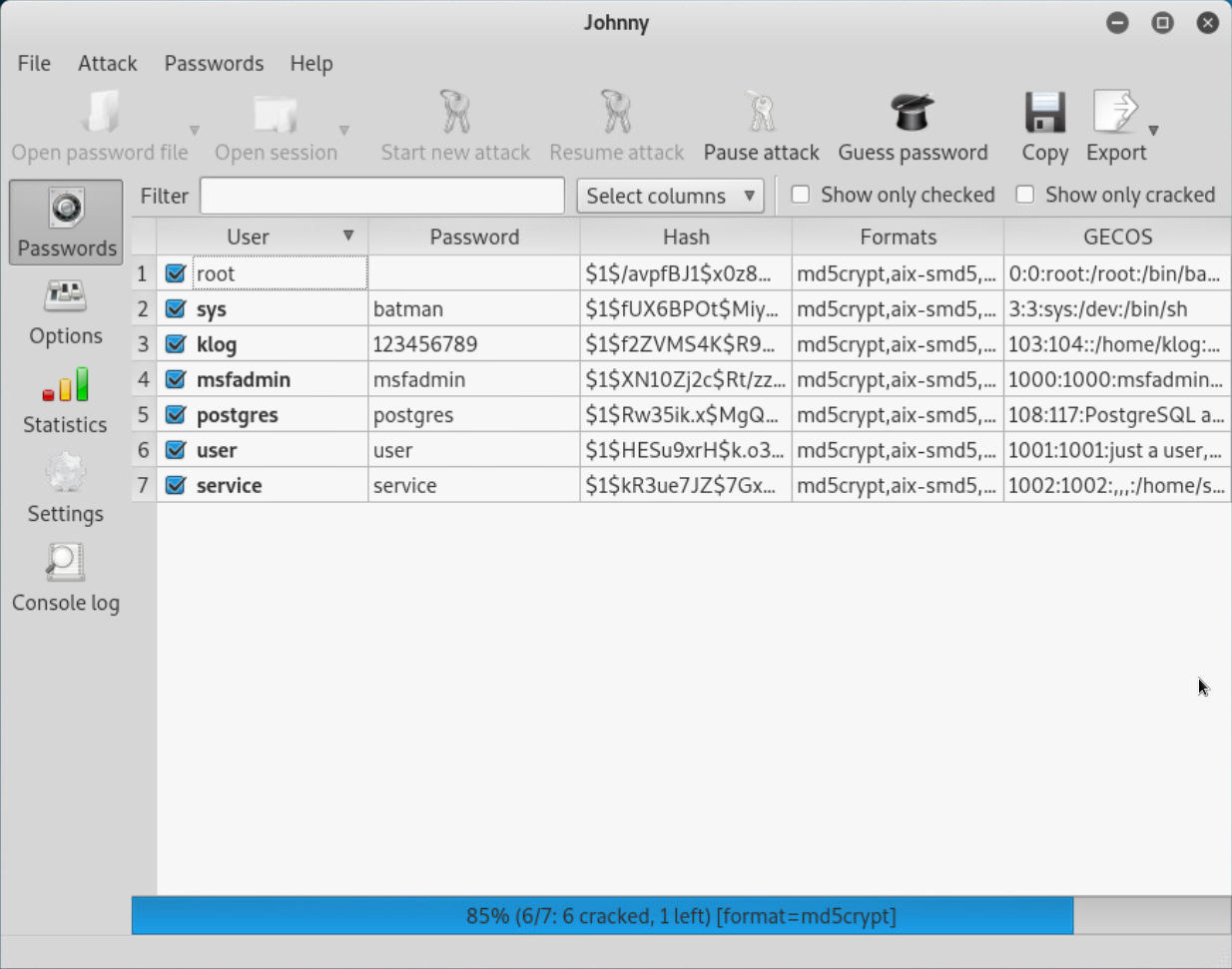
Something we can do using Armitage now that we have a remote shell is get a hashdump containing all the users and their encrypted passwords. It will create some new files in “/root/.msf4/loot” when we do this.



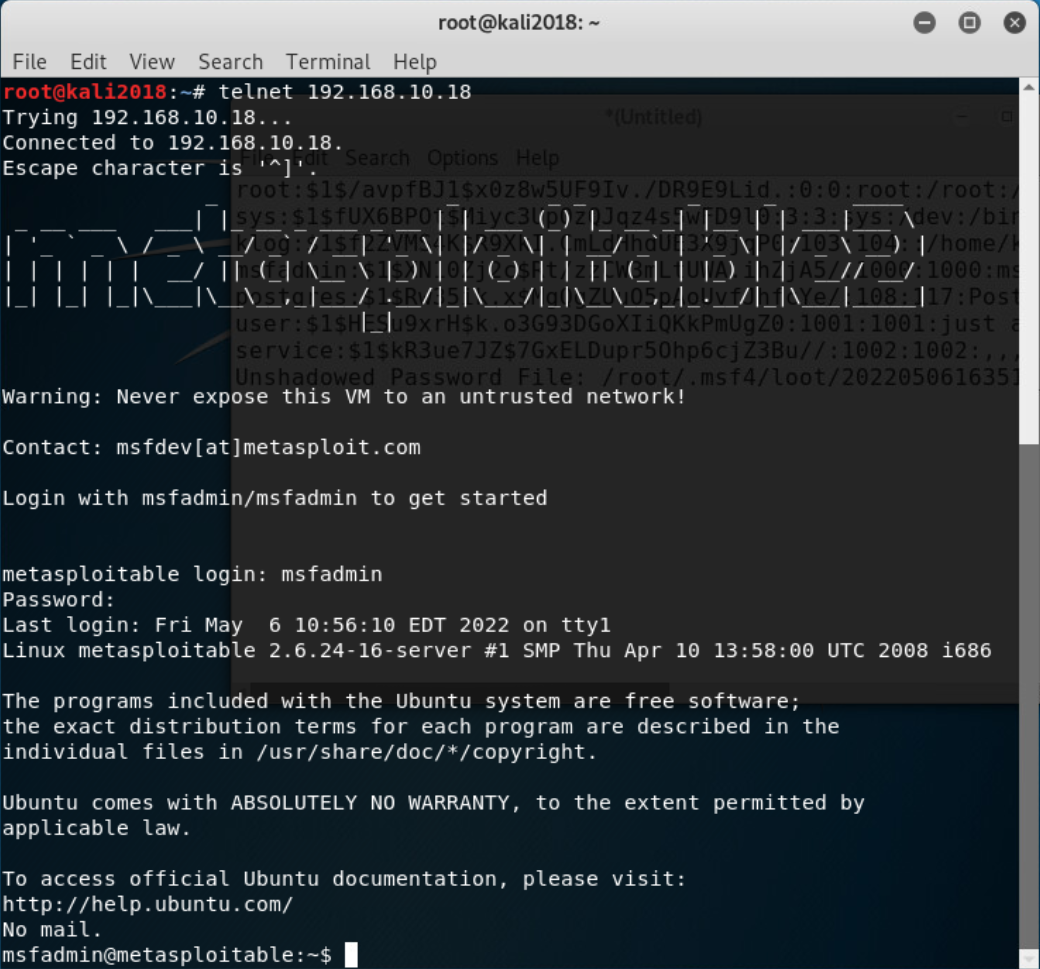
We can then use another program called Johnny to crack these hashed passwords by pointing it to the file that was created by Armitage in our case “/root/.msf4/loot/\*hashes\_954357.txt”







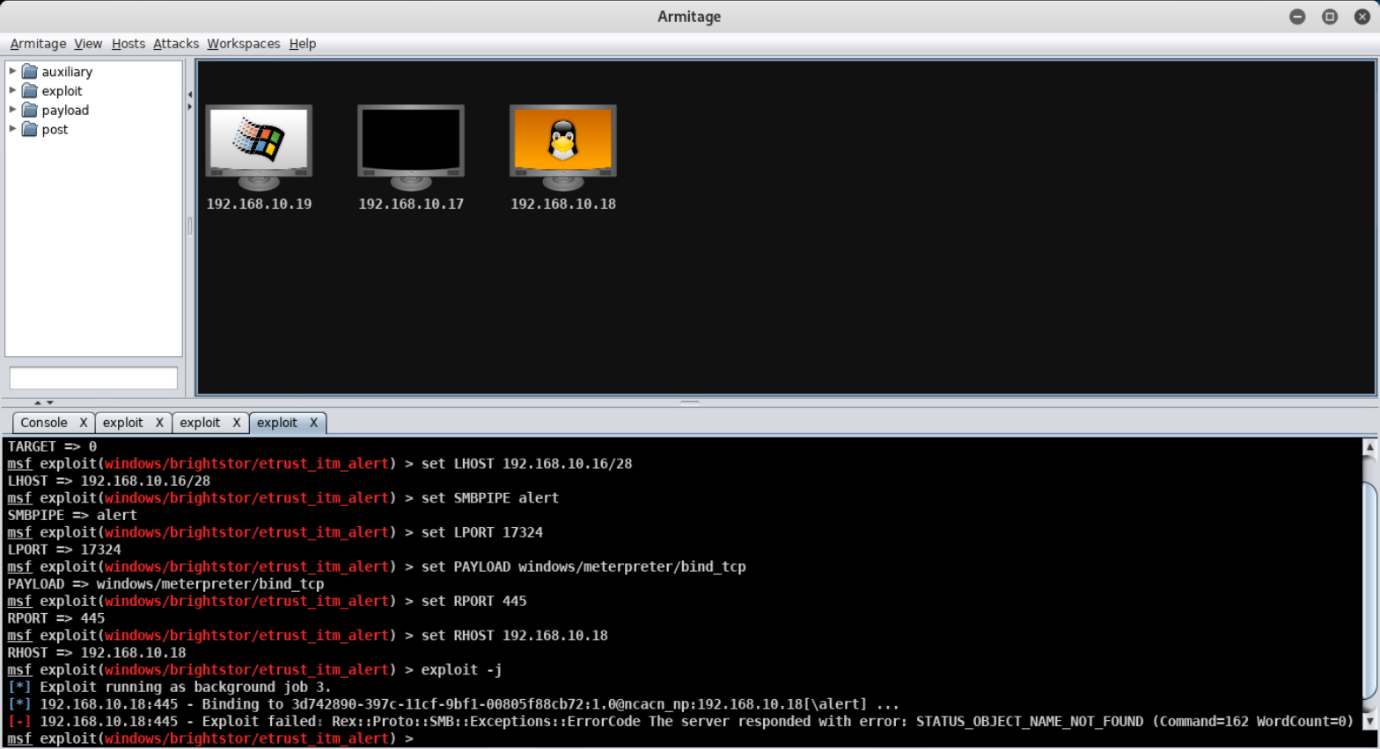
We were able to discover all but one of the passwords using Johnny. As the target system is running a telnet service, we should be able to get a remote shell by creating and logging into a telnet session with the target system as shown below.



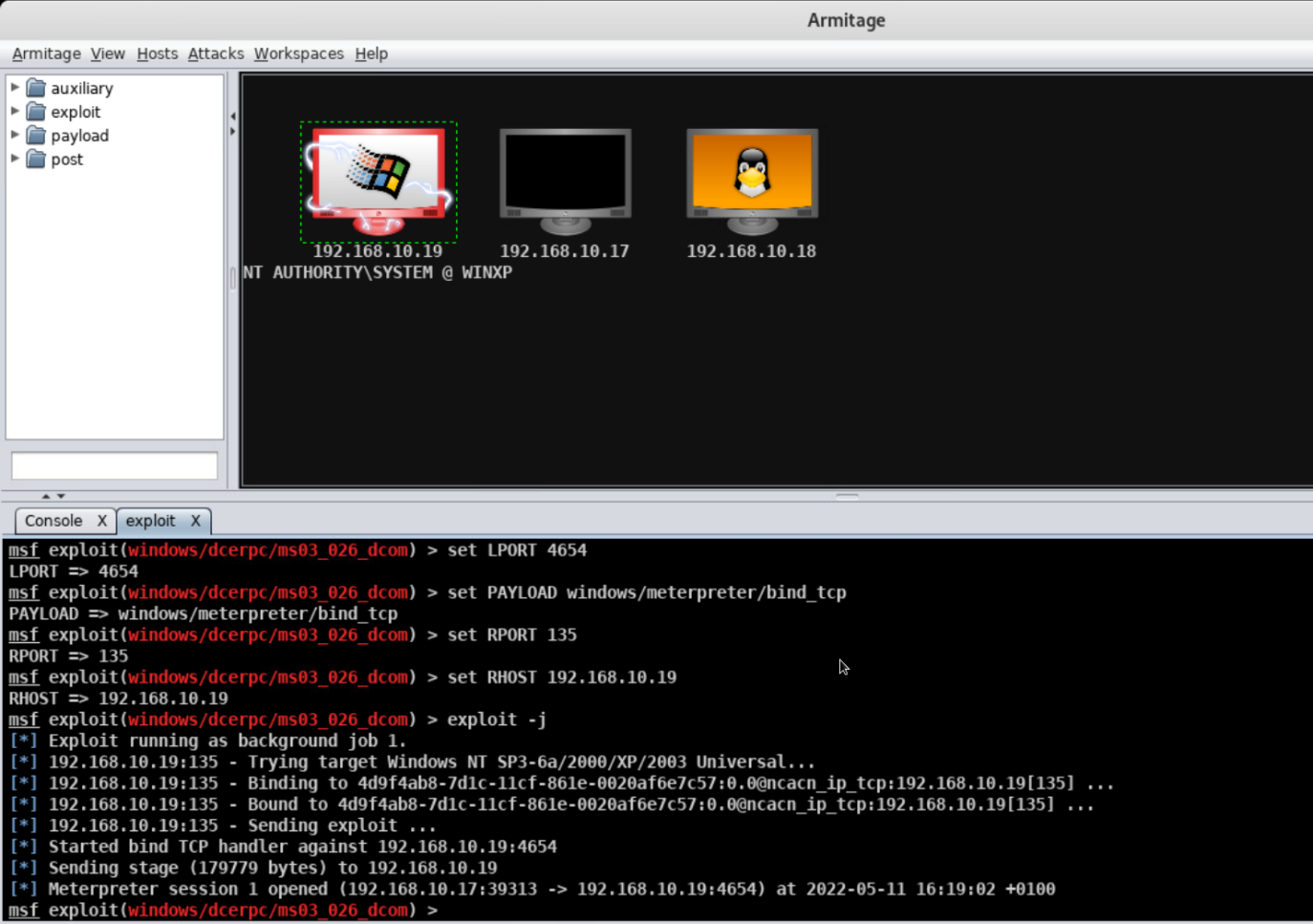
I will now for completeness include a table showing which attacks were successful when attempted on the Linux system.

|  |  |  |
| --- | --- | --- |
| **Target Name** | **Attack Name** | **Result** |
| ftp | vsftpd\_234\_backdoor | Exploit succeeded – gained backdoor shell |
| ftp | proftp\_sreplace | Exploit Failed. |
| ftp | proftp\_133c\_backdoor | Exploit Failed. |
| ftp | proftp\_modcopy\_exec | Exploit Failed. |
| ftp | proftp\_telnet\_iac | Exploit Failed. |
| ftp | pureftpd\_bash\_env\_exec | Exploit Failed. |
| ftp | wuftpd\_site\_exec\_format | Exploit Failed. |
| http | accellion\_fta\_getstatus\_oauth | Exploit Failed. |
| http | activecollab\_chat | Exploit Failed. |
| http | advantech\_switch\_bash\_env\_exec | Exploit Failed. |
| http | airties\_login\_cgi\_bof | Exploit Failed. |
| http | ajaxplorer\_checkinstall\_exec | Exploit Failed. |
| http | alcatel\_omnipcx\_mastercgi\_exec | Exploit Failed. |
| http | alienvault\_exec | Exploit Failed. |
| http | alienvault\_sqli\_exec | Exploit Failed. |
| http | apache\_mod\_cgi\_bash\_env\_exec | Exploit Failed. |
| http | apprain\_upload\_exec | Exploit Failed. |
| ids | snort\_dce\_rpc | Exploit succeeded – gained backdoor shell |
| irc | unreal\_ircd\_3281\_backdoor | Exploit succeeded – gained backdoor shell |
| mysql | mysql\_udf\_payload | Exploit Failed. |
| mysql | mysql\_yassl\_getname | Exploit Failed. |
| mysql | mysql\_yassl\_hello | Exploit Failed. |
| php | php\_unserialize\_zval\_cookie | Exploit Failed. |
| postgres | postgres\_createlang | Exploit Failed. |
| postgres | postgres\_payload | Exploit Failed. |
| samba | chain\_reply | Exploit Failed. |
| samba | is\_known\_pipename | Exploit Failed. |
| samba | lsa\_transnames\_heap | Exploit Failed. |
| samba | nttrans | Exploit Failed. |
| samba | setinfopolicy\_heap | Exploit Failed. |
| samba | trans2open | Exploit Failed. |
| samba | usermap\_script | Exploit Failed. |
| smtp | clamav\_milter\_blackhole | Exploit Failed. |
| smtp | exim4\_dovecot\_exec | Exploit Failed. |
| smtp | exim4\_string\_format | Exploit Failed. |
| smtp | exim\_gethostbyname\_bof | Exploit Failed. |
| smtp | qmail\_bash\_env\_exec | Exploit Failed. |
| ssh | array\_vxag\_vapv\_privkey\_privesc | Exploit Failed. |
| ssh | ceragon\_fibeair\_known\_privkey | Exploit Failed. |
| ssh | exagrid\_known\_privkey | Exploit Failed. |
| ssh | f5\_bigip\_known\_privkey | Exploit Failed. |
| ssh | loadbalanceorg\_enterprise\_known\_privkey | Exploit Failed. |
| ssh | mercurial\_ssh\_exec | Exploit Failed. |
| ssh | quantum\_dxi\_known\_privkey | Exploit Failed. |
| ssh | quantum\_vmpro\_backdoor | Exploit Failed. |
| ssh | sshexec | Exploit Failed. |
| ssh | symantec\_smg\_ssh | Exploit Failed. |
| telnet | netgear\_telnetenable | Exploit Failed. |
| telnet | telnet\_encrypt\_keyid | Exploit Failed. |
| vnc | vnc\_keyboard\_exec | Exploit Failed. |
| webapp | actualanalyzer\_ant\_cookie\_exec | Exploit Failed. |
| webapp | arkeia\_upload\_exec | Exploit Failed. |
| webapp | awstats\_configdir\_exec | Exploit Failed. |
| webapp | awstats\_migrate\_exec | Exploit Failed. |
| webapp | awstatstotals\_multisort | Exploit Failed. |
| webapp | barracuda\_img\_exec | Exploit Failed. |
| webapp | base\_qry\_common | Exploit Failed. |
| webapp | basilic\_diff\_exec | Exploit Failed. |
| webapp | cacti\_graphimage\_exec | Exploit Failed. |
| webapp | cakephp\_cache\_corruption | Exploit Failed. |
| wyse | hagent\_untrusted\_hsdata | Exploit Failed. |
| x11 | x11\_keyboard\_exec | Exploit Failed. |

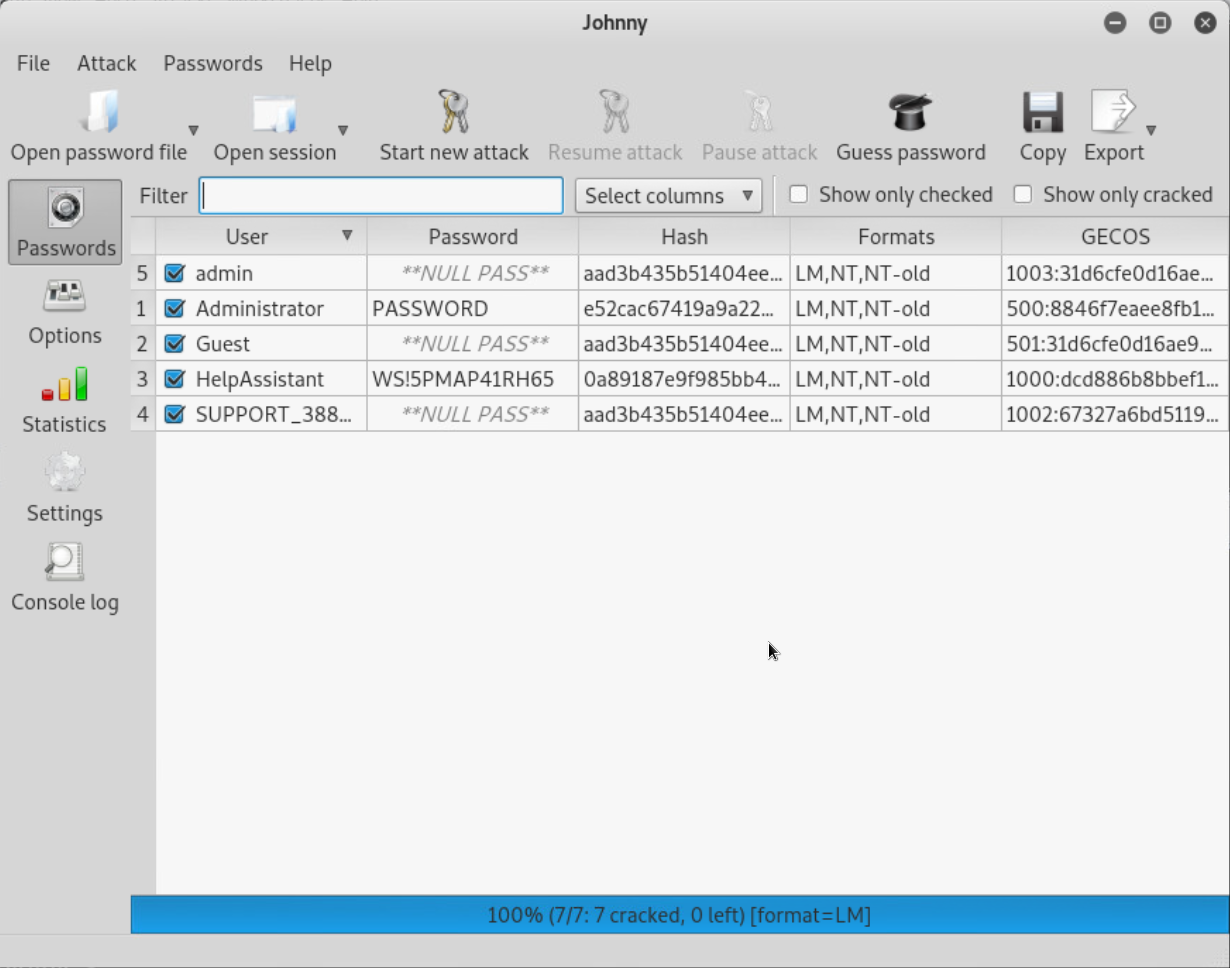
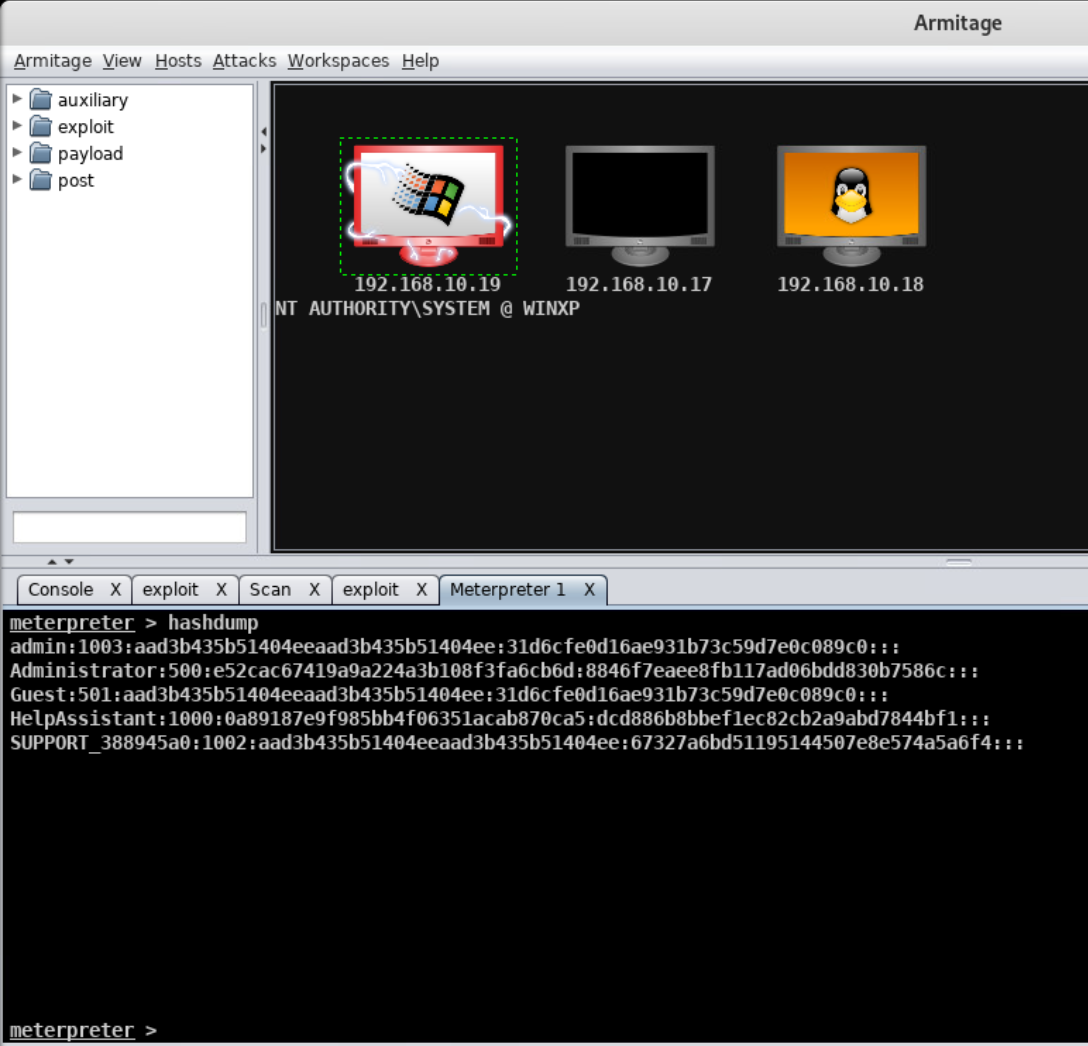
We will now move onto the Microsoft XP System. As the XP system has significantly less ports open and services running it will likely be more difficult to exploit. We will start by attempting the first exploit in the list which is an attack on brightstor called etrust\_itm\_alert:



As you can see that attack was unsuccessful so we will try the next exploit in the list which is an attack on dcerpc called ms03\_026\_dcom:



This time we have been successful and have gained a Meterpreter shell into the windows system which will allow us to run commands on the target machine. The command *hashdump* will give us all the hashed passwords on the System which we can run through johnny to get the passwords of the users as we did on the Linux machine.



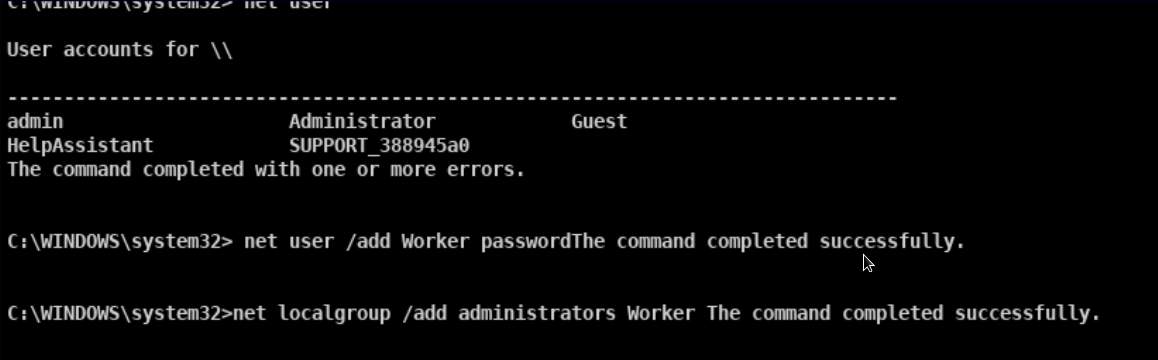
As the windows system doesn’t have telnet running (or any remote desktop services) we are unable to use these stolen passwords to gain access. However, because we have access through a shell we could theoretically install one and then be able to login using the stolen credentials.

As I did with the Linux system I will include a table showing which attacks were successful when attempted on the windows system.

|  |  |  |
| --- | --- | --- |
| **Target Name** | **Attack Name** | **Result** |
| brightstor | etrust\_itm\_alert | Exploit failed. |
| dcerpc | ms03\_026\_dcom | Exploit succeeded – meterpreter shell session opened on target. |
| ids | snort\_dce\_rpc | Exploit failed. |
| oracle | extjob | Exploit failed. |
| samba | nttrans | Exploit failed. |
| samba | usermap\_script | Exploit failed. |
| smb | Ipass\_pipe\_exec | Exploit failed. |
| smb | Ms03\_049\_netapi | Exploit failed. |
| smb | Ms04\_007\_killbill | Exploit succeeded – meterpreter shell session opened on target. |
| smb | Ms04\_011\_lsass | Exploit failed. |
| smb | Ms04\_031\_netdde | Exploit failed. |
| smb | Ms05\_039\_pnp | Exploit failed. |
| smb | Ms06\_025\_rras | Exploit failed. |
| smb | Ms06\_025\_rasmans\_reg | Exploit failed. |
| smb | Ms06\_040\_netapi | Exploit failed. |
| smb | Ms06\_066\_nwapi | Exploit failed. |

### Maintaining Access Stage:

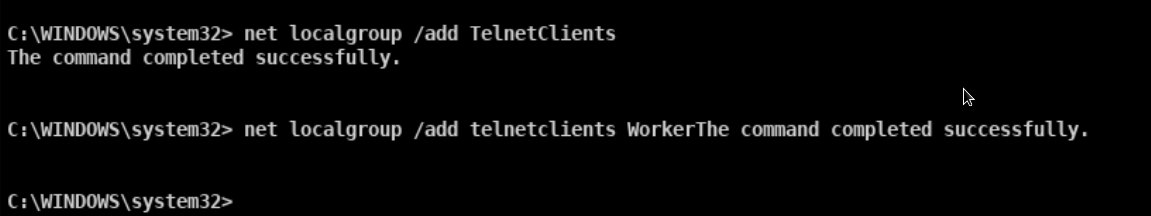
There is no guarantee that the exploits we are using will continue to work so we will be attempting to create user accounts on both systems we have compromised and elevating them to admin accounts. We will start with the windows system by opening a shell to it through Armitage and running a couple of commands to create a user and make them an administrator.

But we still have no way of accessing the system as there are no services running that allow remotely logging in. Windows XP has telnet installed by default, but it must be disabled so we will just start it and set it to auto start when the computer starts with the 2 following command.

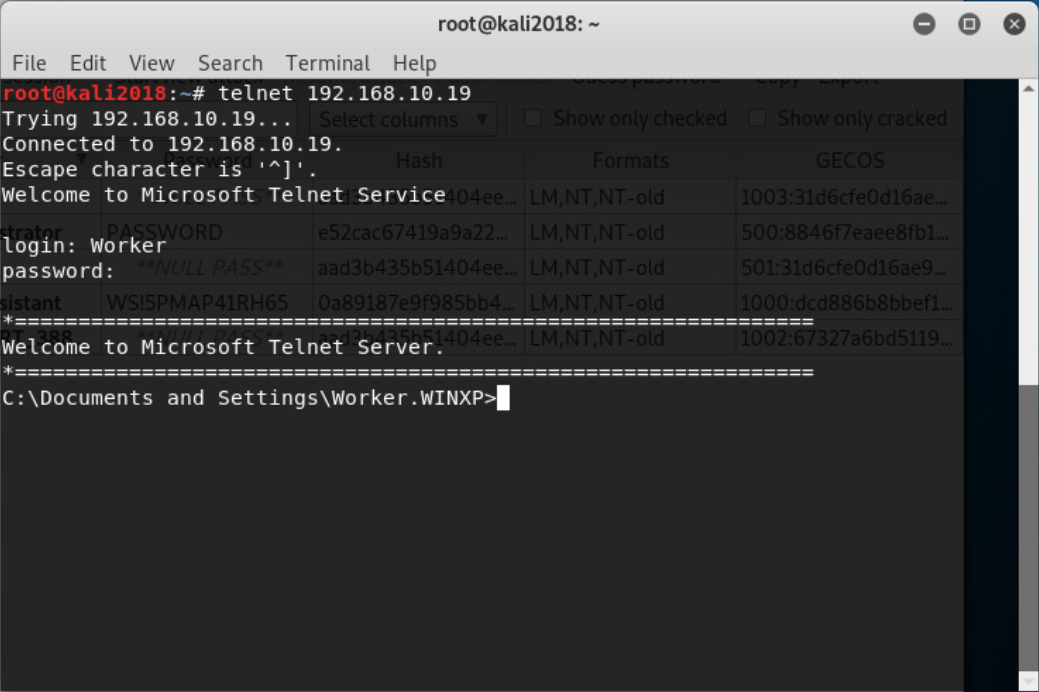
Text

Description automatically generated

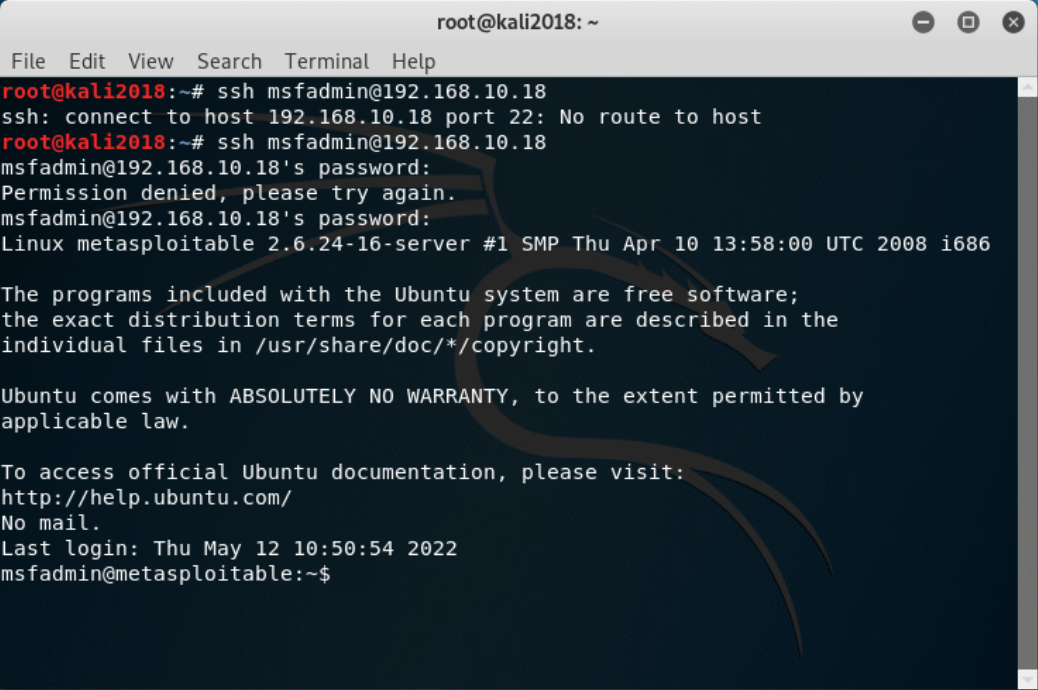
Finally, we need to create a group called and add our newly created user to it in order for telnet to allow us to login as this user.

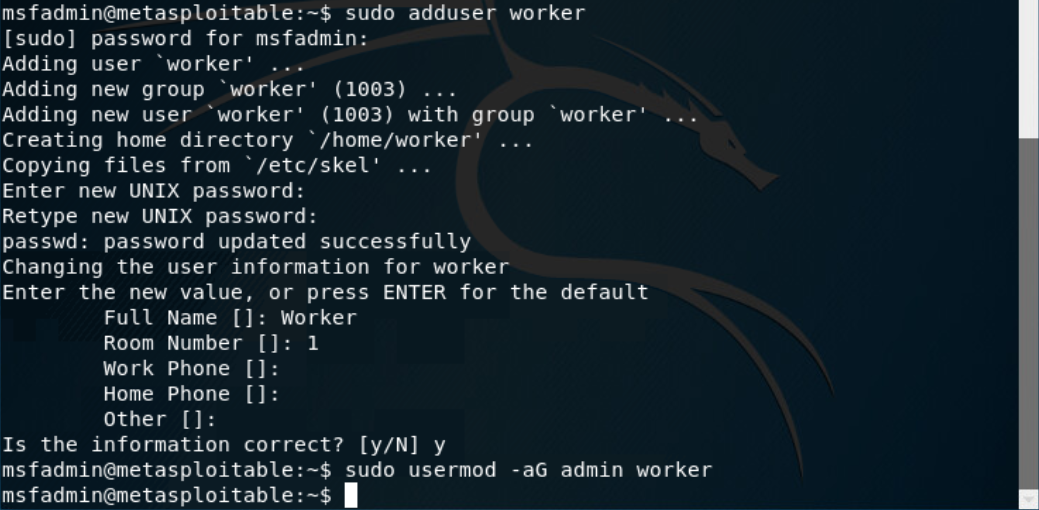


We are now able to telnet into the account from a terminal without the need for exploits and have administrator level permissions.

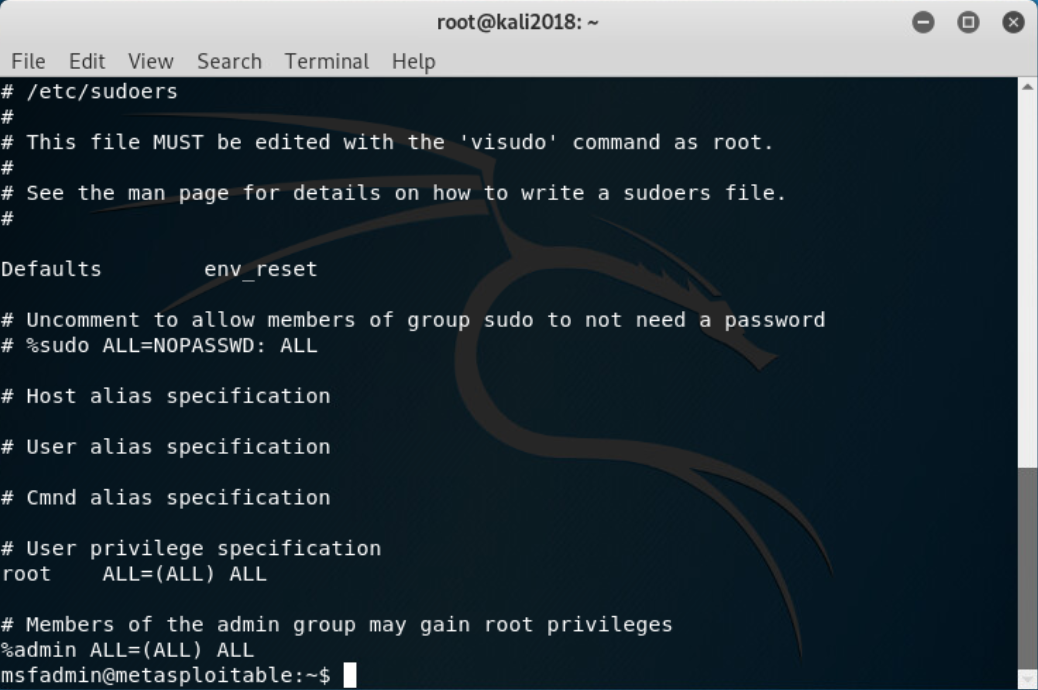


Now we will move onto the Linux system. With the Linux system we will use some stolen credentials to get a ssh connection and use the shell it provides to run a couple of commands which will create a new user and add them to the administrator group.



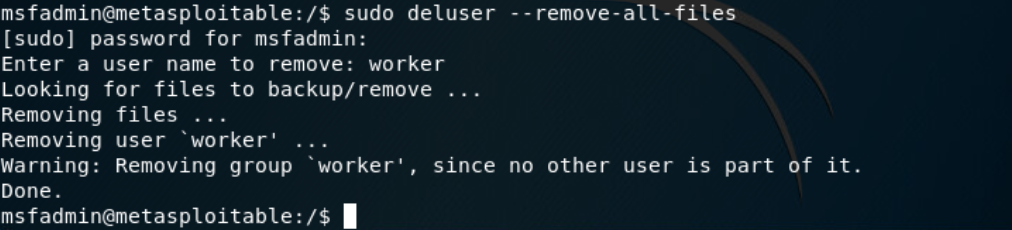


We have now created a user account which we can log into remotely that is able to use sudo to act as root. We can show that users which are part of the admin group can use the sudo command by printing /etc/sudoers to the console using cat or less.

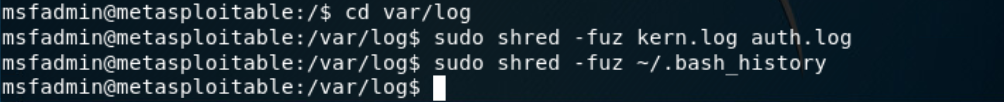


### Covering Tracks Stage:

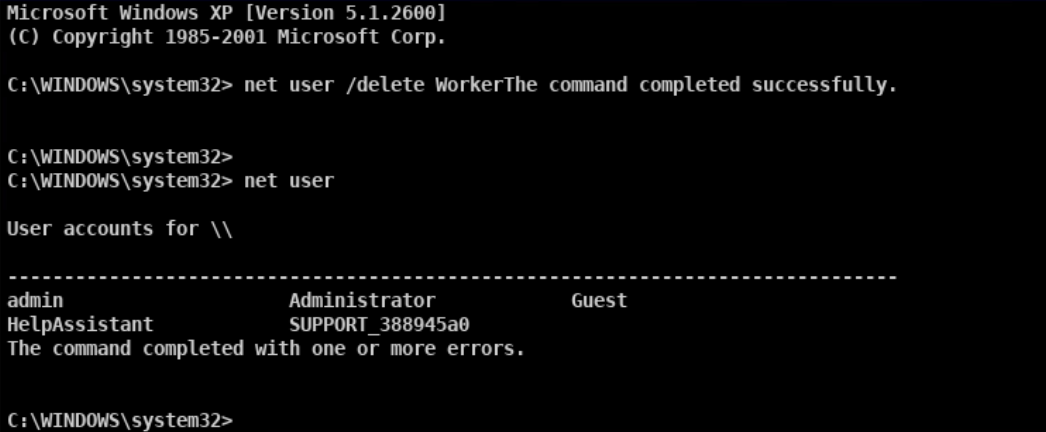
We will begin by removing the account we created on the Linux system, ensuring that all related files are destroyed with the following command run in a ssh session logged in as msfadmin.



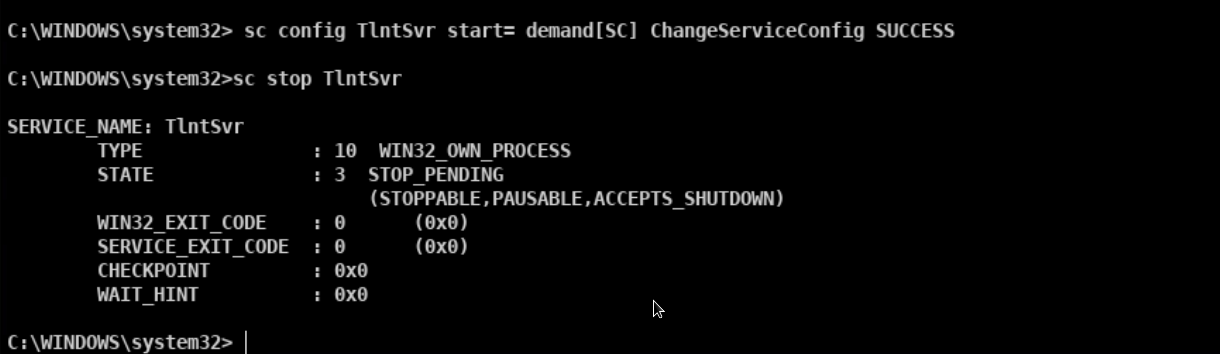
Now we will use the shred command to delete and overwrite the history of bash commands as well as the authentication and kernal logs to hide our activity.



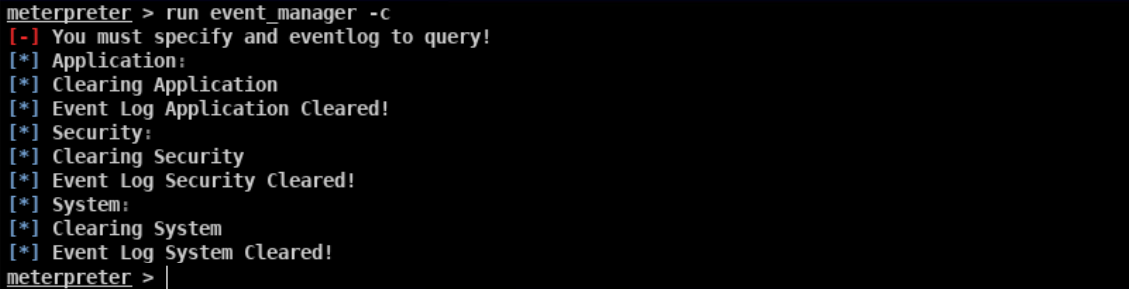
Now we will move onto the windows system which will mostly be the same, we will start by removing the user we created in a windows command prompt spawned by Meterpreter.



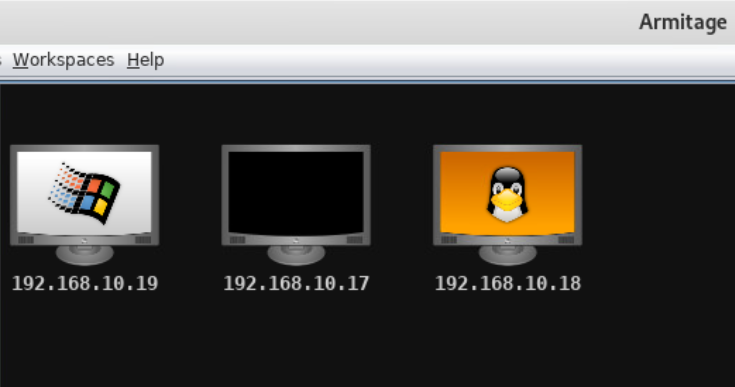
Next, we need to disable telnet from auto starting and stop the service running.



Now we will open a Meterpreter shell and run the next command to clear the application, system and security logs to hide our activity.



Finally, we can close the remote shells we had to both target machines leaving us with no exploited machines in Armitage.



### Implement Countermeasures Stage:

1. **Windows System**
   1. The operating system being used on this computer is very old and has not been receiving security updates for quite some time and so changing to a newer operating system would significantly increase security.
   2. A password policy should be put in place as 3 accounts had no password, and the Administrator account had a very weak password that could quite easily be guessed.
2. **Linux System**
   1. There are many open ports on the system, these should be carefully audited and any ports that do not need to be open should be closed.
   2. There are a lot of services running on the system, any services not being used or not required should be removed.
   3. Password strength on most of the accounts was very poor and would be quite vulnerable to a basic dictionary attack so a password policy should be put in place to ensure staff members are using good passwords.
   4. The operating system should be updated or replaced with a newer version as Linux v2.6.33 is now over 10 years old and so naturally has significant security holes due to the length of time people have had to discover them.
3. **Both Systems**
   1. 2 Factor Authentication could be put in place to make it much more difficult for an attacker to gain access to the systems.
   2. All software installed on the systems should be updated to the latest versions available.
   3. Staff should be trained to keep the software up to date and log any suspicious activity on the network or systems they are using.
   4. A firewall should be enabled with all ports closed and then the ports can be manually opened when and where it is necessary.

### Report conclusions and recommendations:

Both systems had very outdated operating systems, both systems had several outdated services running with known exploits which could be used to gain access to the systems and modify them in any way the attacker might choose to, both systems had poorly chosen passwords which could be guessed or easily cracked with a dictionary attack, and the linux system had a lot of services running which may no longer be required but have been left installed and running.

My recommendation would be to update and/or replace the operating systems on both the computers to the latest versions possible, enable/enforce a password policy which requires passwords to be cryptographically strong up to an industry standard, enable 2 factor authentication if possible to add another security layer, audit the services running and the ports open on both systems and only keep those running and open which are required, update services, drivers and all software and ensure that these are kept up to date at regular intervals, and finally put in place a firewall on both systems that only allows traffic in and out of those systems where and when it is required.

# APPENDIX 1:

# Penetration Test Agreement

This agreement is made as of 26/04/2022 By and between: Calum Lindsay, located in CalHack Inc, Yell, Shetland ZE2 9BB; hereafter referred to as ‘Calum Lindsay’ and Trilogy Europe, located in London; represented by James Amstel, hereafter referred to as the ‘customer’.

With regard to the Penetration Test, the customer hereby acknowledges and agrees:

1. That Calum Lindsay will perform a Penetration Test — which will consist of a partially automated test that will attempt to remotely identify security vulnerabilities and/or any software misconfiguration — on one or more computer systems owned and/or operated by the customer.
2. That the customer has the legal right to subject the designated computer system to the aforementioned Penetration Test and that if it is not the owner of the computer system it has obtained such right from the legal owner of the system.
3. Not to hold Calum Lindsay liable for any indirect, special, incidental, or consequential damage, which will include but not be limited to loss of business, revenue, profits, use, or data, however it may arise.
4. That it has the sole responsibility for adequate protection and backup of data and/or equipment used in connection with this Penetration Test and will not make a claim against Calum Lindsay for lost data, backup restoration time, inaccurate output, work delays or lost profits resulting from the Penetration Test.
5. That Calum Lindsay will not divulge any information about the customer's network it received as a result of this Penetration Test. All results are confidential and belong to the customer.
6. That it should recognise that the results of this test will provide a reasonably accurate view of the current security level of the tested computer system(s), Calum Lindsay can not be held responsible if the Penetration Test fails to discover certain security or configuration issues on the target computer system(s).
7. The customer’s systems will respond in a normal fashion when they detect the Penetration Test in its firewall logs, alert systems, etc as it would do in the case of a real security penetration; this is so that it will not distort the results of the test. However, the customer agrees not to notify legal or public authorities of this penetration.
8. That Calum Lindsay will use any security vulnerabilities found to attempt to gain access and create a new user account with administrator permissions on the devices where the vulnerabilities are found.
9. That Calum Lindsay will attempt to cover up and/or delete any evidence of their actions on the network.
10. That Calum Lindsay will not use any form of social engineering during the course of the penetration test.
11. That Calum Lindsay will perform an internal investigation only and no penetration attempts will be made by Calum Lindsay from outside of the network being investigated.
12. That Calum Lindsay will not test WiFi security on any devices owned by the customer.

The customer requests Calum Lindsay to perform the Penetration Test on the following IP address(es) under the aforementioned conditions:

All devices in the network 192.168.10.1/28 which includes any devices with the IP addresses listed below:

* 192.168.10.17
* 192.168.10.18
* 192.168.10.19
* 192.168.10.20
* 192.168.10.21
* 192.168.10.22
* 192.168.10.23
* 192.168.10.24
* 192.168.10.25
* 192.168.10.26
* 192.168.10.27
* 192.168.10.28
* 192.168.10.29
* 192.168.10.30

Calum Lindsay will inform the customer of the Penetration Test originating IP address.

Calum Lindsay\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed for and on behalf of Calum Lindsay

J Amstel\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed for and on behalf of the customer. Company legally binding signature required.

1. Note: the lecturer contact number and email may not be used to contest a mark. Please see the latest version of the UHI academic regulations <https://www.uhi.ac.uk/en/about-uhi/governance/policies-and-regulations/regulations> for more information. [↑](#footnote-ref-1)