COMPANY NAME :XYZ

SECURITY PEN TESTING

PRASHANTH M EDGE

SECURITY TESTING ESSENTAILS

SECTION :CSC 570

SUMMARY:

This report consists of penetration testing performed on XYZ company.For the following lab we used certain terms and concepts in order to perform the actions which are required.

Nmap – Nmap is a free program that can be used in Linux, Mac, or Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open.

Armitage – Metasploit is a very powerful exploitation framework but it requires that the user be comfortable using the command line. Armitage is a GUI frontend for Metasploit that has many powerful capabilities.

This report also includes

1 – Extracting Information from the Database Using SQL Injection

2 – Making the Poison Ivy Payload

3 – Using the xp\_cmd shell to upload and launch a Malicious Payload

An SQL backend is attached to an Internet facing web server, an attacker may be able to gain access to the internal network through SQL injection if the application is unsecure.

SQL Injection – This is a technique by which attackers will use code, which includes SQL commands, to manipulate a web front end into revealing database information.

Hackers can exploit weaknesses in computer systems when vulnerabilities exist. An individual responsible for the network security of a company will need to patch systems that have vulnerabilities. It is also a best practice for a network administrator to shut down any unnecessary services that are running on their systems. If systems are not maintained or properly secured, hackers can take advantage of them. After a hacker breaks into a remote system, they will take steps to entrench themselves by creating accounts, stealing credentials, and exfiltrating data from the network

RISK RATINGS

The risk rating is based on the PTES (Penetration Testing Execution Standard) risk rating recommendation for reporting.

1. [USING ARMITAGE TO ATTACK THE NETWORK](https://bb.uis.edu/bbcswebdav/pid-914737-dt-content-rid-5766041_1/xid-5766041_1)

Network  [susceptibility](http://thesaurus.yourdictionary.com/susceptibility)

Rating – 8(Medium) :This rating is based on the network reaction upon the webdav attack and how it easily gives away the information to the attacker when he tries to control it remotely.

Remedation :My suggestion on this is to make the network more strong by not giving away the information.By keeping it more secure by certain strong network firewalls and not making it easy for the hacker to pass by the odds and get into the network and grab all the information.

1. SQL INJECTION:

URL Vulnerability

Rating – 12 (Extreme) : This rating is based on the vulnerabilty of the website https:216.1.1.1 to attacks and the manner in which it is taken control of.

Remedation :My suggestion is to use more stored procedures than using single sql commands which makes the hacker easy t crack them.The logic is very easy and the hacker might be very clever and take it forward and make changes to the current one.

.

**Discoveries Made:**

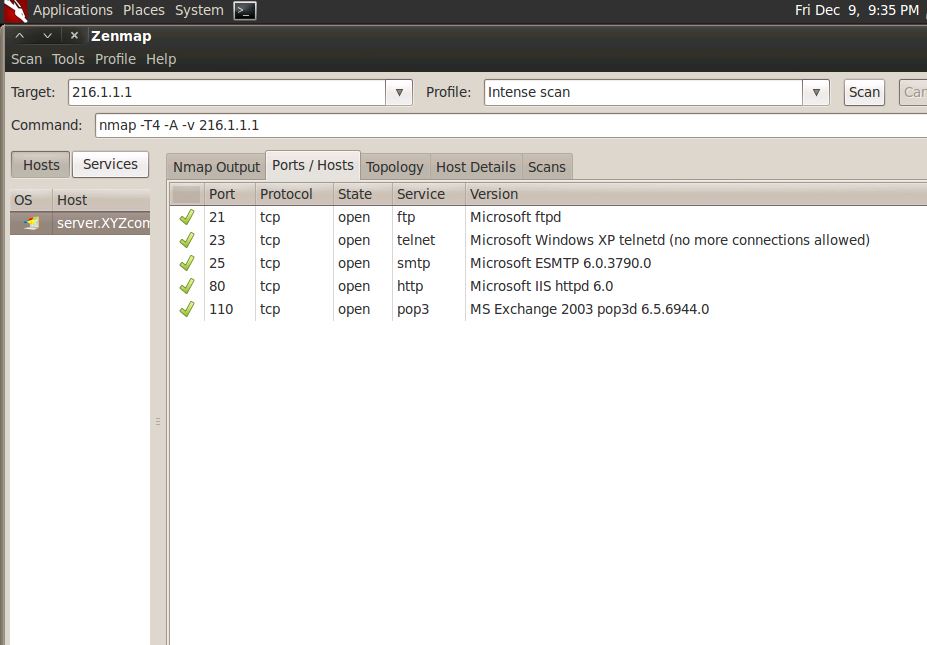
1. [USING ARMITAGE TO ATTACK THE NETWORK](https://bb.uis.edu/bbcswebdav/pid-914737-dt-content-rid-5766041_1/xid-5766041_1)



In the above screenshot, we have opened the zenmap after going into the terminal of the Backtrack 5 using the following command:

root@bt:~#zenmap : This command opens the Zenmap GUI front-end for Nmap.

STEP-2

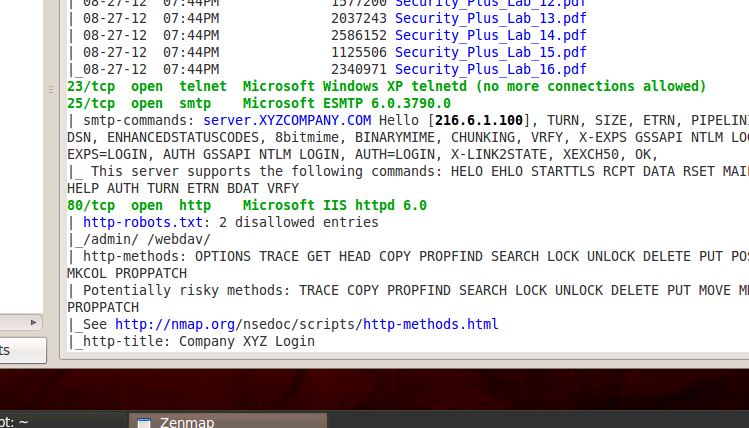


After opening the Zenmap, inside the Target box we need to give the public IP address 216.1.1.1 of XYZ company.

Then click the Ports/Hosts tab where all the 5 ports have opened.  
The following are the ports in the Zenmap:

21 File Transfer Protocol (FTP)   
• 23 TELNET  
• 25 Simple Mail transfer Protocol (SMTP)   
• 80 Hyper Text Transfer Protocol (HTTP)   
• 110 Post Office Protocol

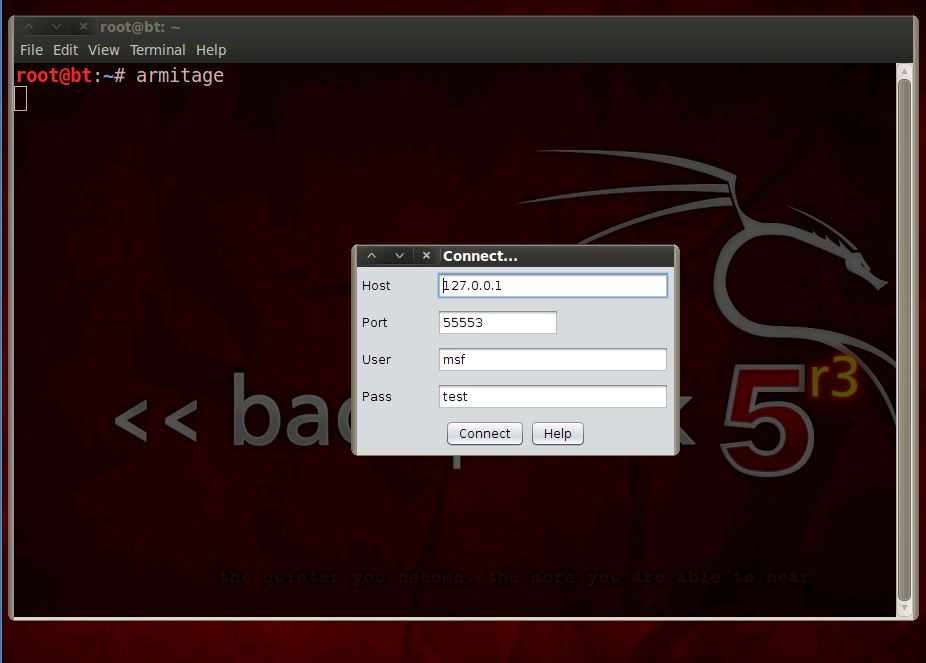
STEP-3



We scrolled down to the 80/tcp in the Nmap output tab to examine the robots.txt file which restricts the directory locations that web roots can reverse.

The above screenshot contains the information about robots.txt file.

STEP-4

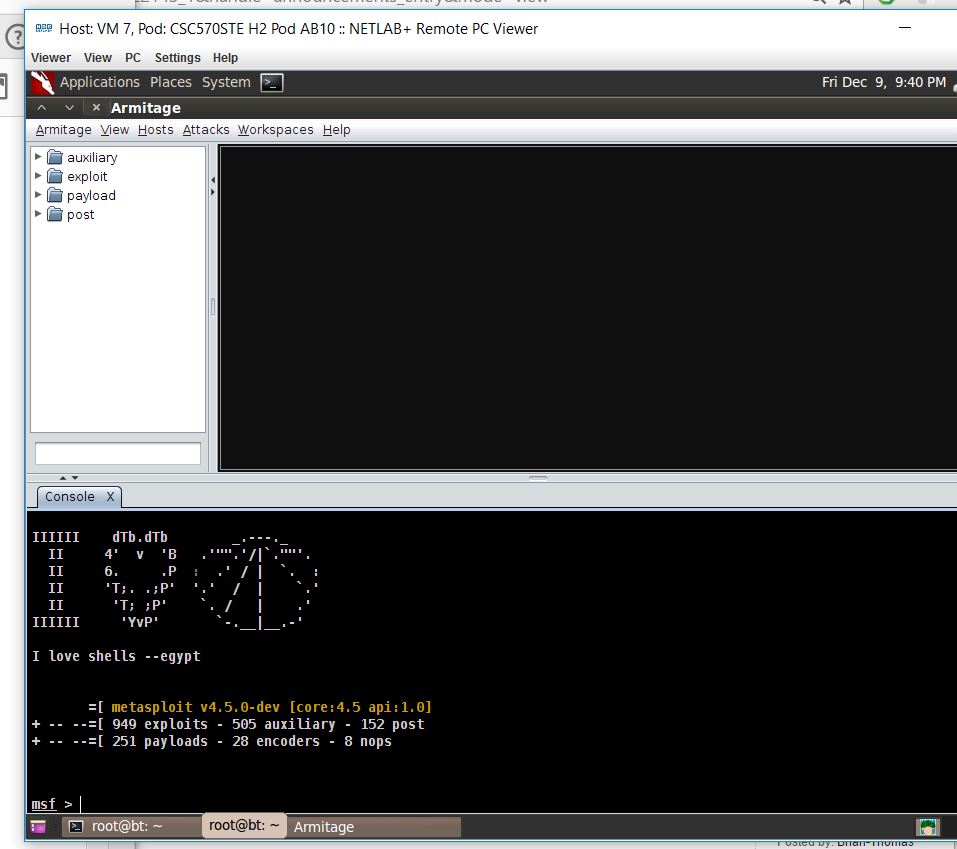


After closing the Zenmap without saving the changes, launch the Armitage using the following command:

root@bt:~# Armitage

In the screenshot, we need to connect to the localhost with username as “msf” and password as “test”.

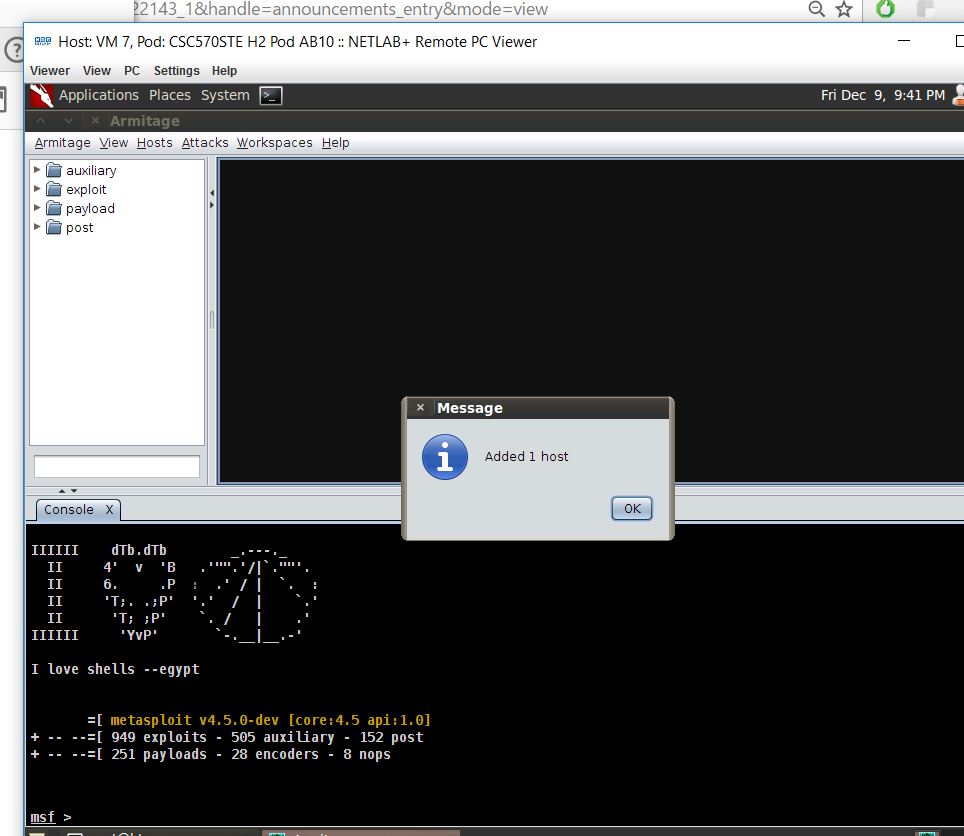
STEP-5



After starting the Metasploit’s Remote Procedure Call (RPC) Server, connect to the Java where initially we get an error which needs to be rectified.

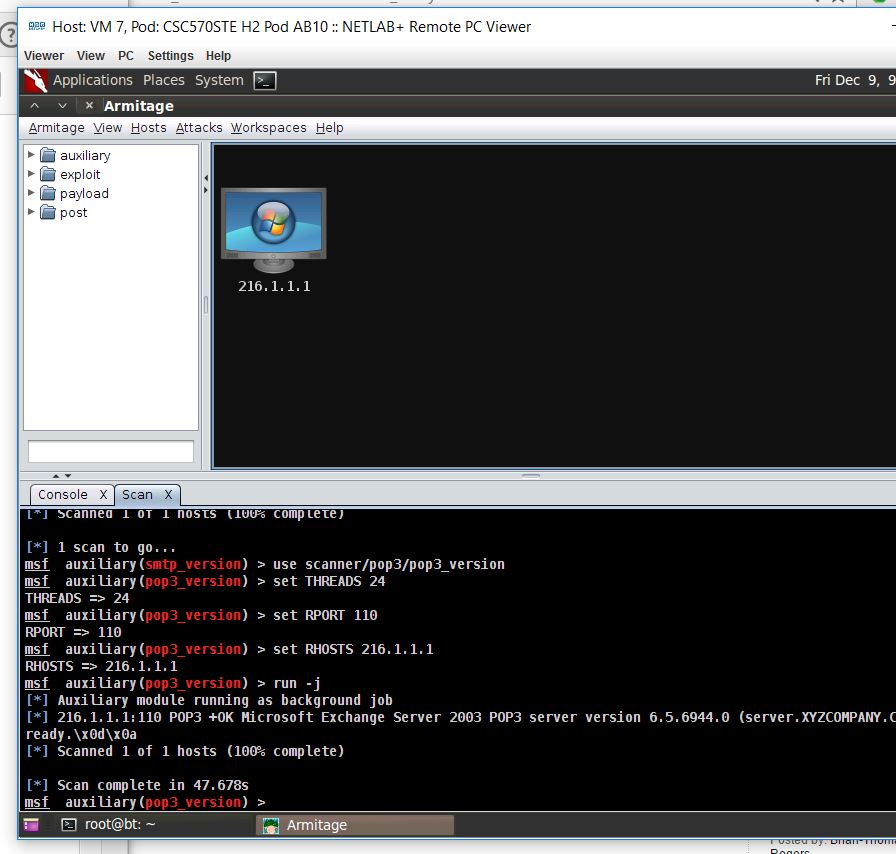
The Armitage windows will open, with the Metasploit Console on the bottom left.

STEP- 6



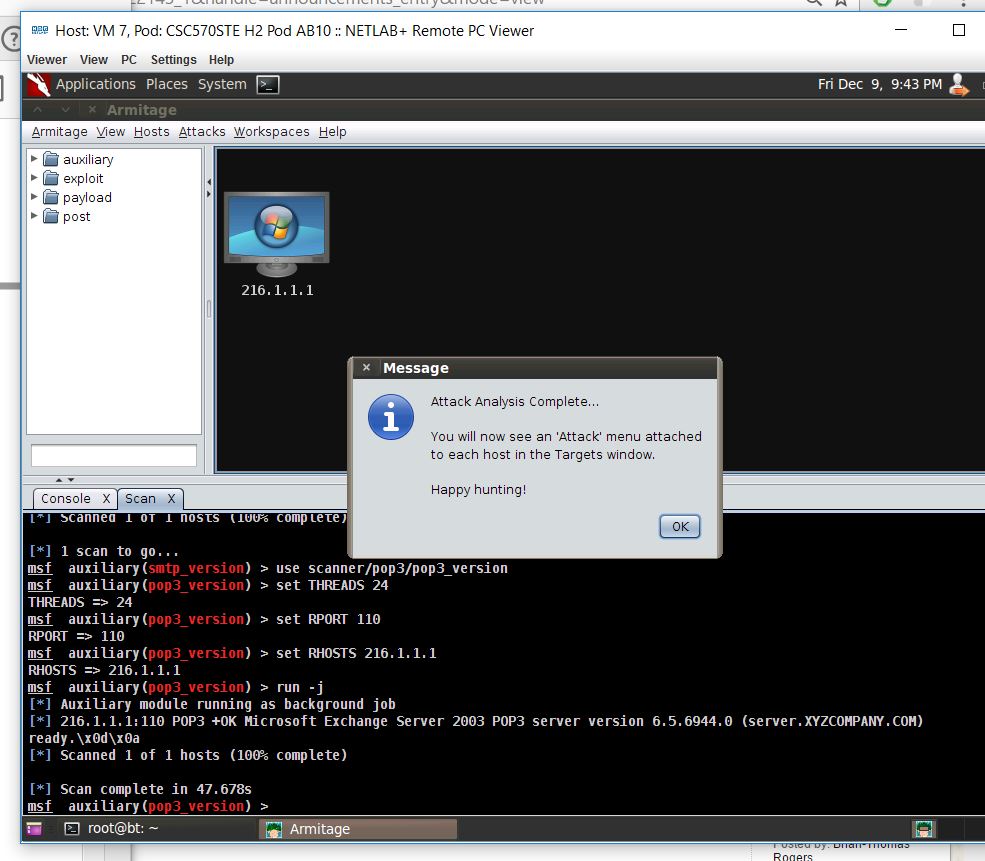
Now in the Armitage menu bar we need to select Hosts, and then select Add hosts. We added the host in the box by typing 216.1.1.1, the Public IP address of XYZ Company.  
Finally 1 host has been added in the Armitage.

STEP-7



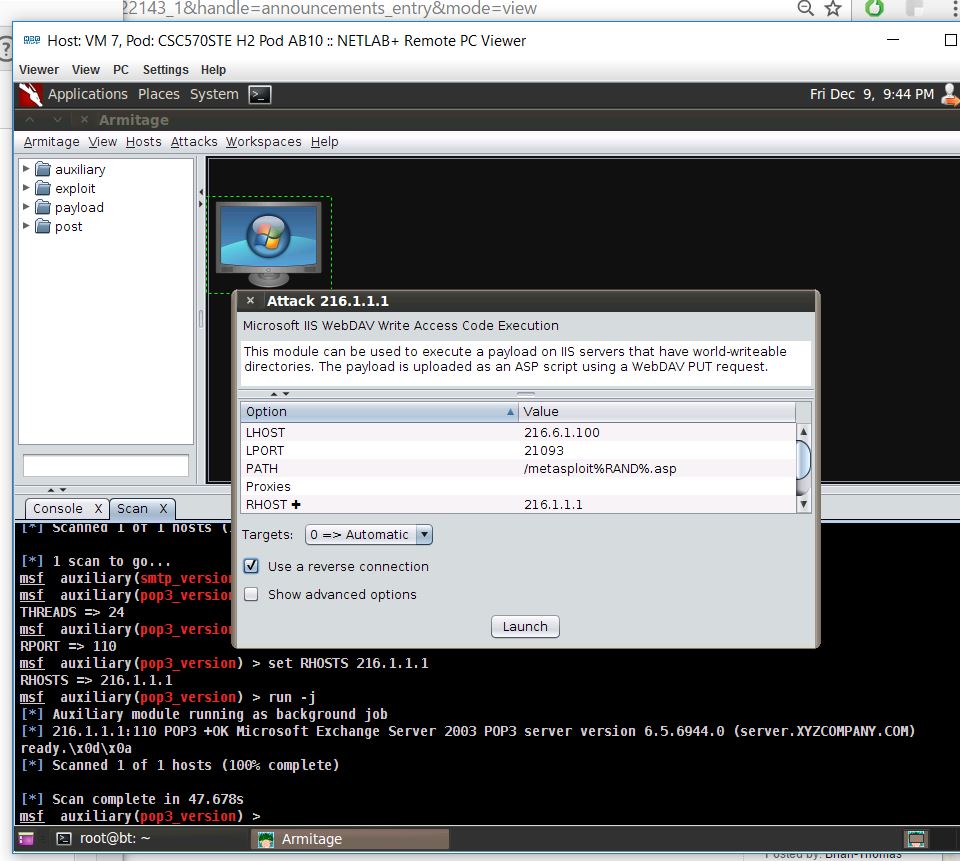
Right-click on host 216.1.1.1, and select Scan from the list of menu choices. The black screen changes to a Microsoft Windows emblem. The version is not identified.

STEP-8



From the Armitage menu bar, select Attacks and then Find Attacks.

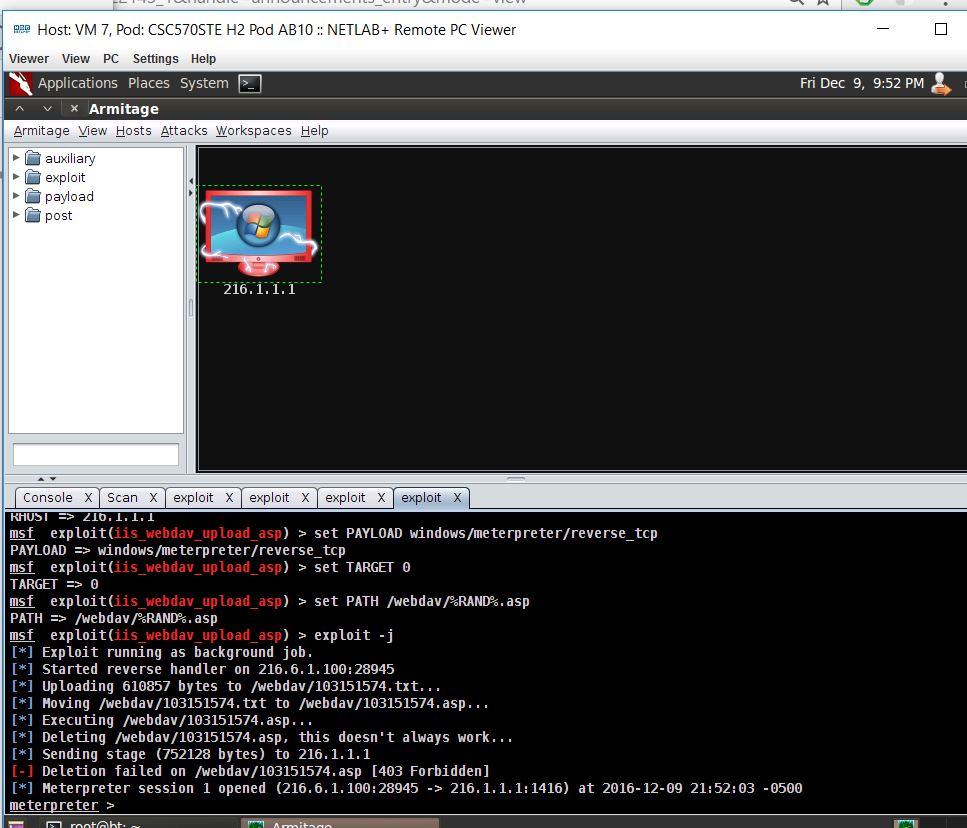
STEP-9



In this screenshot you can the the launch of the exploit by the following actions

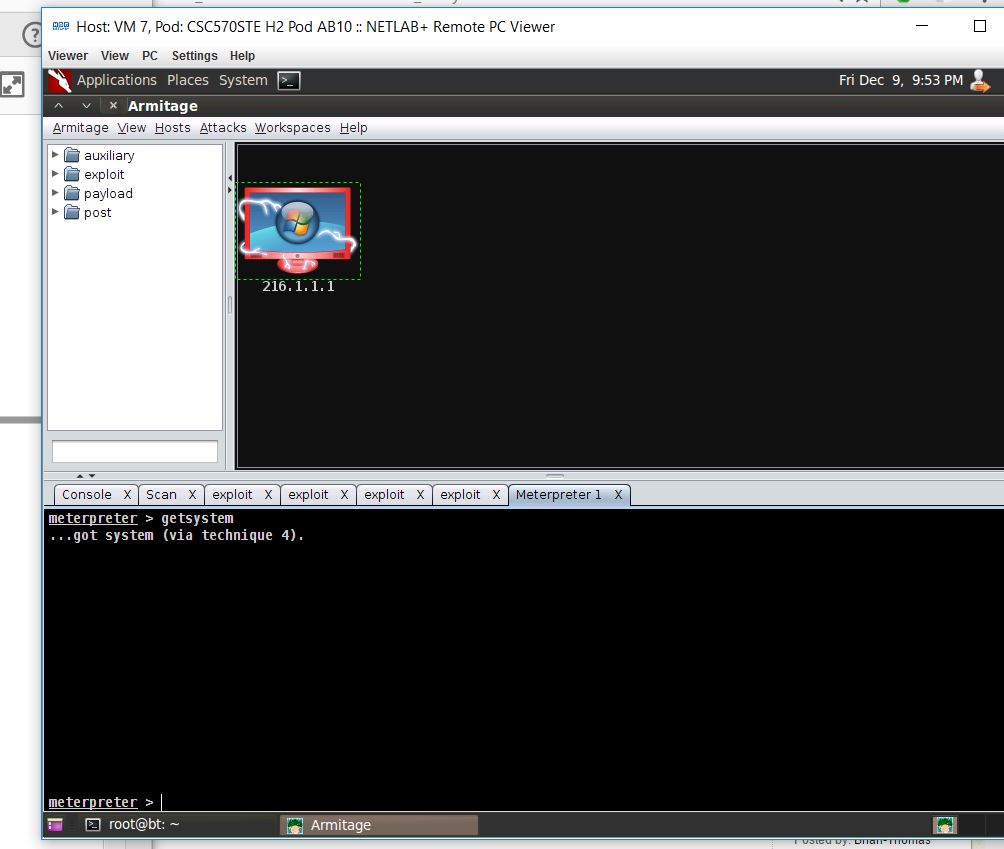
Right-click on 216.1.1.1 and select Attack, then select IIS from the menu, and then select iis\_webdav\_upload\_asp.  
Double-click in the PATH field and change the path to /webdav/%RAND%.asp. Check the box under target that states Use a reverse connection and click Launch.

STEP-10



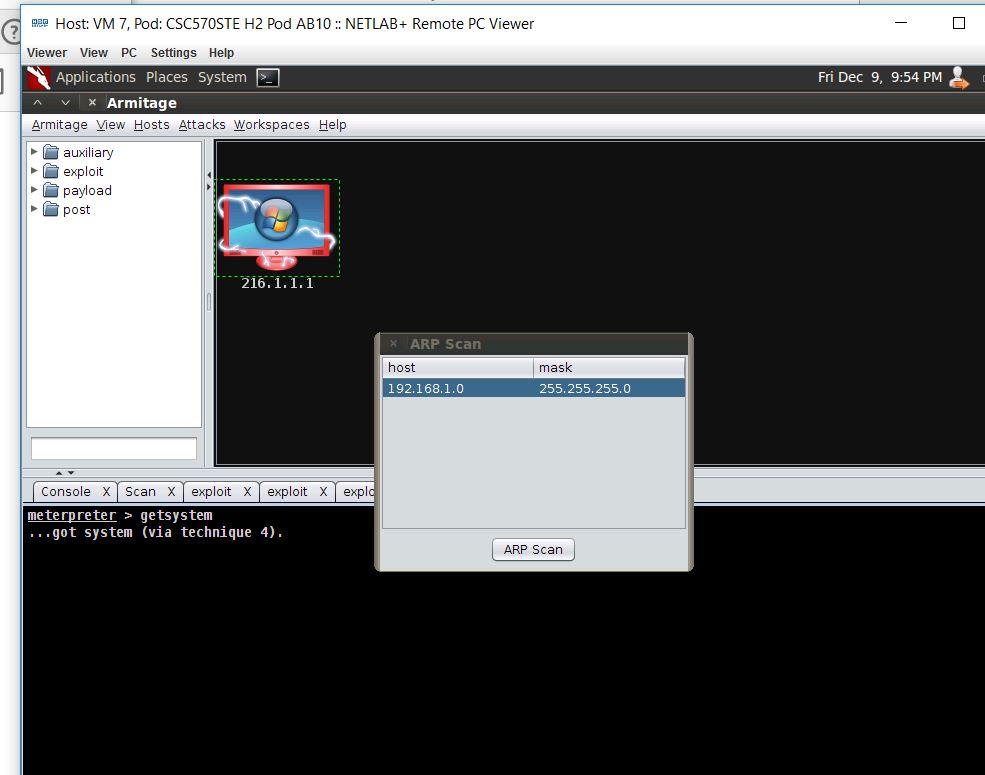
The target has changed to red (with lightening) which indicates that it has been compromised.

STEP-11



In the above screenshot we have interacted with the meterpreter by following: Right-click on 216.1.1.1, select Meterpreter 1, interact, and Meterpreter Shell. In the Meterpreter 1 below, type the following command to escalate privileges. meterpreter > getsystem.

STEP-12

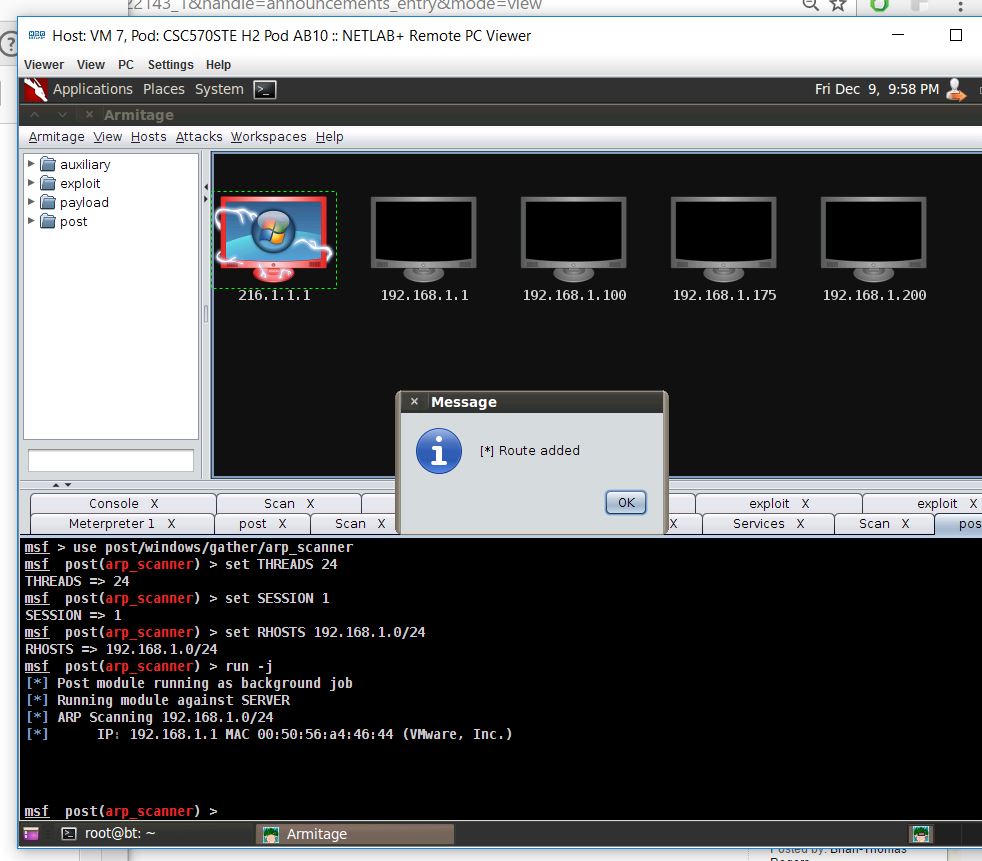


Here in the above screenshot we are scanning the ARP and its netwok by following the Armitage menu, choose Set Exploit Rank, and select Poor.

STEP-13

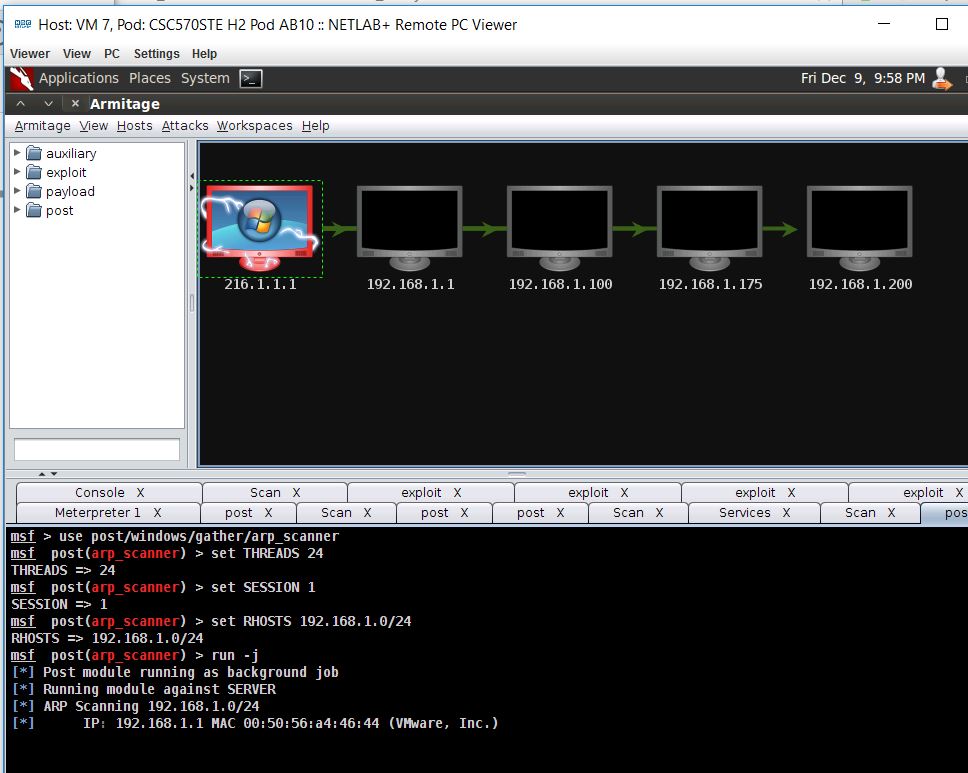


In this above image you can see the Internal Netwok Layout by loging into the boxes and ping the gateway of 192.168.1.1.

STEP-14

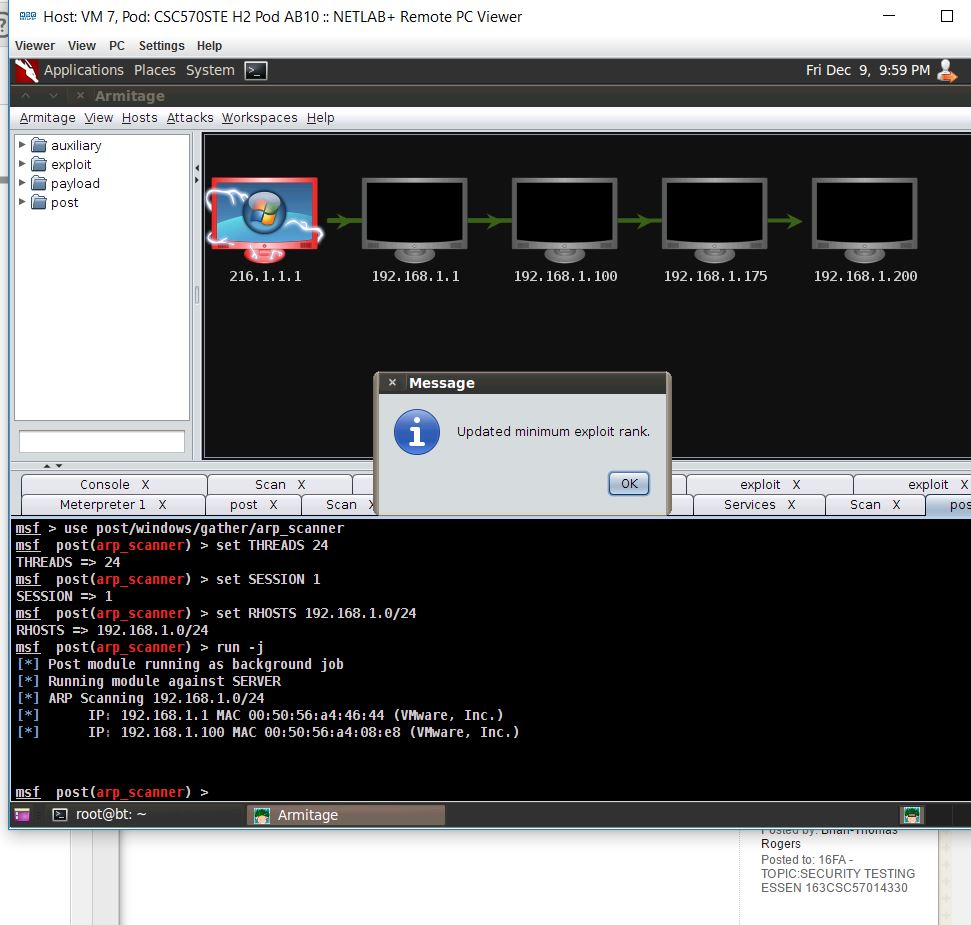
In this image we are setting up pivoting by viewing the internal network and adding the Pivot.

STEP-15



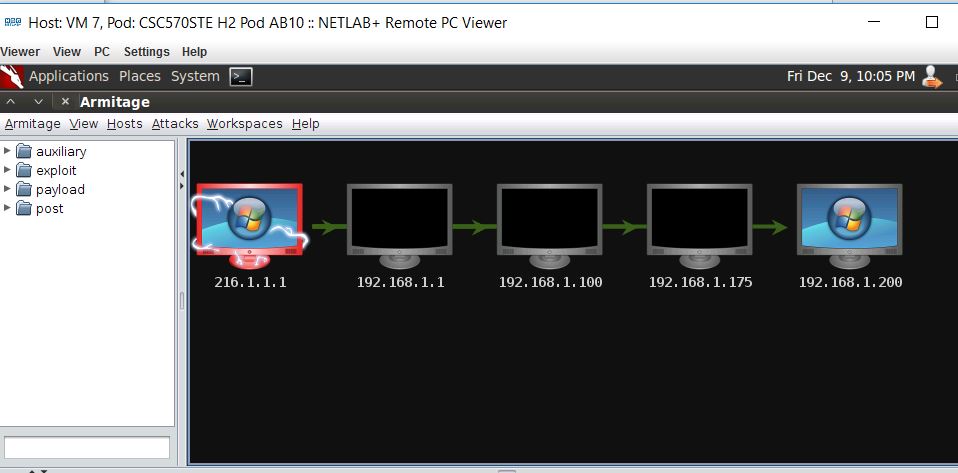
In the above image you will see a Green arrow connecting 216.1.1.1 to all of the Internal Victims.

STEP-16



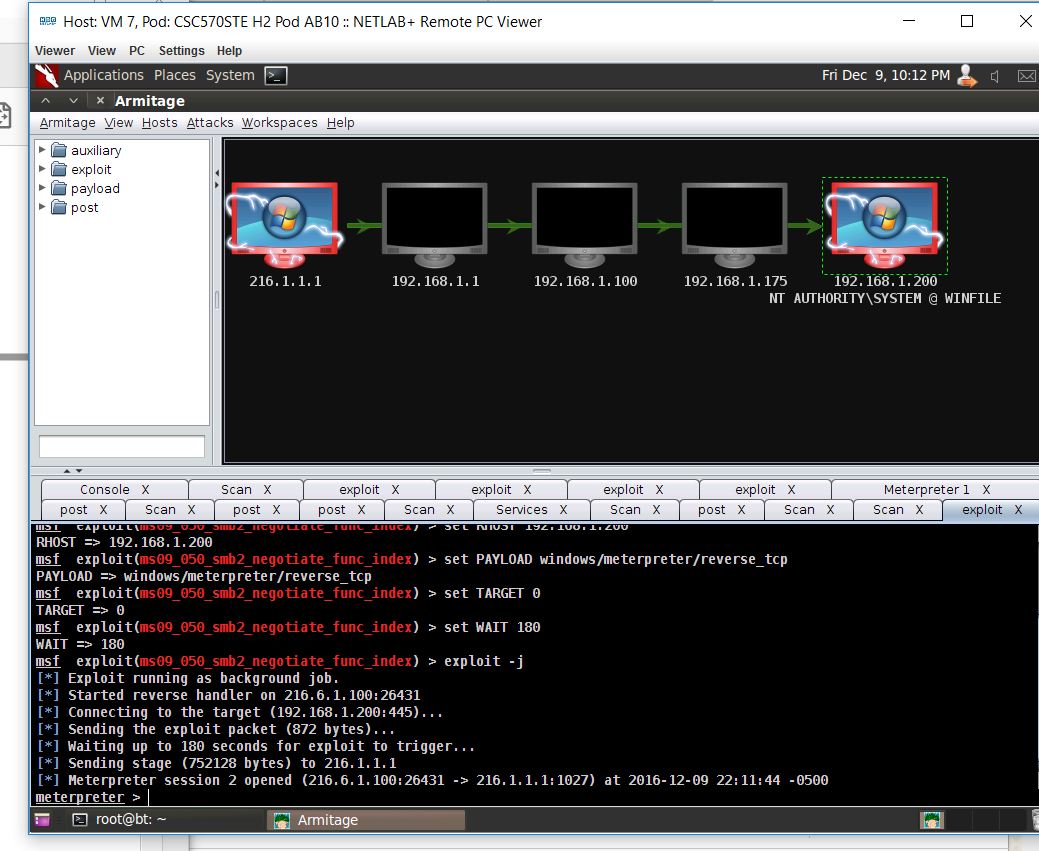
Here in this screenshot we are updating the minimum exploit rank after lowering the exploit rank in the Armitage menu.

STEP-17



The target is identified. If you hover over the icon, the remote machine will be identified as Windows Server 2008 Standard without Hyper-V SP1.

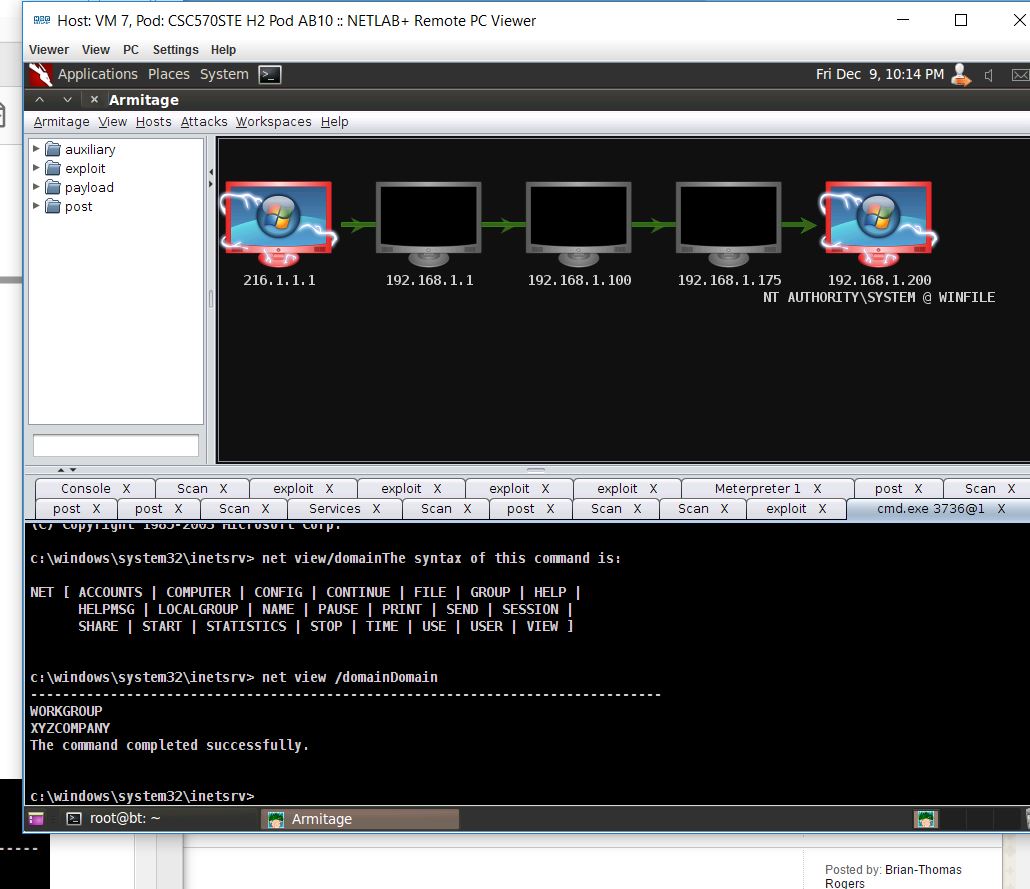
STEP-18



The above image is the result of finding the attacks by using the reverse connection for the attack titled 192.168.1.200 against the victim machine.

Finally the attacker is connected to the victim machine as system.

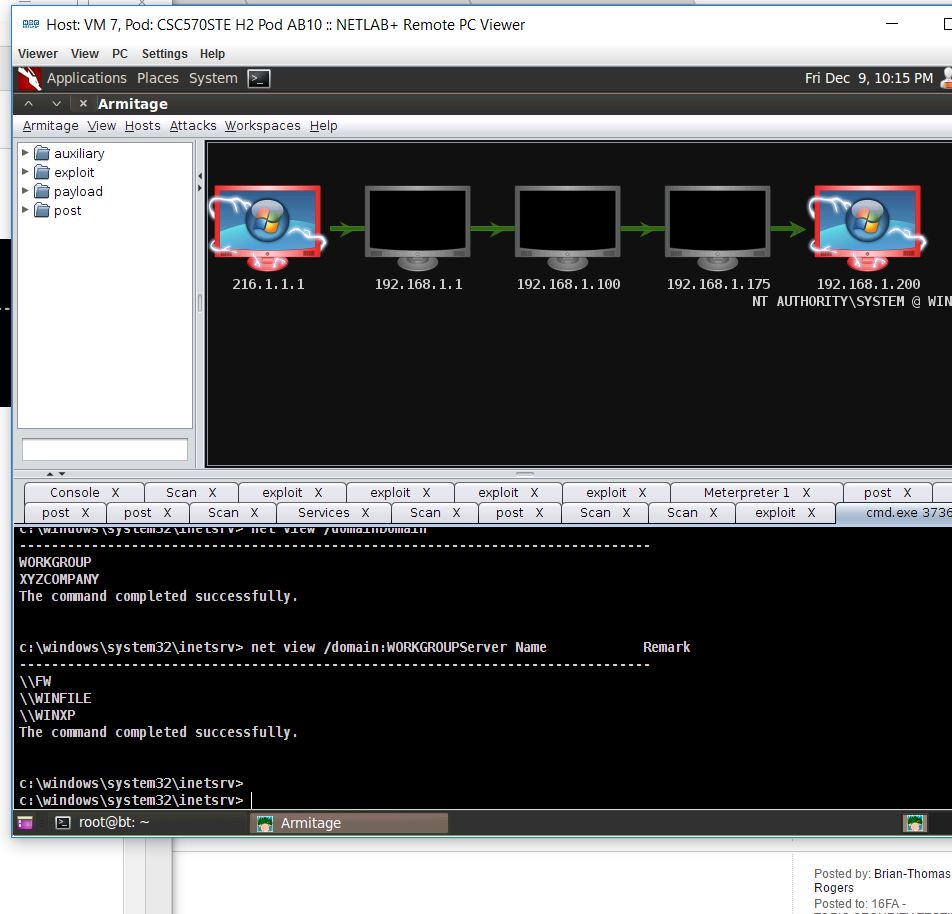
STEP-19



After interacting with a command shell on Windows 2003 SQL, we listed the available domains on the network by the command for the net view:

c:\windows\system32\inetsrv> net view /domain

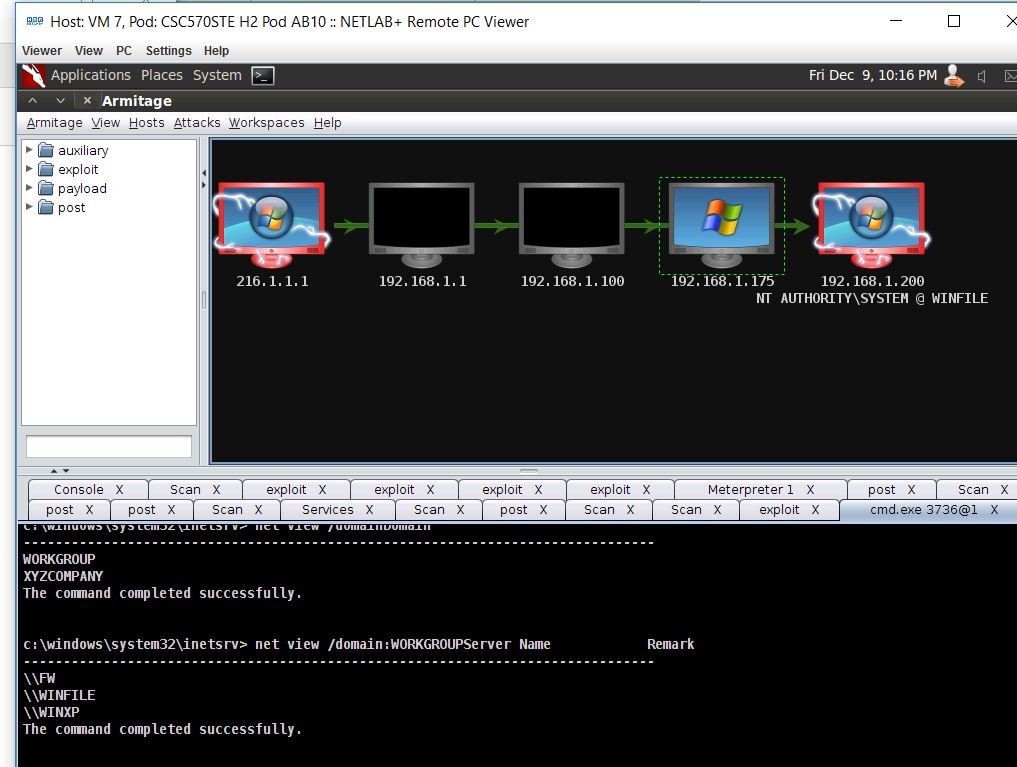
STEP-20



This screenshot displays the domains on the internal network WORKGROUP and XYZCOMPANY which is obtained by the command:

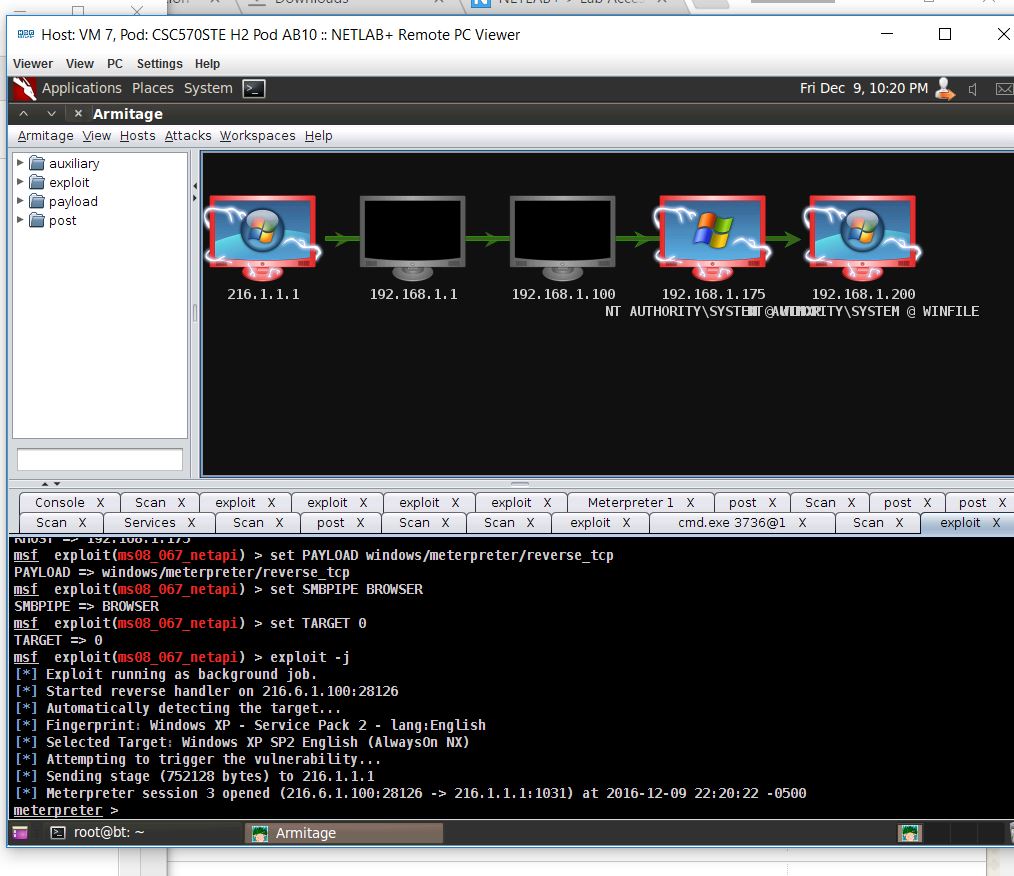
c:\windows\system32\inetsrv> net view /domain:WORKGROUP

STEP- 21



After manually designating the operating system with the IP Address: 192.168.1.175 and OS identified.  
Now we scanned for the open ports and the found attacks which exploited the targets

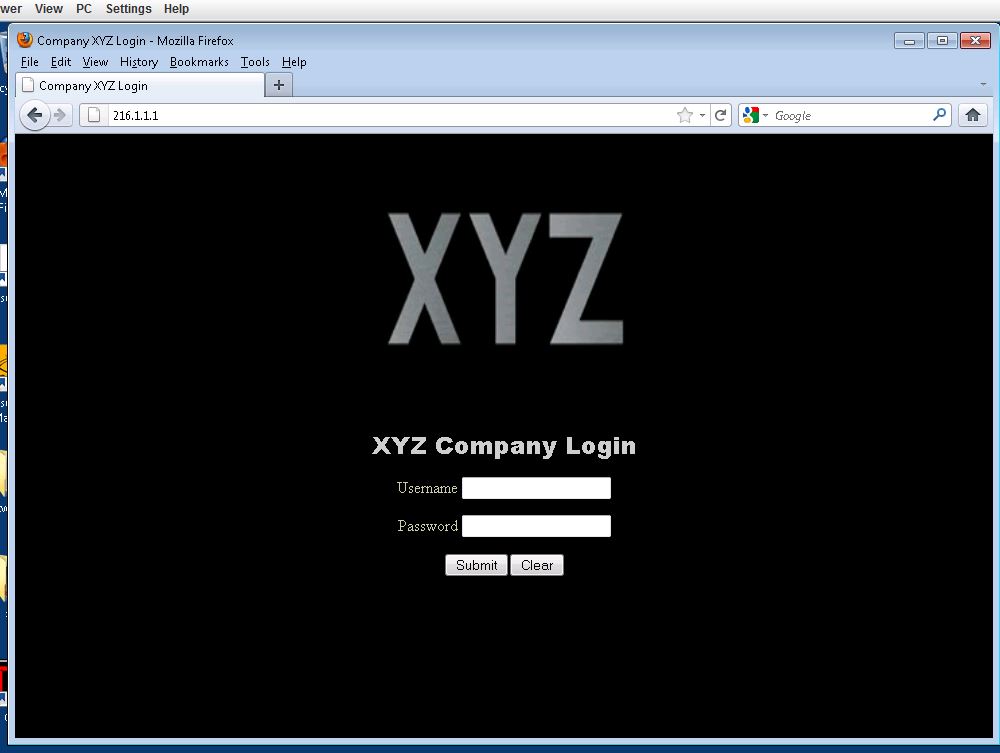
STEP-22



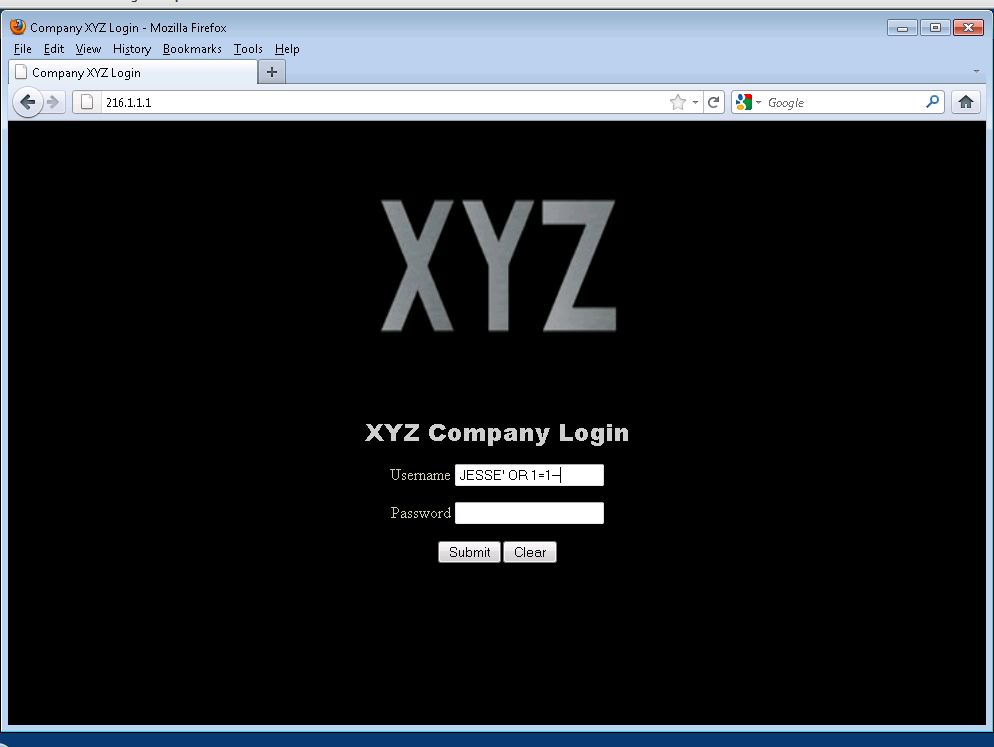
In the final screenshot, we scanned for the open ports and the found attacks which exploited the targets by the attack titled 192.168.1.175 using the reverse connection.

We can see the 3 compromised machines on the internal network.

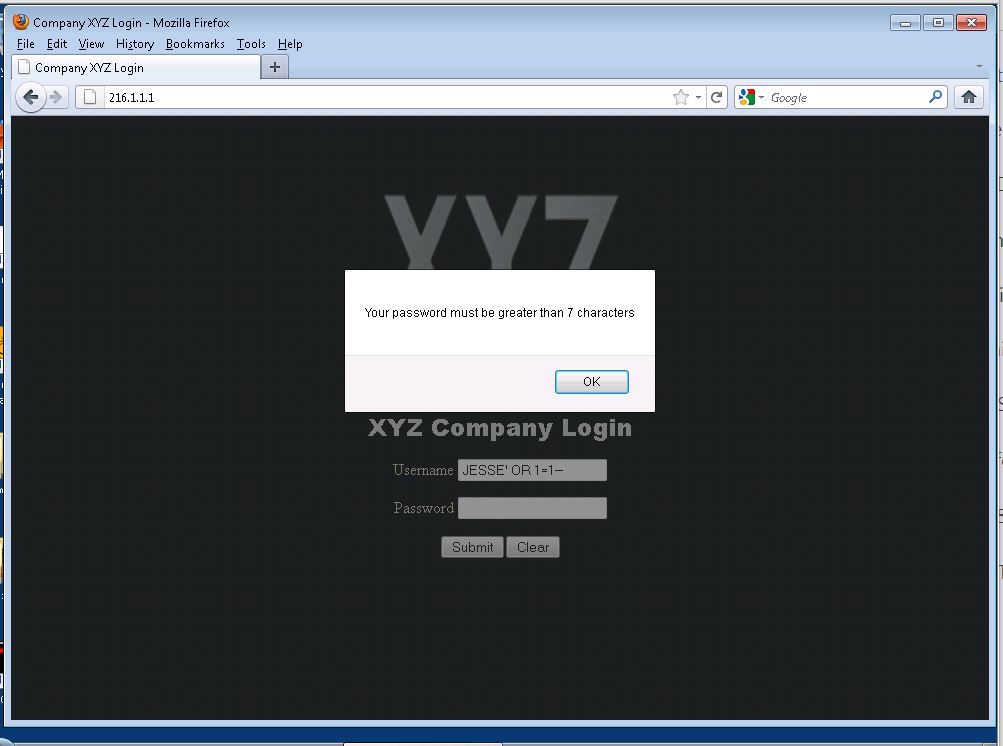
1. SQL INJECTION



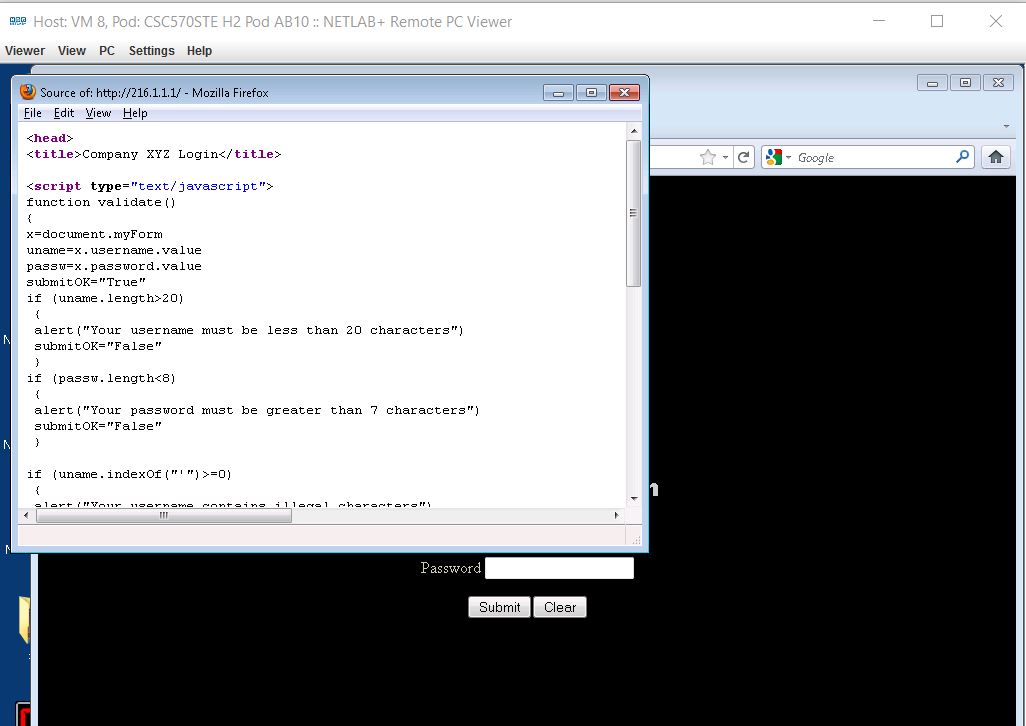
Step 1 : Logging in to the company xyz, a web front end of an sql server.



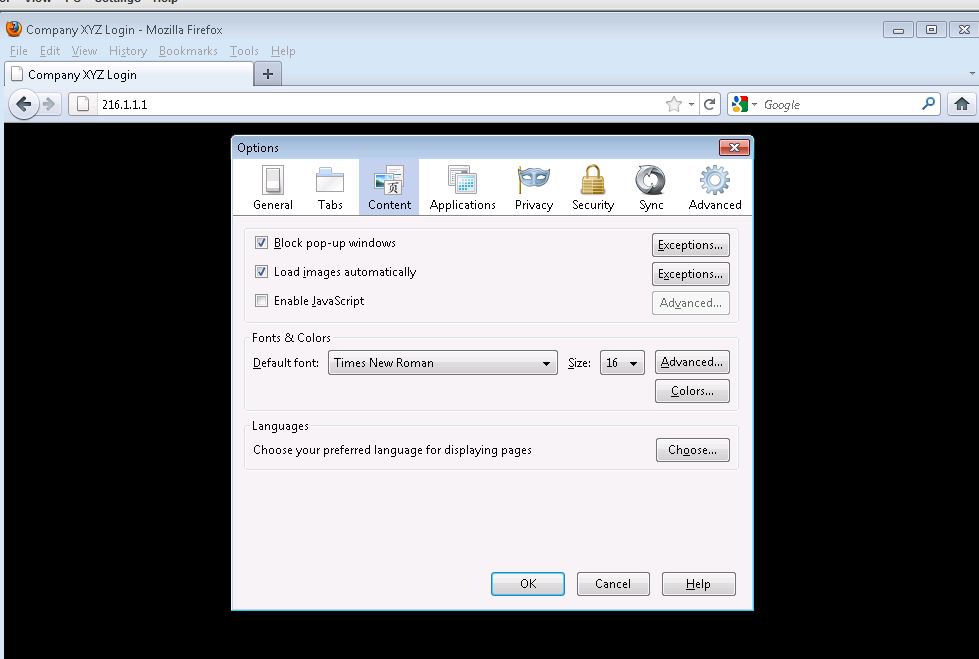
Step 2 : Login with the username and password as shown in the screenshot.



Step 3 : The dialogue box shows that the password must be 7 characters. So we type in the password with more than 7 characters and login.



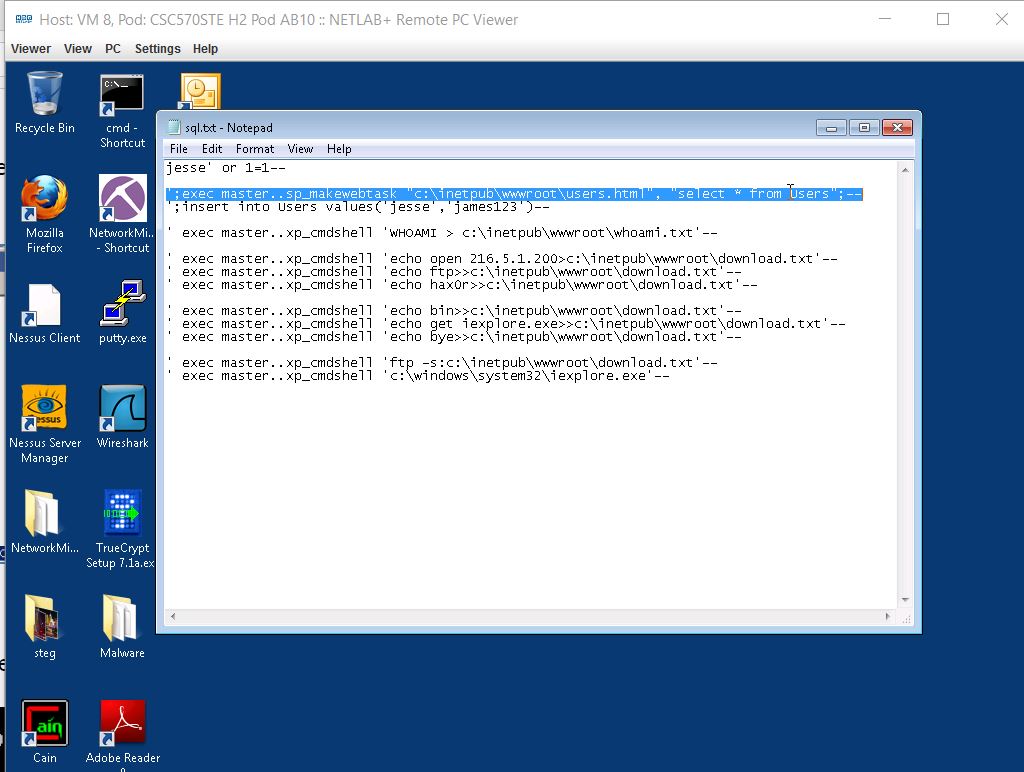
Step 4 : We right click on the login page to get the source page. The web application is using JavaScript to check the input validation.



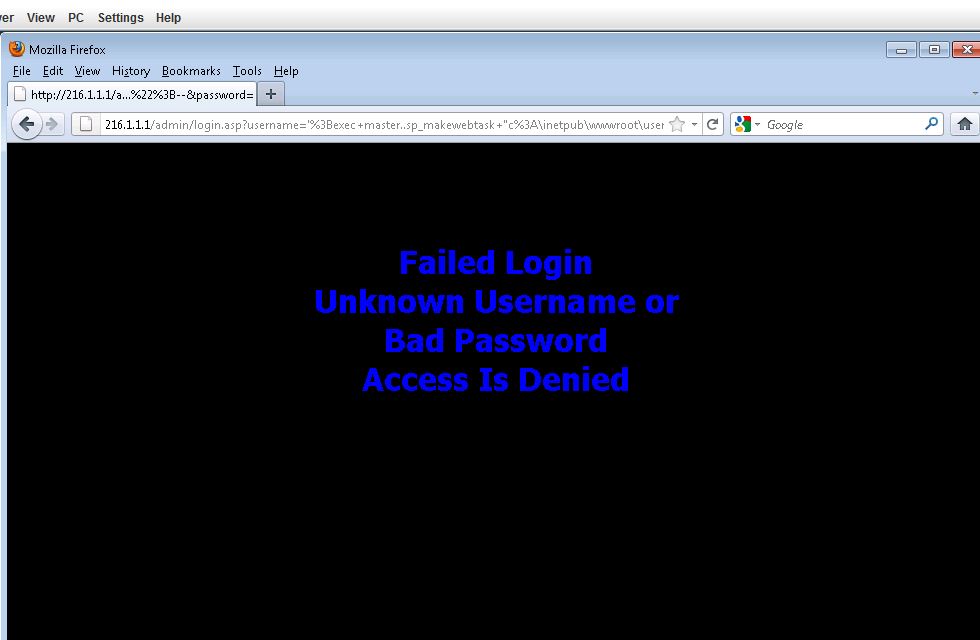
Step 5 : The above screenshot shows how to disable the JavaScript



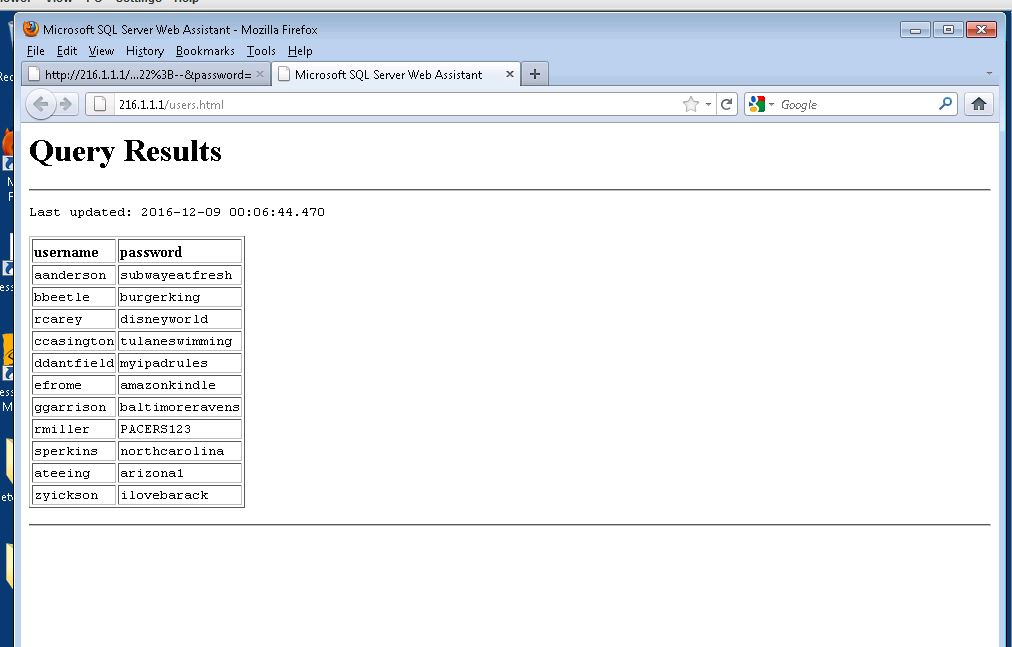
Step 6 : After giving the correct credentials, we will be successfully logged in as user aanderson as shown above.



Step 7 : Open the sql.txt file on desktop and the above content is shown.

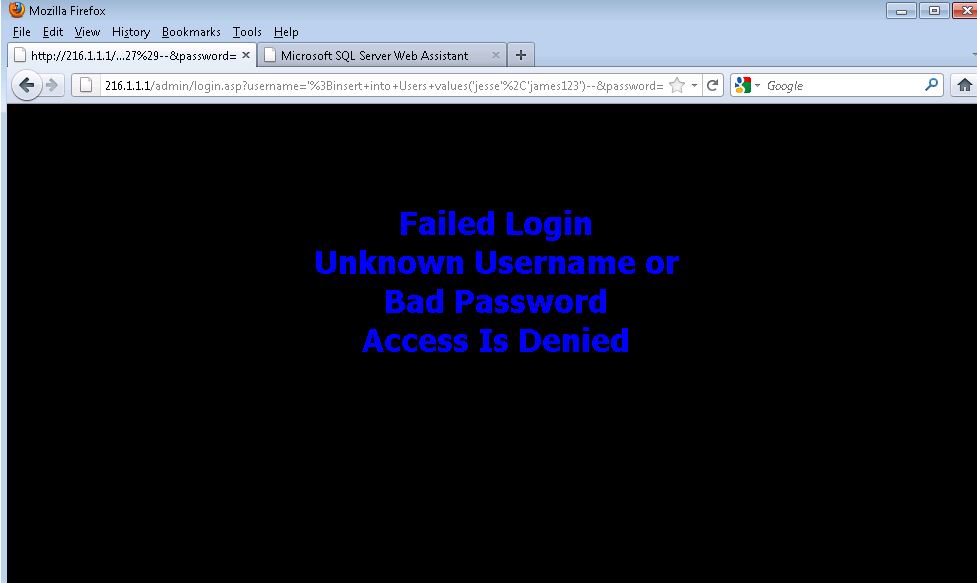


Step 8 : The above content is shown when the wrong username is given.

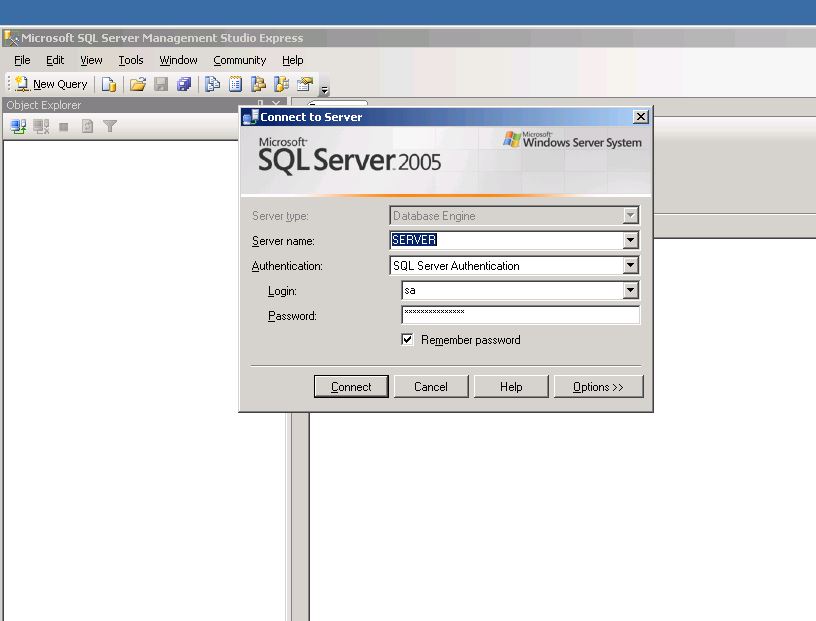


Step 9 : These are the list of updated users and their passwords to login from 216.1.1.1.

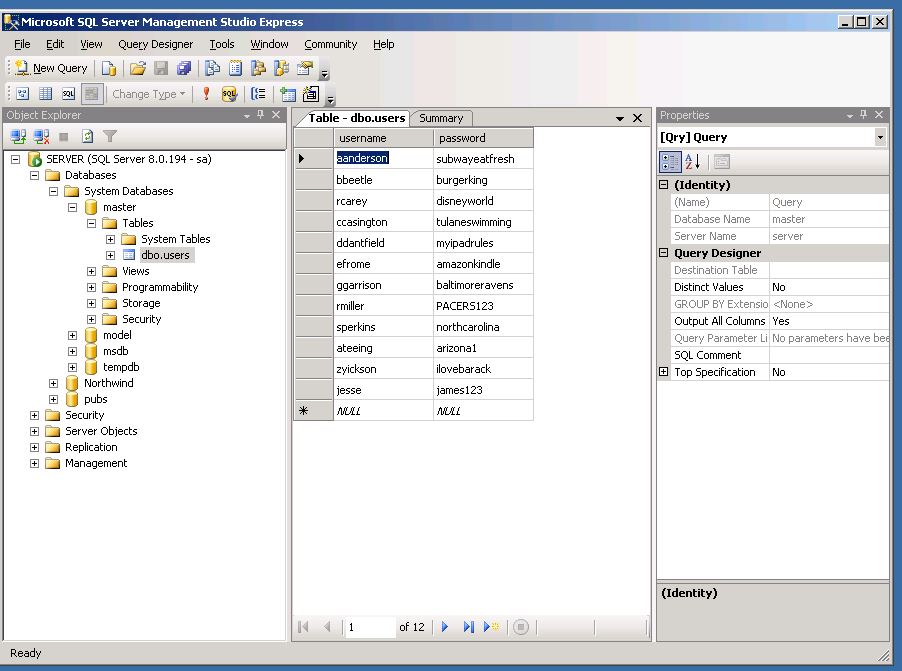




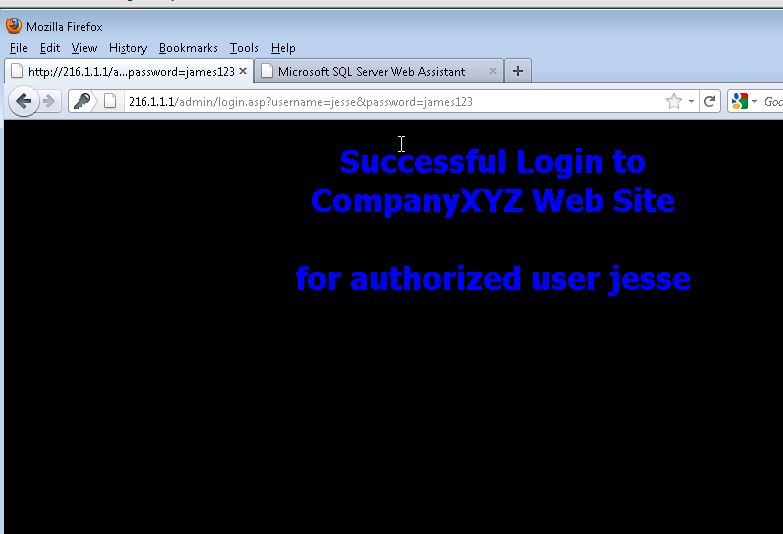
Step 10 : We try multiple usernames and passwords, the above content is repeated.



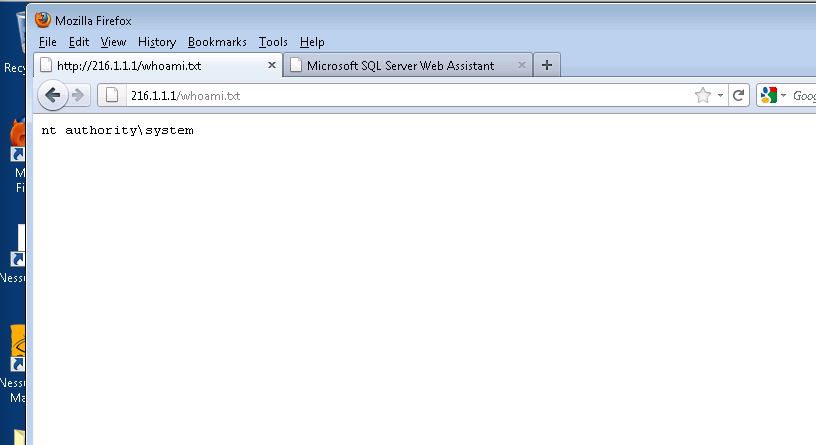
Step 11 : We open the SQL Server Management Studio and connect to the SQL server as shown above.



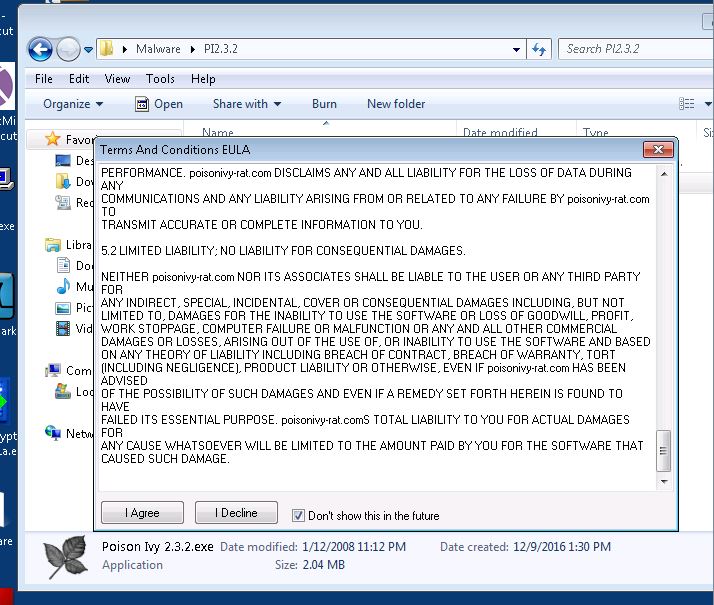
Step 12 : Expand Servers, databases, system databases, master and tables. View the second to last tables that match up with the login credentials.



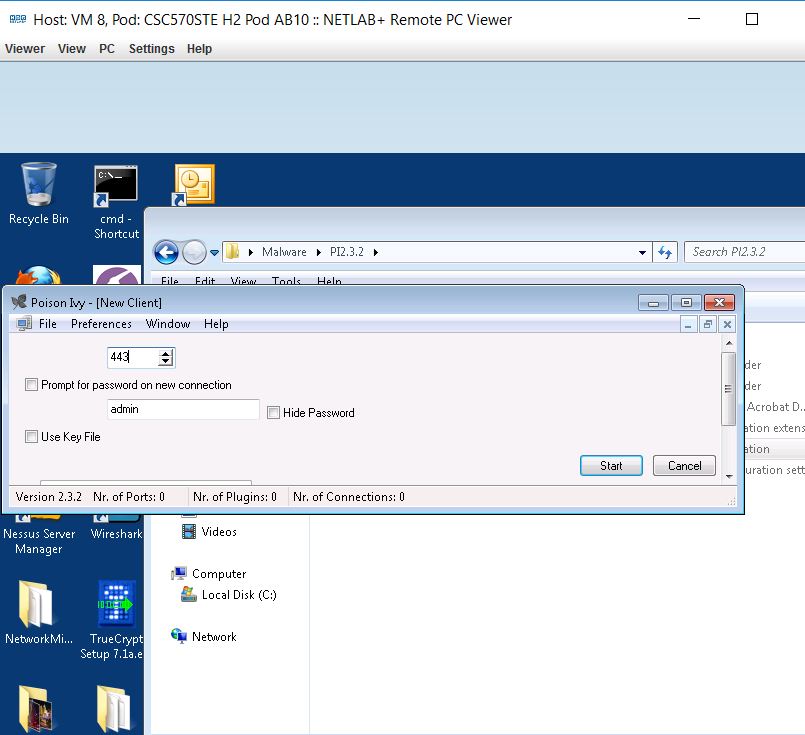
Step 13: Now, we will be successfully logged in to the company XYZ as shown above.



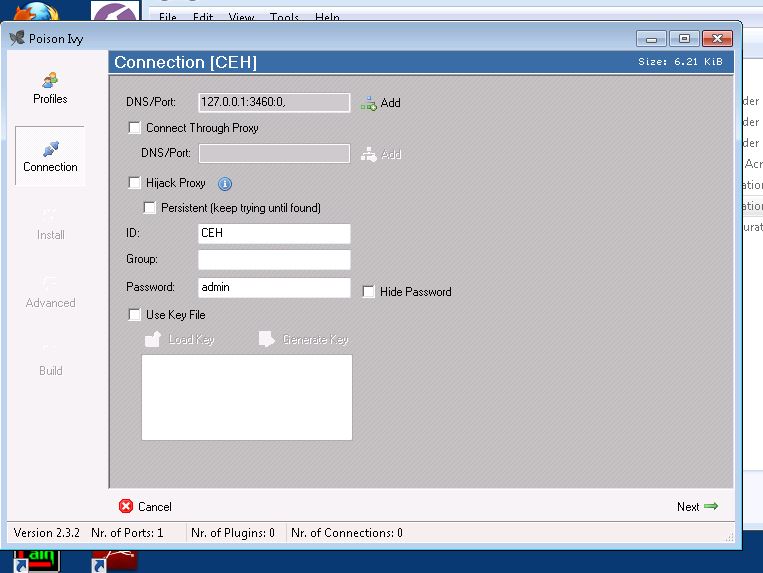
Step 14 : The public page of 216.1.1.1



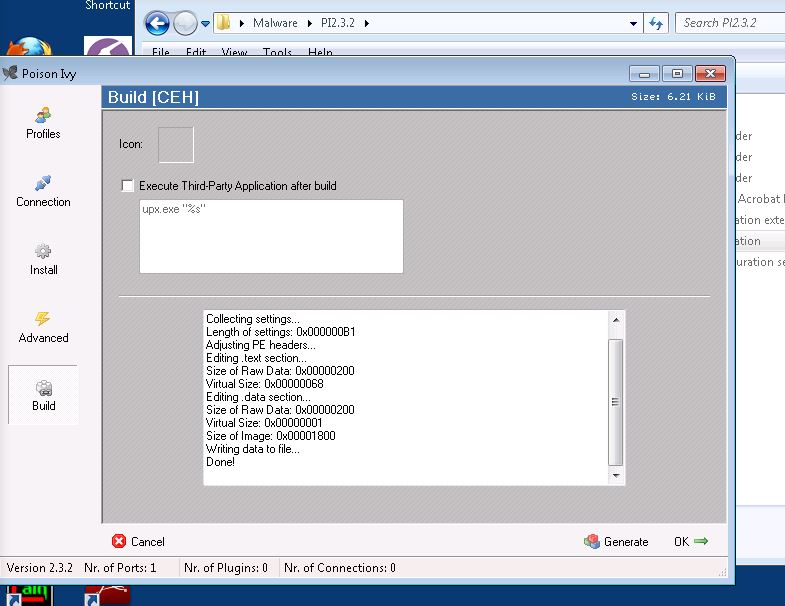
Step 15 : This is the Poison Ivy 2.3.2.exe. We need to check ‘Don’t show this in the future’ and click ‘ I Agree’.



Step 16 : As shown above, type 443 and click start

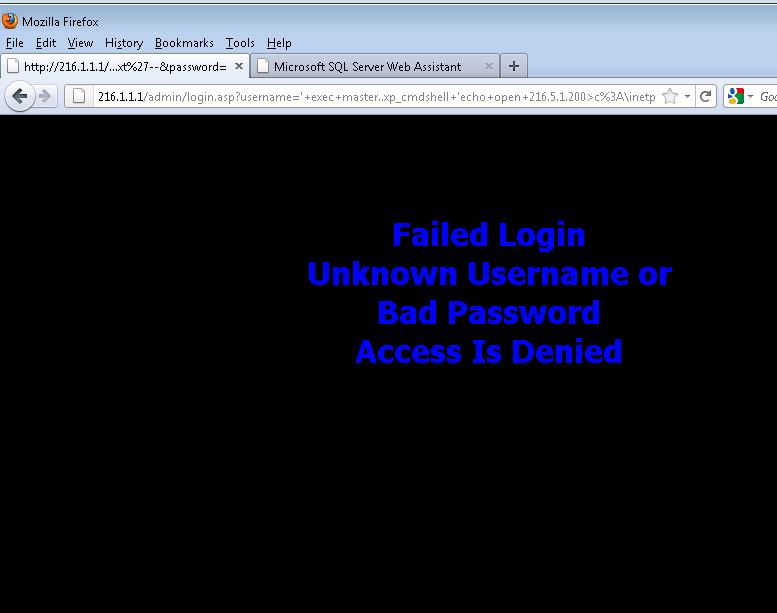


Step 17 : This is the connection screen, Type the above port and click next.

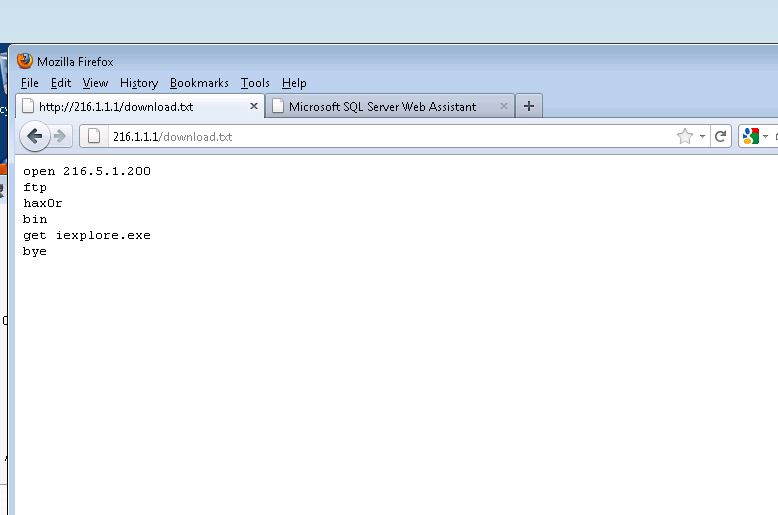


Step 18 : This is the Build screen of Poison Ivy.



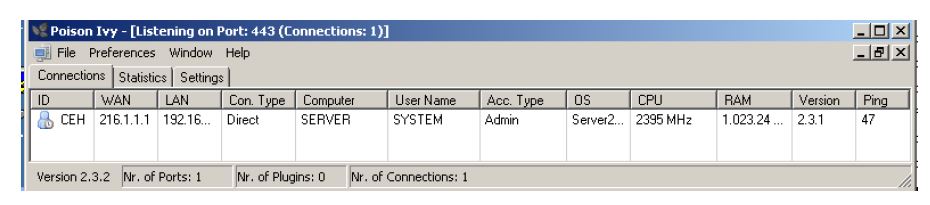


Step 19 : Attempting to login for another time

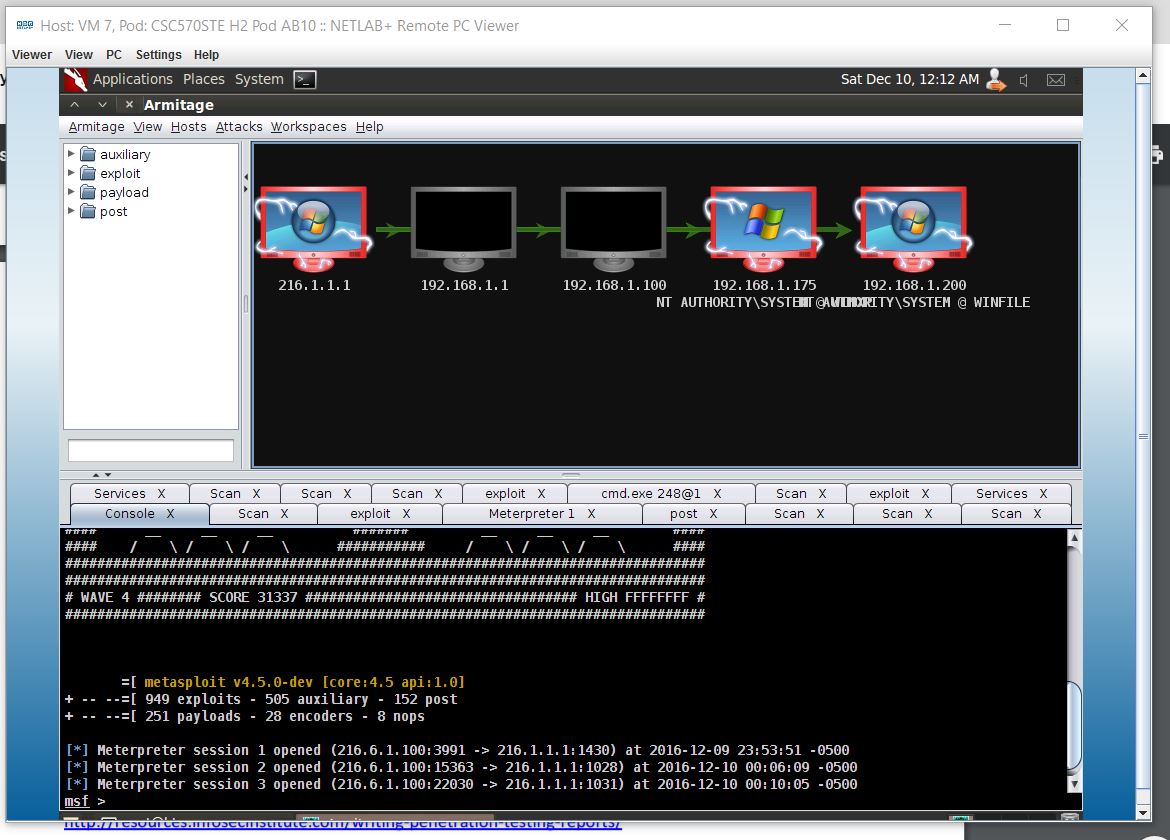


Step 20 : The final display for the public page 216.1.1.1.

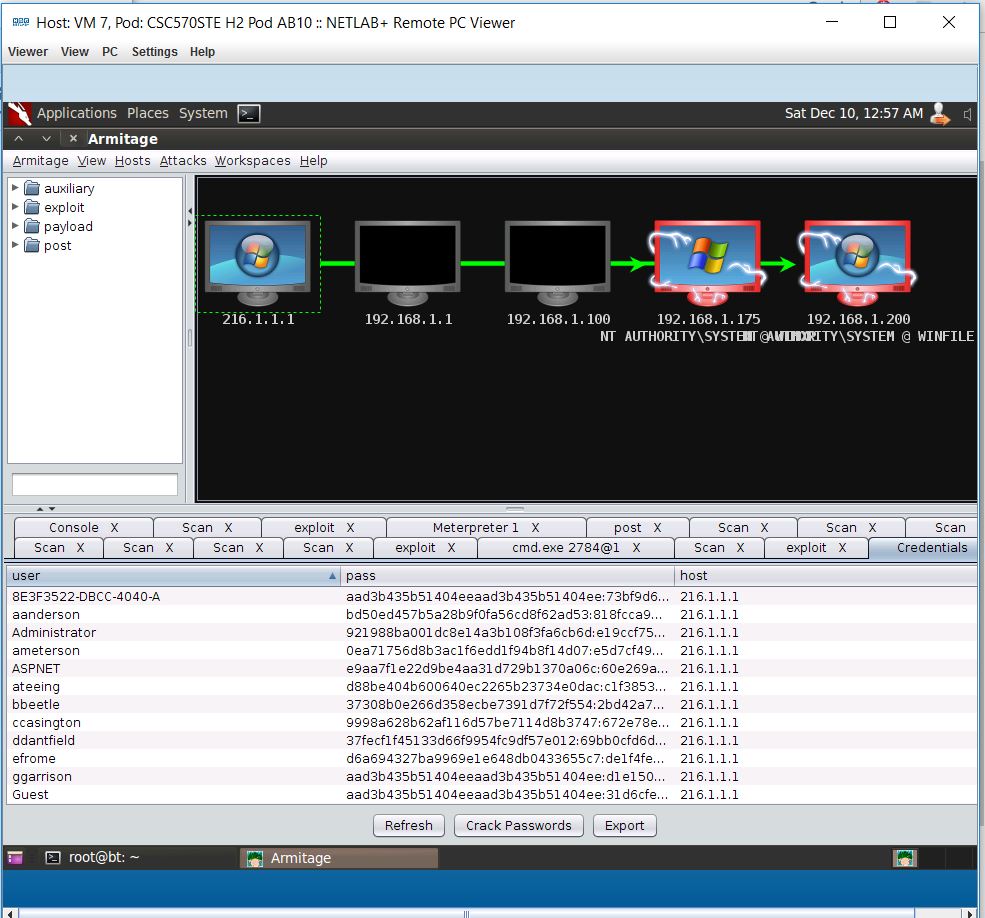
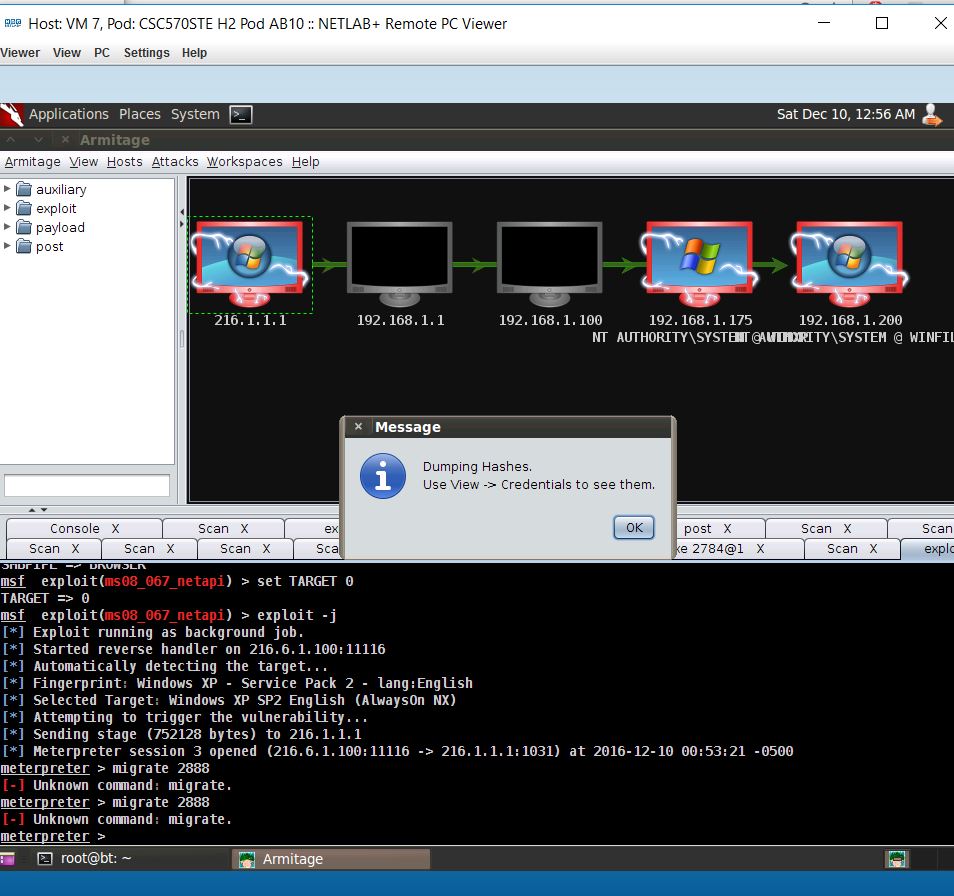
Finally we have a Poison Ivy connection to the victim SQL server machine.



EXPLOITING THE MACHINE:



GRABBIING THE HASHES:



CRACKING THE PASSWORDS:

––

