Module: LD7010-Ethical Hacking for Cyber Security

Student university identifier: W19049250

Course of study: MSc Cyber Security

Word count for Part-A: 2,103 Words

Excludes cover sheet, contents, list of figures and references

2,564 Words

Includes cover sheet, contents, list of figures and references

Word count for Part-B: 2,193 Words

Excludes cover sheet, contents, list of figures and references

2,751 Words

Includes cover sheet, contents, list of figures and references

Contents

[PART-A 4](#_Toc40658346)

[Introduction: 4](#_Toc40658347)

[Software Requirement: 4](#_Toc40658348)

[Tools Used: 4](#_Toc40658349)

[Machine Setup: 4](#_Toc40658350)

[Attack 1: FTP Backdoor Command Execution 5](#_Toc40658351)

[Steps to Perform Attack 5](#_Toc40658352)

[Countermeasures 9](#_Toc40658353)

[Attack 2: SSH Brute Force 13](#_Toc40658354)

[Steps to Perform Attack: 13](#_Toc40658355)

[Countermeasures 20](#_Toc40658356)

[Attack 3: DOS Attack on Client Machine through SSL/ms-wbt-server 21](#_Toc40658357)

[Steps to perform Attack 21](#_Toc40658358)

[Countermeasures 25](#_Toc40658359)

[Attack 4: Phishing User Credentials with BlackEye 25](#_Toc40658360)

[Steps to perform Attack 26](#_Toc40658361)

[Countermeasures: 29](#_Toc40658362)

[References 30](#_Toc40658363)

[PART-B 31](#_Toc40658364)

[Abstract 31](#_Toc40658365)

[Introduction 31](#_Toc40658366)

[The DNS Attack at GitHub 32](#_Toc40658367)

[Critical Discussion, analysis, and reflection 33](#_Toc40658368)

[Methodology 35](#_Toc40658369)

[Countermeasures for DNS attack at GitHub 35](#_Toc40658370)

[Conclusion 36](#_Toc40658371)

[References 36](#_Toc40658372)

**List of Figures**

Figure 1: Fully loaded virtual machine 4

Figure 2: IP address of Metasploitable server 5

Figure 3: Port scanning using Nmap 6

Figure 4: Using msfconsole 7

Figure 5: Setting RHOST 8

Figure 6: Exploiting 8

Figure 7: Exploit conformation 9

Figure 8: Hacked Successfully 9

Figure 9: Disabling Anonymous Login 10

Figure 10: Failure of Exploitation 10

Figure 11: Enumerating FTP Banner 10

Figure 12: Banner disabled 11

Figure 13: Configuring IP table 11

Figure 14: Configuring IP table 12

Figure 15: Scanning for open ports of metasploitable server 12

Figure 16: IP address of Ubuntu server 13

Figure 17: Port scanning with Nmap 14

Figure 18: Using Searchsploit 15

Figure 19: Creating Usernames 15

Figure 20: Creating Passwords 16

Figure 21: Running msfconsole 17

Figure 22: Setting up the host, usernames and passwords 18

Figure 23: exploiting 19

Figure 24: Access gained by attacker 19

Figure 25: Exploring credential information of Ubuntu server 20

Figure 26: Disabling the open ports 21

Figure 27: IP Address of Client Machine 22

Figure 28: Port Scanning Using NMAP 22

Figure 29: Running msfconsole 23

Figure 30: Setting up the host 23

Figure 31: Exploiting 24

Figure 32: Client System Crashed 24

Figure 33: Configuring the Vulnerability 25

Figure 34: Installing BlackEye 26

Figure 35: Options provided by Tool 26

Figure 36: Configuring 27

Figure 37: Code for creating application 27

Figure 38: Application That Sends Anonymous Email 28

Figure 39: Email received by Client 28

Figure 40: Entering Username and Password 29

Figure 41: Exploiting 29

# 

# PART-A

Introduction:Part-A is a practical part which demonstrate 4 attacks. FTP, SSH, SSL and Phishing are the attacks which fall under service or social engineering attacks. When effected with any of these attacks it can be mitigated by following some countermeasures.

**Configuration required**

## **Software Requirement**:

* **Virtual machine**: virtual machine is to provide a powerless working environment and creating various administrations that operate on an operating system. VMware, and VM virtual box, for example. To run the virtual machine makes a point to empower Virtualization in BIOS.
* **Operating Systems**: Kali Linux, Parrot, Windows 7.
* **Servers**: Ubuntu server, Metasploitable web server.

## Tools Used:

* **Nmap:** Nmap (Network Mapper) is a free, open-source resource for organising disclosure and security checks. Mainly used for checking ports of a given IP address. Loads of Nmap content is available to distinguish weakness on track. (adminVRT, 2016)
* **Metasploit Framework:** It is an open-source programme that is unhindered to use. The system has established vulnerabilities in the process which are misused differently. The list of projects is usually enhanced by impressions of the new discoveries that have opened up to the world
* **Searchsploit:** Searchsploit is an offline database of exploits available at Exploit-DB
* **Meterpreter:** It is a Metasploit assault payload that gives an intuitive shell from which an assailant can investigate the objective machine and execute code.

## Machine Setup:

* Download and install Oracle VM Virtual Box and install windows 7, Parrot, Kali Linux, Ubuntu Server, Metasploitable server in VM box and check for network connectivity.

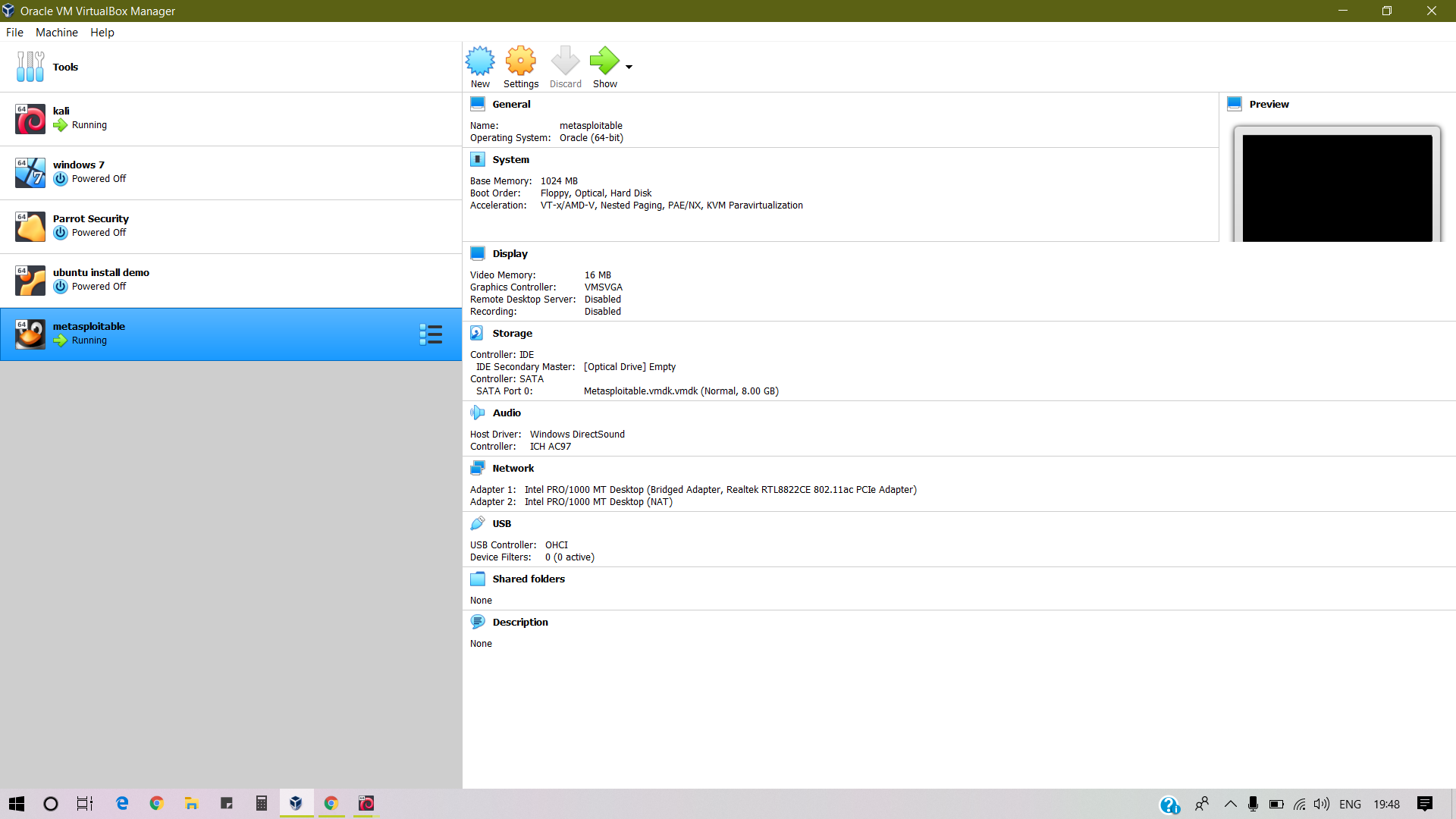


Figure 1: Fully loaded virtual machine

## Attack 1: FTP Backdoor Command Execution

In this attack FTP service is compromised to hack / gain access of the Client Machine.

**OS Guidance:**

Use **Kali Linux** as Attacker Machine

**Metasploitable sever** as Client Machine

### Steps to Perform Attack

**Step 1:** Open Metasploitable server in oracle VM virtual box and execute the “ifconfig” command to know the IP address.

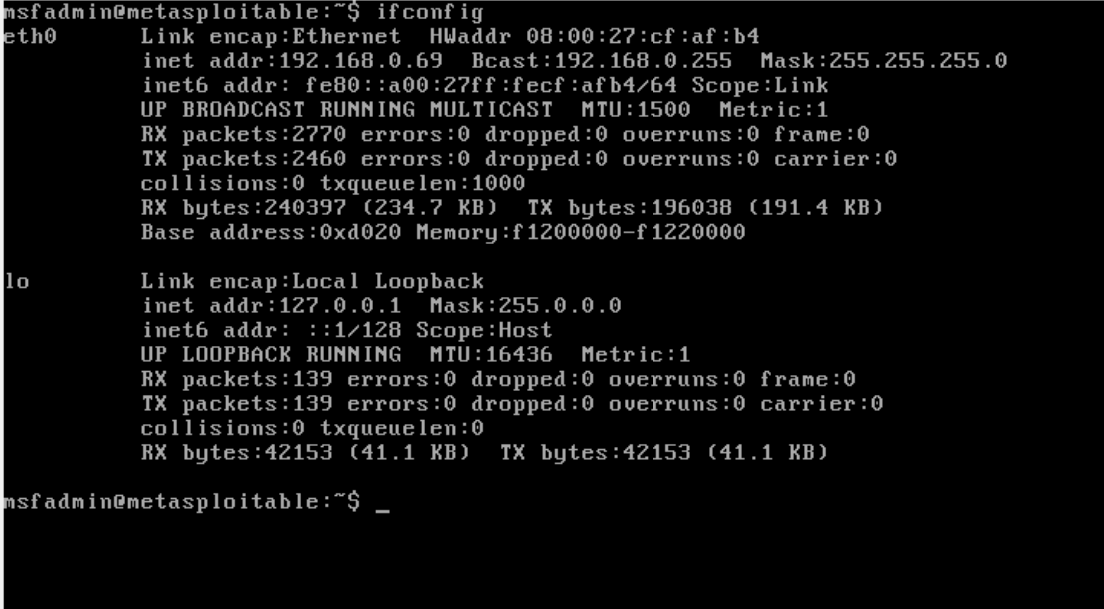
****

Figure 2: IP address of Metasploitable server

**Step 2**: 192.168.0.69 is an IP Address to be noted or to be recalled.

**Step 3:** Using NMAP tool in kali Linux/Attacker Machine to search open ports of Client machine.

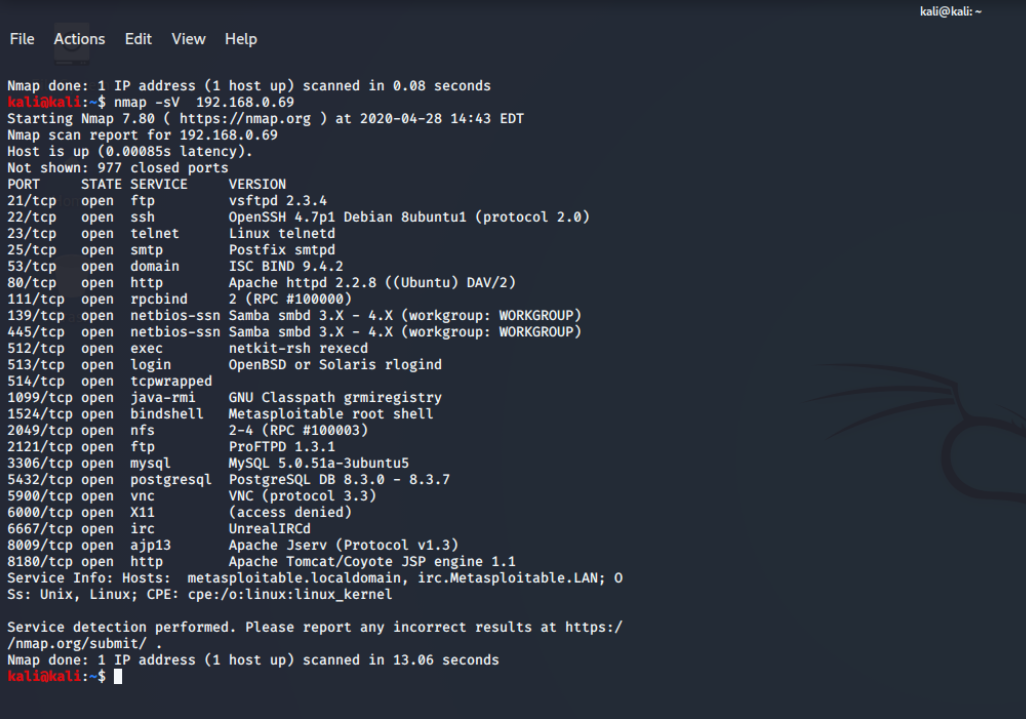
****

Figure 3: Port scanning using Nmap

Figure 3 shows all the open ports of the metasploitable server.

“nmap -sV 192.168.0.69” was the command used for port scanning.

-sV: Attempts to determine the version of the server running on ports

**Step 4:** Hacking / Exploiting the victim

Metasploit tool is used for exploiting.

In Kali terminal, use msfconsole to operate Metasploit

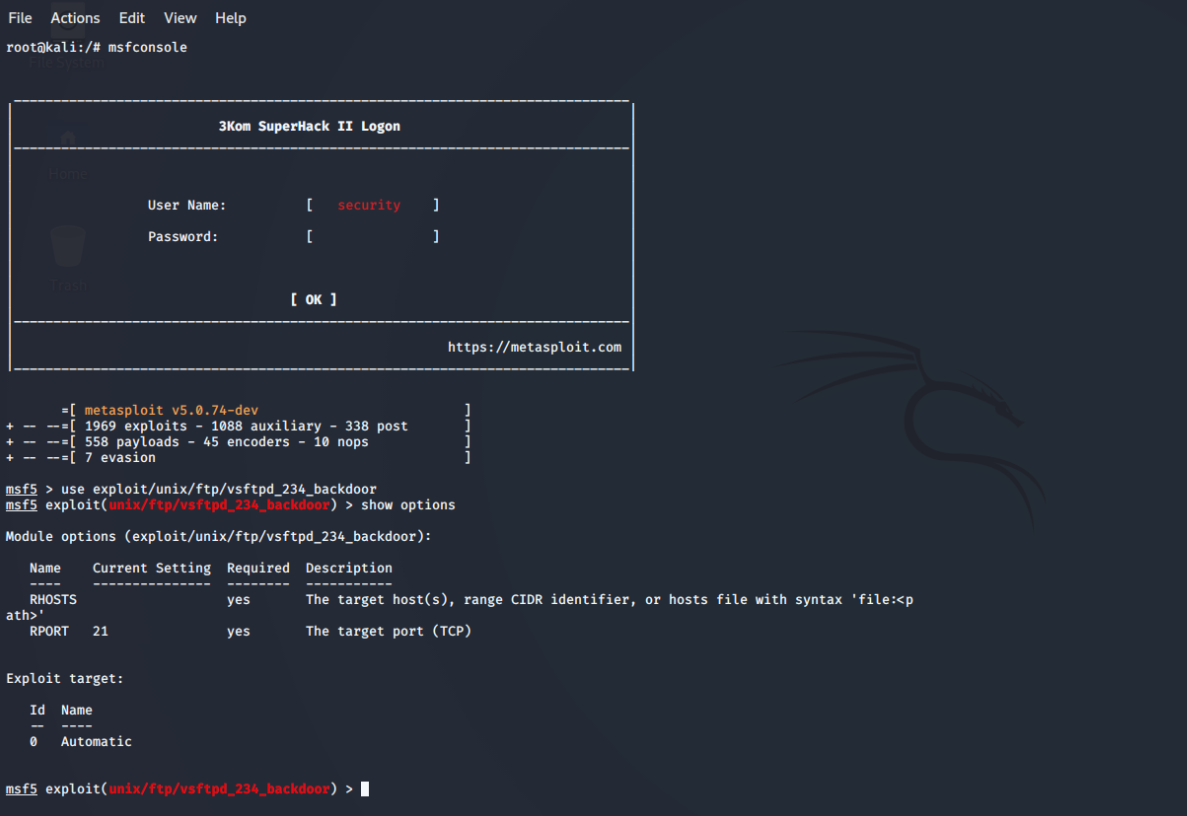


Figure 4: Using msfconsole

An attacker can easily use following Metasploit exploit (as shown in the figure 5) to check for anonymous login authorization.

****

Figure 5: Setting RHOST

The targeted machine is known as the remote host (RHOST) which should assign certain values to the exploit and payload options required where they are blank by default.

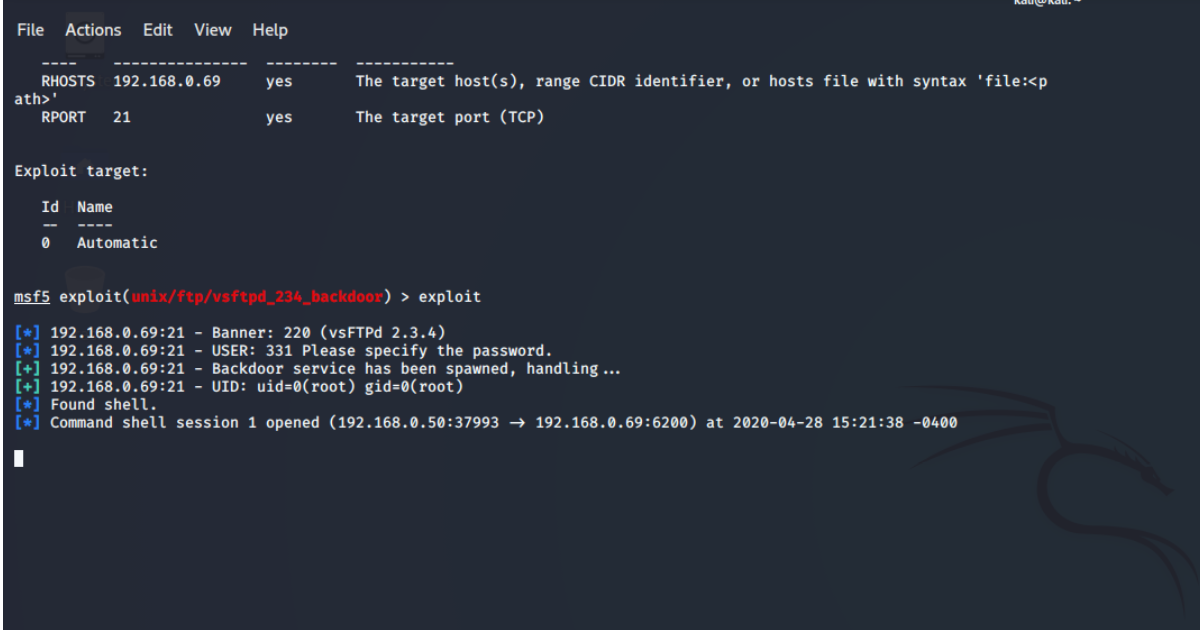
****

Figure 6: Exploiting

The **exploit** command is like pulling the trigger. With one click attacker will have complete control of the targeted machine. Successful exploit will receive the conformation in the terminal as shown in the figure 7



Figure 7: Exploit conformation

**Step 5:** Accessing the client meachine

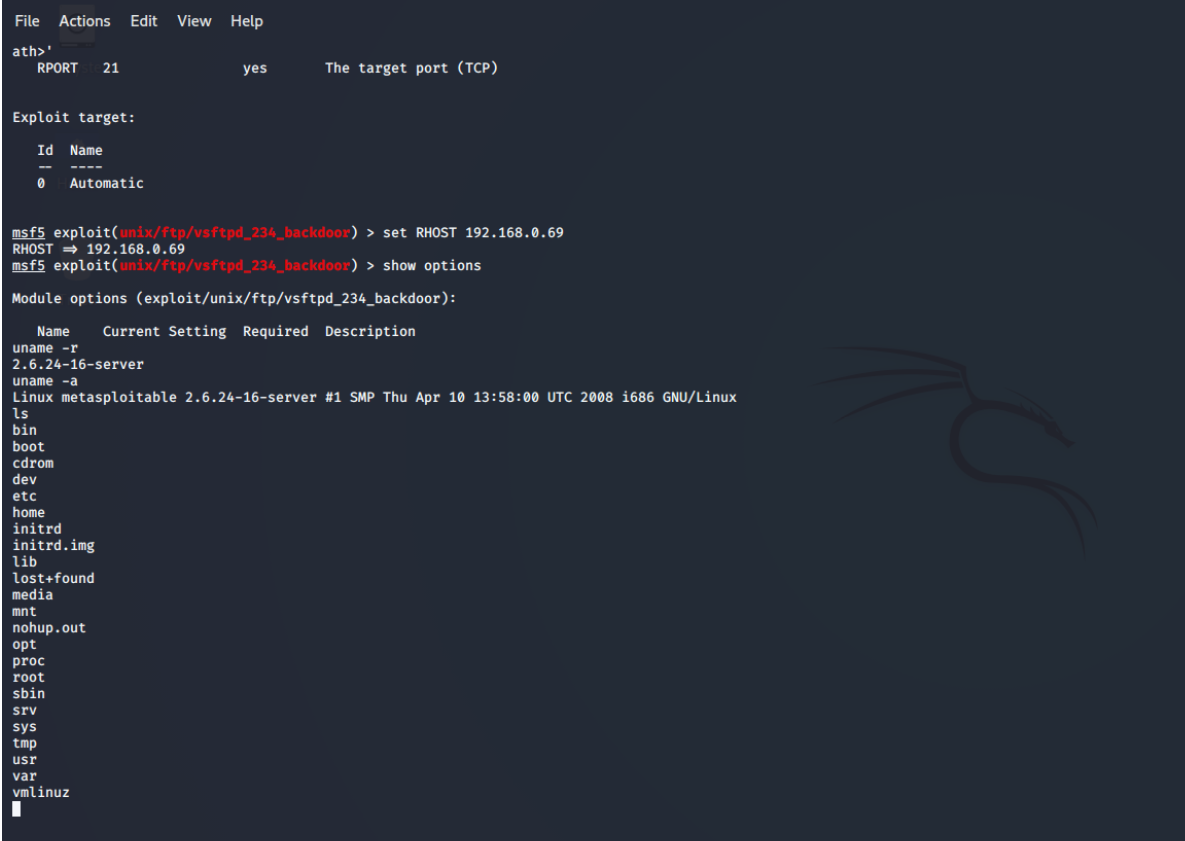


Figure 8: Hacked Successfully

Target was hacked successfully and Attacker gain the complete access.

### Countermeasures

**Countermeasure 1: Disable Anonymous Login and Enumerating FTP Banner**

1. Follow the measures below to protect servers from anonymous user login

* Open vsftpd.conf file in terminal
* #Set anonymous enable = No
* #Service vsftpd restart

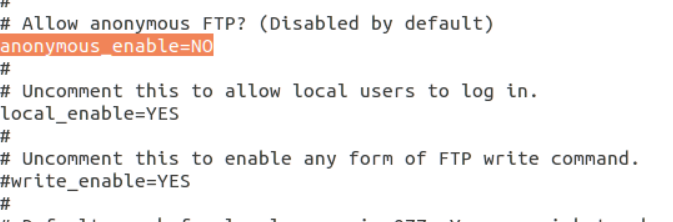


Figure 9: Disabling Anonymous Login

Rehash the assault to check for unknown login authorization utilizing Metasploit as above

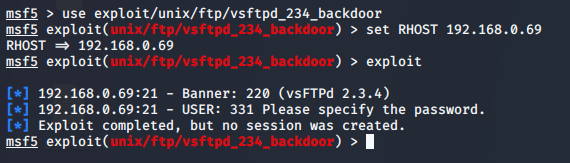


Figure 10: Failure of Exploitation

The adventure will neglect to take out data about mysterious client login authorization.

1. The administrator should roll out after improvements in their design document to forestall standard data

* Overview conf file
* Trigger a statement “ftp\_banner=Welcome to blah FTP service” With # separated from the edge. (Amir, 2017)

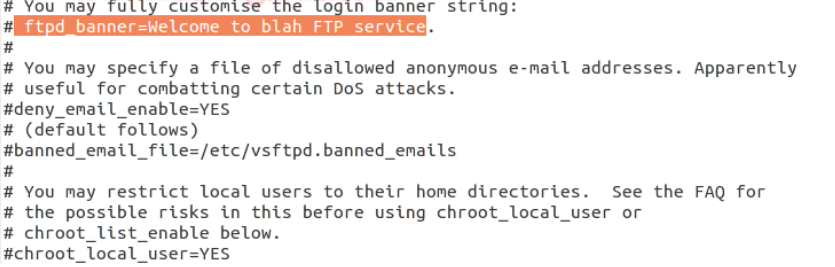


Figure 11: Enumerating FTP Banner

After modification save the entire text file and follow the steps below to resume operation.

**#Service vsftpd restart**

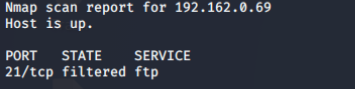
****

Figure 12: Banner disabled

**Countermeasure 2:** **Configuring the IP tables**



Figure 13: Configuring IP table

****

Figure 14: Configuring IP table

* **A:** append
* **j**: Specifies the packet's target disposition as it correlates to the law. \
* **p**: Characterizes the default strategy for one of the implicit chains, INPUT, OUTPUT, or FORWARD. The strategy is either ACCEPT or DROP.
* **i:** Specifies the interface name on which the standard applies for approaching bundles on either the INPUT or the FORWARD chains or their client characterized sub chain. If no interface is defined it means all interfaces.
* **Eth0**: interface

**Checking open ports of metasploitable web servers using NMAP once again:**

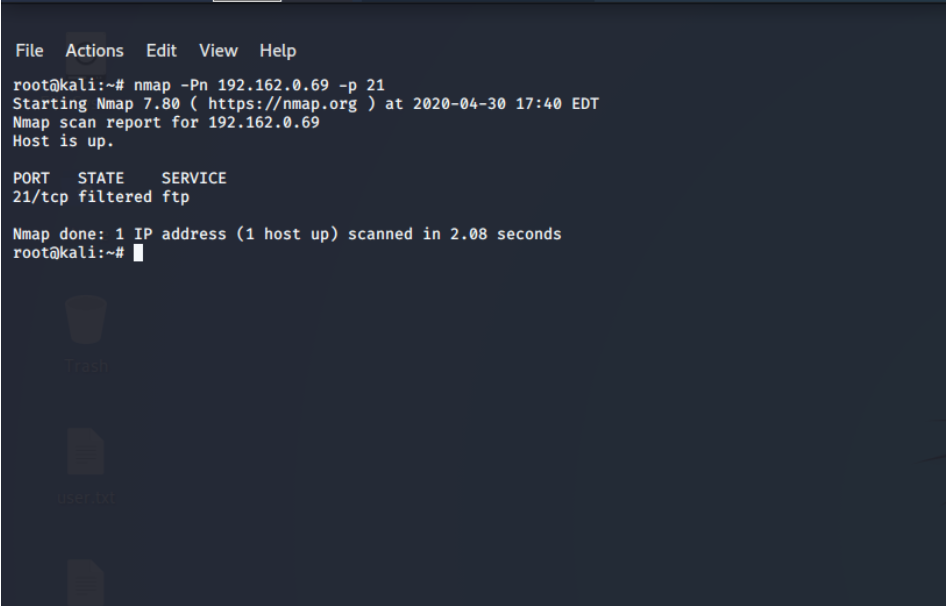


Figure 15: Scanning for open ports of metasploitable server

All the ports of the server including FTP are closed/filtered so the attacker can’t access/hack the server through its vulnerabilities.

## Attack 2: SSH Brute Force

In this attack SSH service is compromised to hack / gain access Ubuntu server.

**OS Guidance:**

Use **Kali Linux** as Attacker Machine

**Ubuntu sever** as Client Machine

### Steps to Perform Attack:

**Step 1:** Open Ubuntu server in oracle VM virtual box and execute the “ifconfig” command to know the IP of the server.

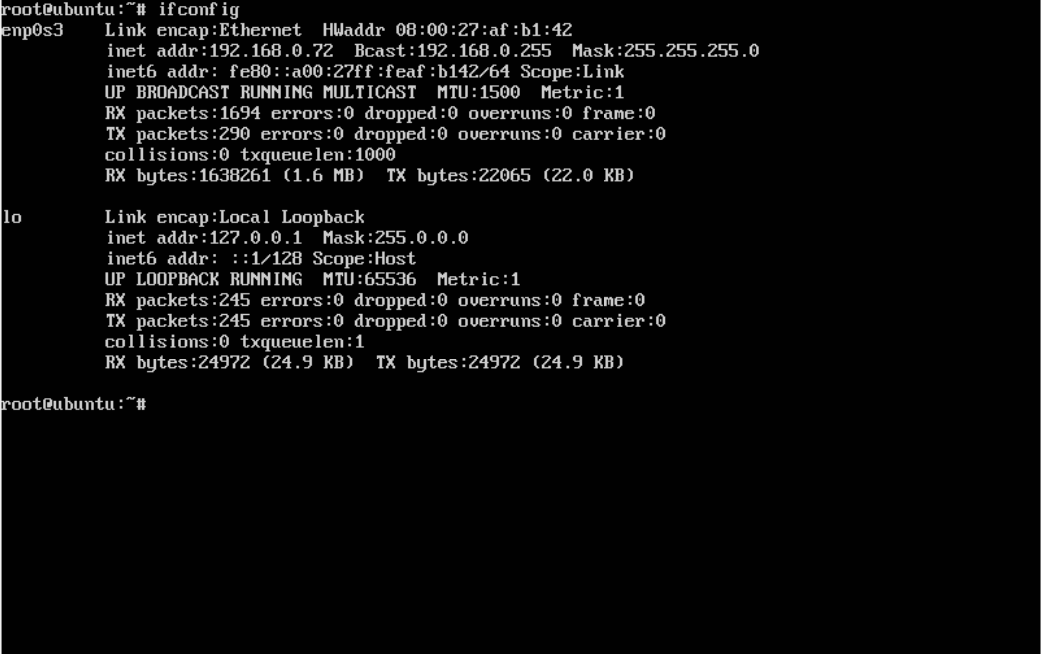


Figure 16: IP address of Ubuntu server

**192.168.0.72** is an IP address which should be recorded or retrieved

**Step 2:** Using NMAP tool in kali Linux to search open ports in Ubuntu server.

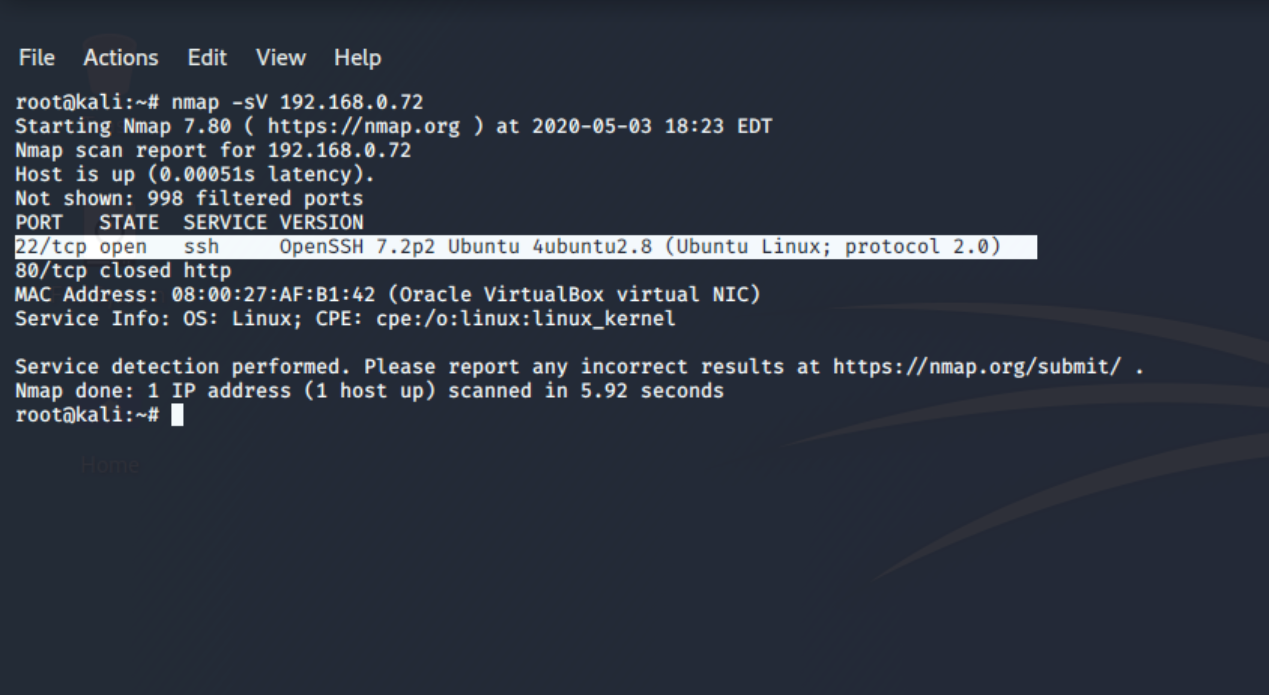


Figure 17: Port scanning with Nmap

SSH service was provided with port 22/tcp and OpenSSH edition 7.2p2

**Step 3:** Using Searchsploit to find Username Enumeration vulnerabilities.

**sudo apt update && sudo apt -y install exploitdb** are the commands used for installing the searchsploit packages manually.

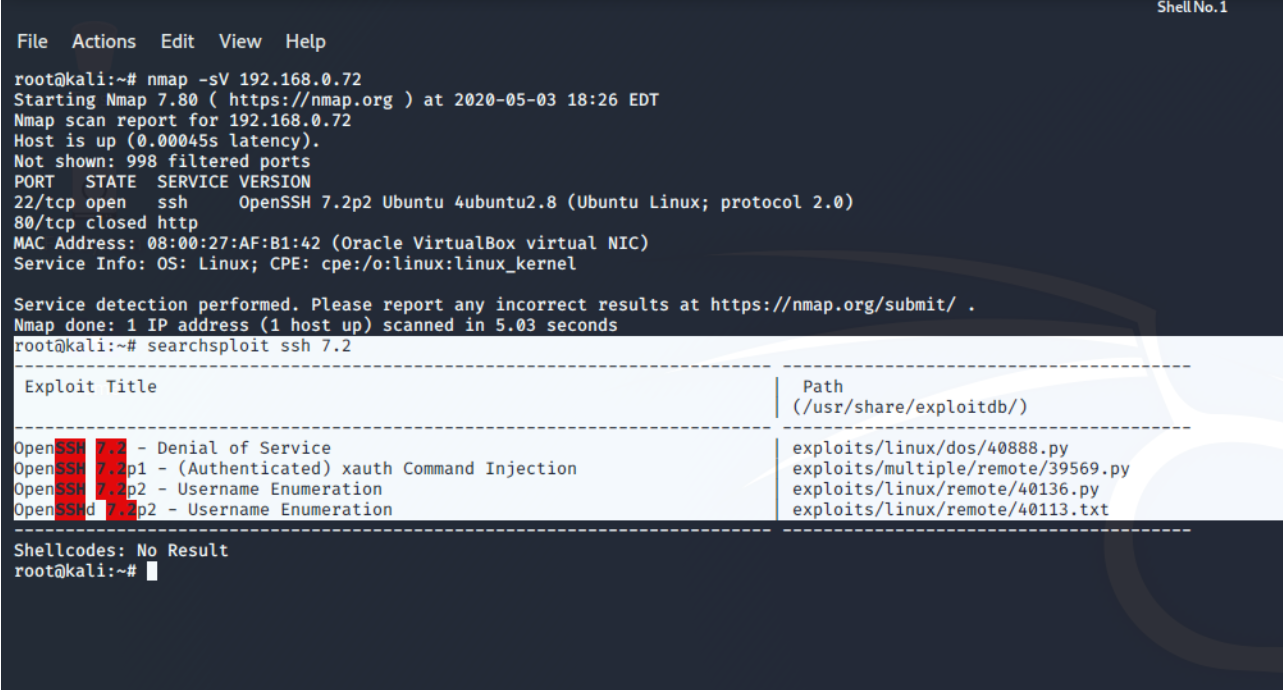


Figure 18: Using Searchsploit

OpenSSH 7.29 is vulnerable for Username Enumeration

**Step 4:** Generating random usernames and passwords for Brute force attack.

Create and store usernames and passwords in .txt format as seen in Figures 4.1 and 4.2

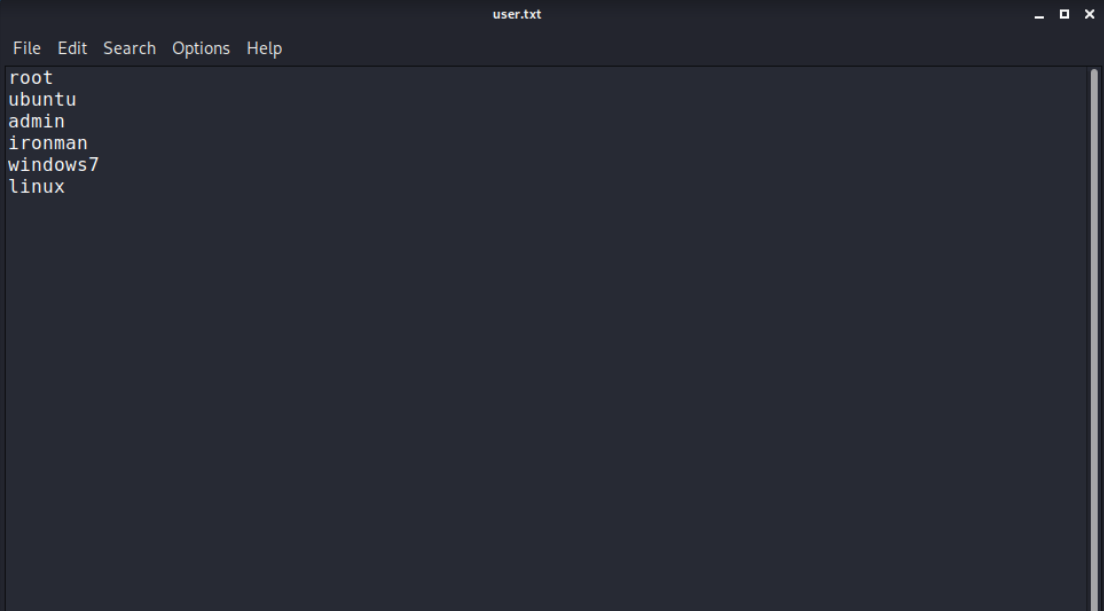


Figure 19: Creating Usernames

Crunch is utilized for the word reference making as an implicit device. The apparatus is adaptable and can make a word reference as per the cover. In the event there is a chance the client can utilize a word reference made secret key, it is smarter to utilize instant arrangement and as experience shows the most mainstream secret word is «123456»



Figure 20: Creating Passwords

**Step 5:** Using Metasploit to exploit

Execute “**service postgresql start**” and “**msfconsole**” commands in kali Linux to run database services and Metasploit.

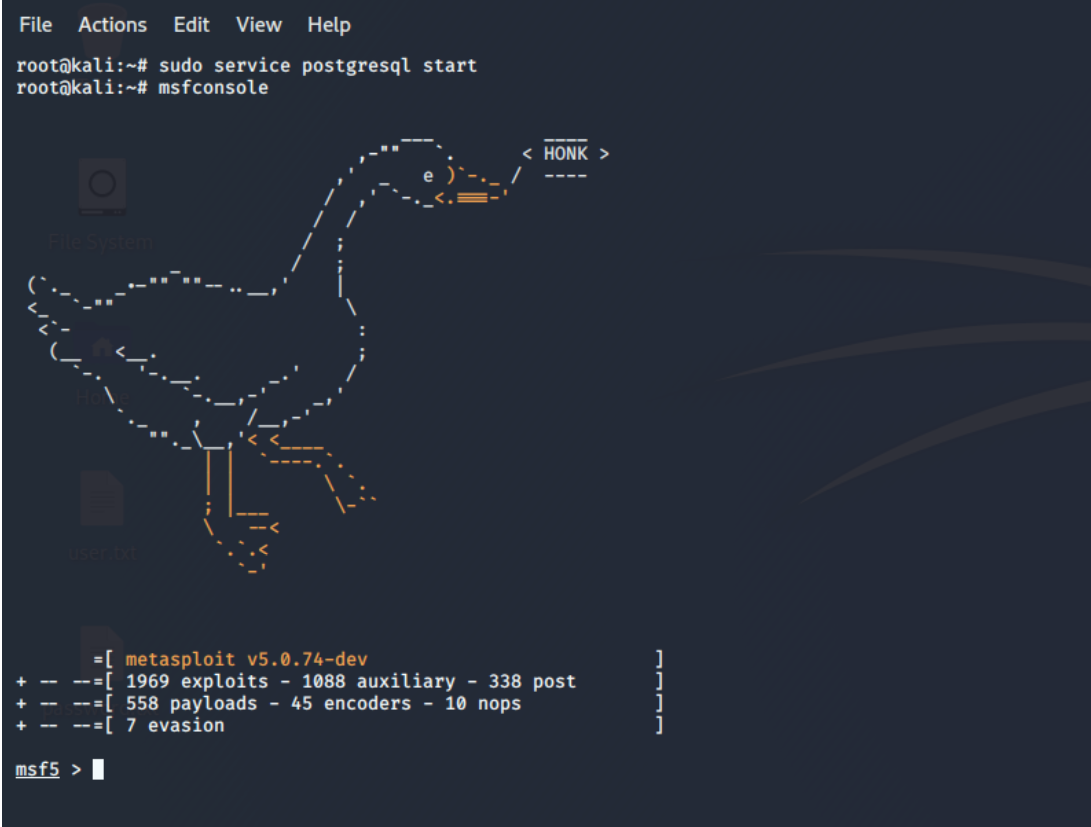


Figure 21: Running msfconsole

The module ssh\_login is used for SSH exploitation

Use **“auxiliary/scanner/ssh/ssh\_login”** command to select the module and set **RHOSTS** (indicates the target's IP address).

**“set USER\_FILE /root/Desktop/user.txt**” and “**set PASS\_FILE /root/Desktop/passwords.txt”** commands are used to break the user’s username and password which is configured in the options of msf5(Metasploit 5).

**“set STOP\_ON\_SUCCESS true”** command is used to stop finding valid credentials.

**“set VERBOSE”** command is used for displaying the attempts.

**“msf5 auxiliary(scanner/ssh/shh\_login) > options”** command is used for the module options.

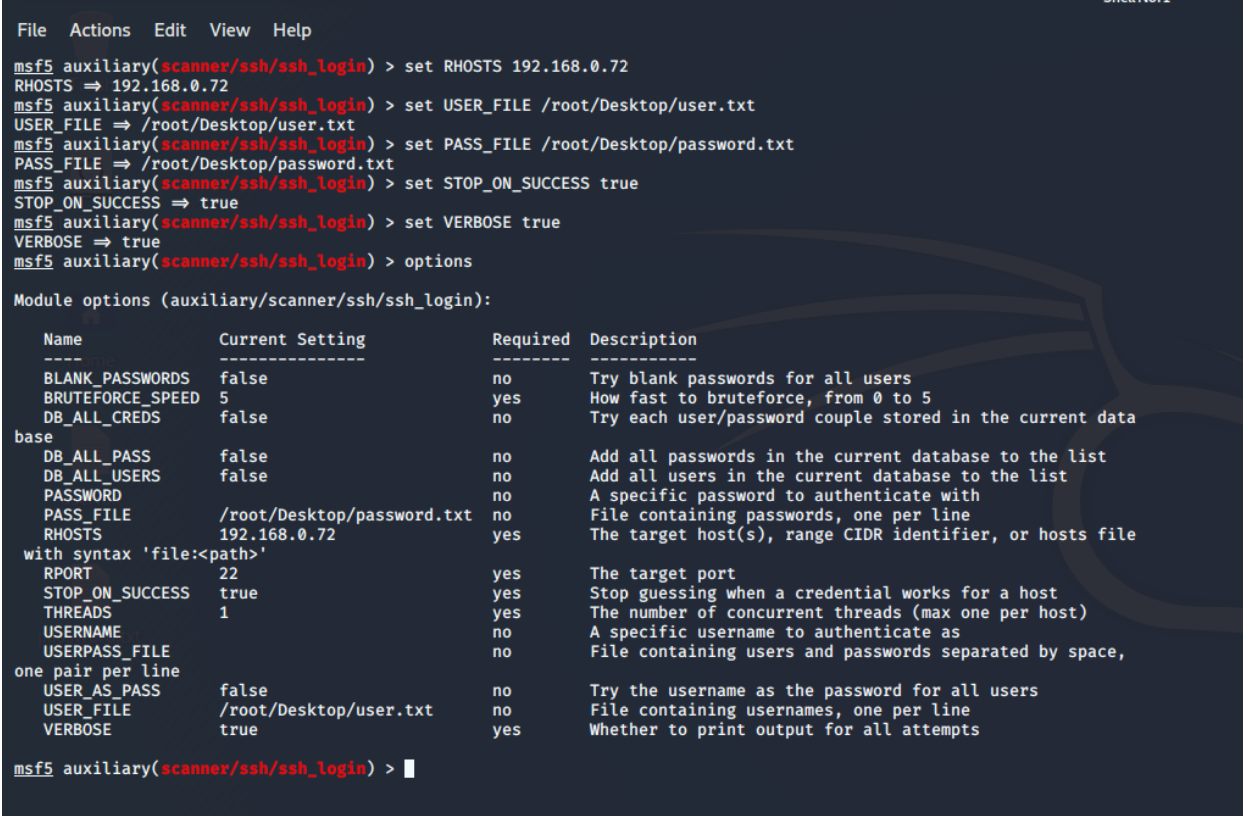


Figure 22: Setting up the host, usernames and passwords

In the above screen capture, the assailant has set the RHOSTS to 192.168.0.72 (IP of client machine) and the username list and password (that is userpass.txt).

**Step 6:** Exploiting and gaining access of Ubuntu server

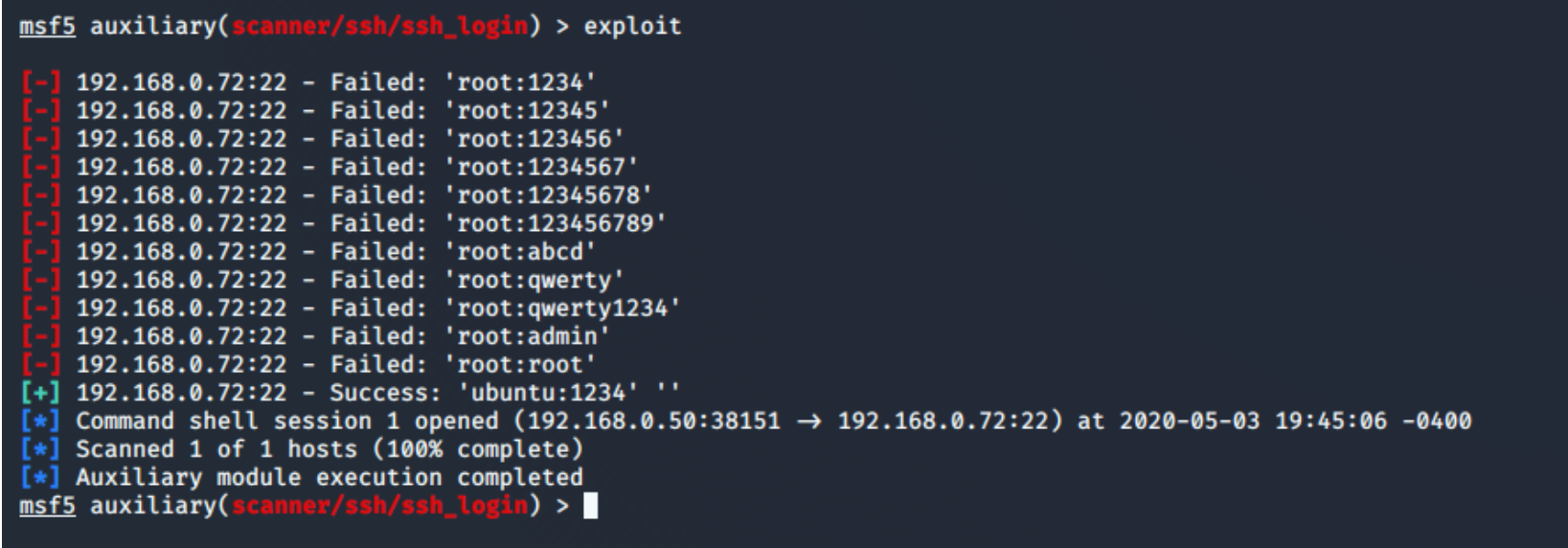


Figure 23: exploiting

**“exploit”** command is used for exploitation

A progress message is shown when valid credentials are detected, and a command shell is opened.

Metasploit will display the brute-force attempts where credentials are being tried depending on the number of usernames and passwords being used. (DRD\_, 2019)

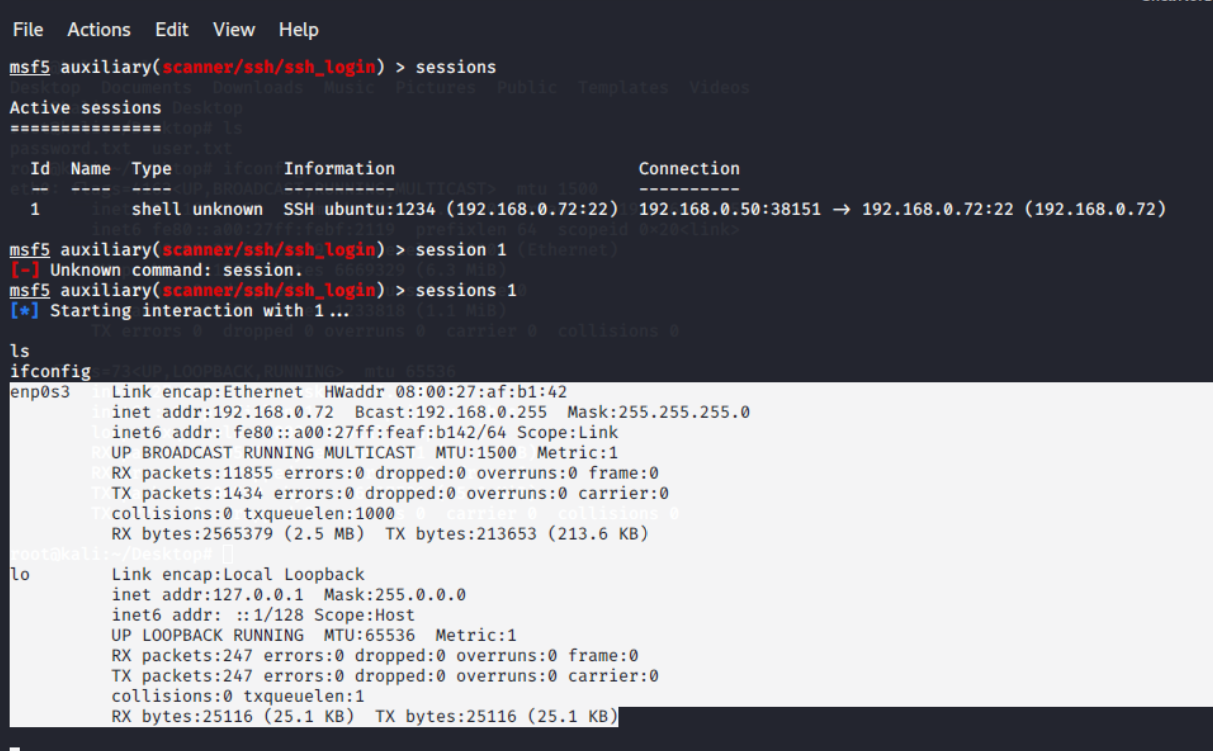
****

Figure 24: Access gained by attacker

**“sessions”** command is used for viewing the active sessions.

**“sessions -i 1”** command used for interaction with the selected session.

Via SSH, the target is connected

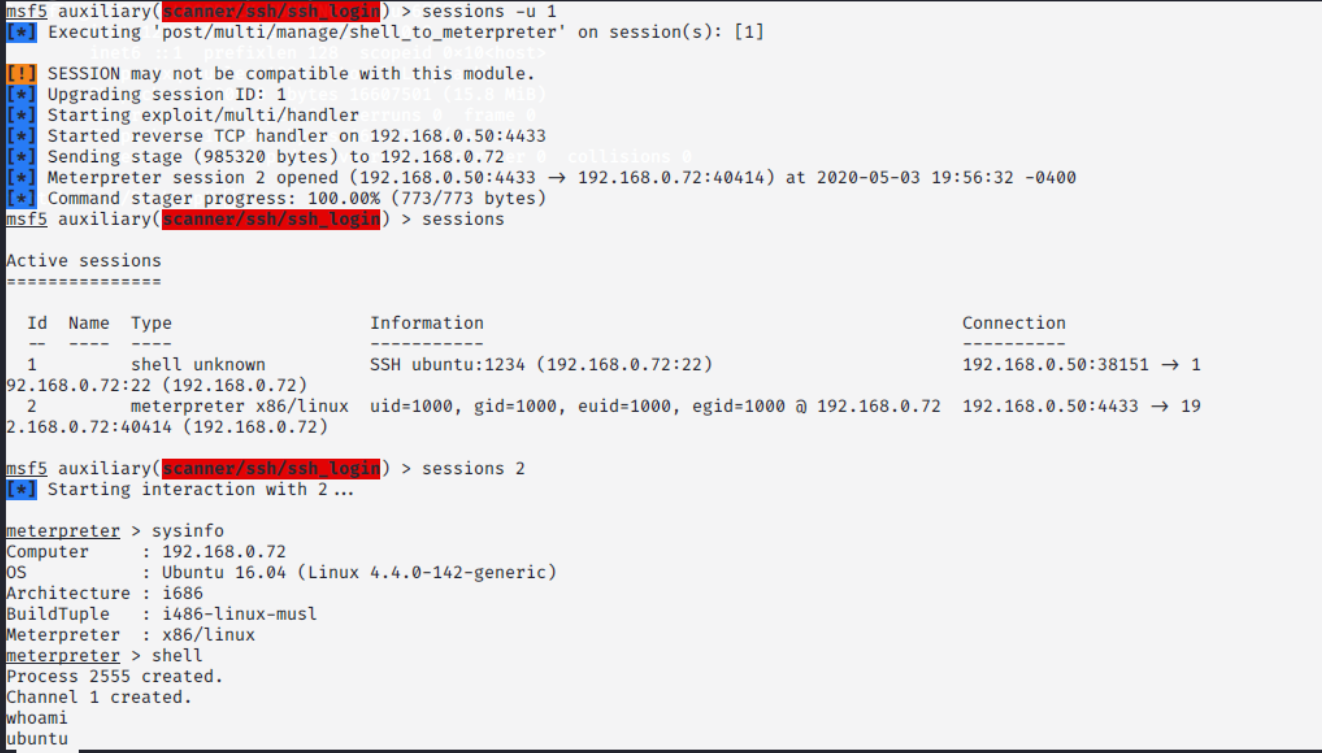
****

Figure 25: Exploring credential information of Ubuntu server

Figure 8 and Figure 9 assert attacker used SSH brute force attack and hacked ubuntu server successfully

### Countermeasures

A more secure arrangement has actualized an assistance, for example, Fail2ban, DenyHosts, or IP-tables to square brute force trials at the host level. Consolidated by using private key validation as opposed to passwords, this will be outside the control of most aggressors. (DRD\_, 2019)

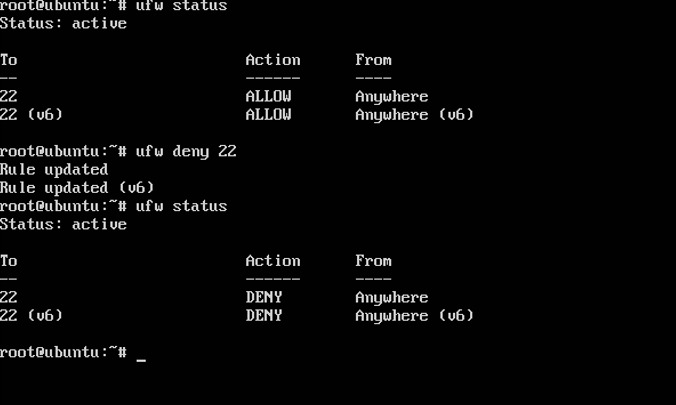
****

Figure 26: Disabling the open ports

Several critical protection measures should be regarded to help deter brute force logins:

Try not to expect root to enter, don't empower ssh qualifications (utilizing private key verification), don't tune in to either gadget, construct an SSH arrange gadget (for example eth1) that is isolated from the interface on which you handle demands (for example eth0), don't utilize explicit usernames, utilizing a grant rundown and afterward approve clients requiring SSH get to.

## Attack 3: DOS Attack on Client Machine through SSL/ms-wbt-server

In this attack **SSl/ms-wbt-server** service is compromised and perform DOS attack to crash client machine.

**OS Guidance:**

Use **Kali Linux** as Attacker

**Windows 7** as Client

### Steps to perform Attack

**Step 1:** Open windows-7 in oracle VM virtual box and execute the “ifconfig” command to know the IP address.

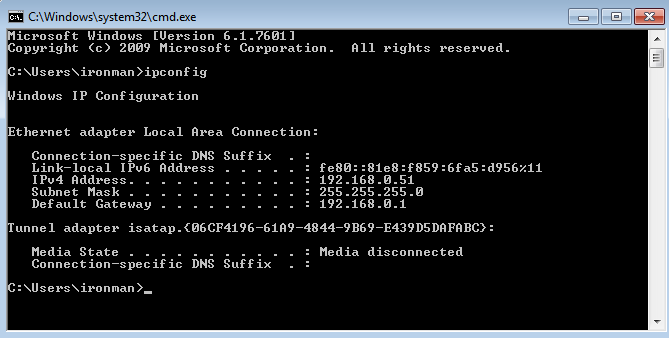


Figure 27: IP Address of Client Machine

192.168.0.51 is an IP address of client which should be retrieved.

**Step 2:** Using NMAP tool in kali Linux to search open ports of Client Machine.

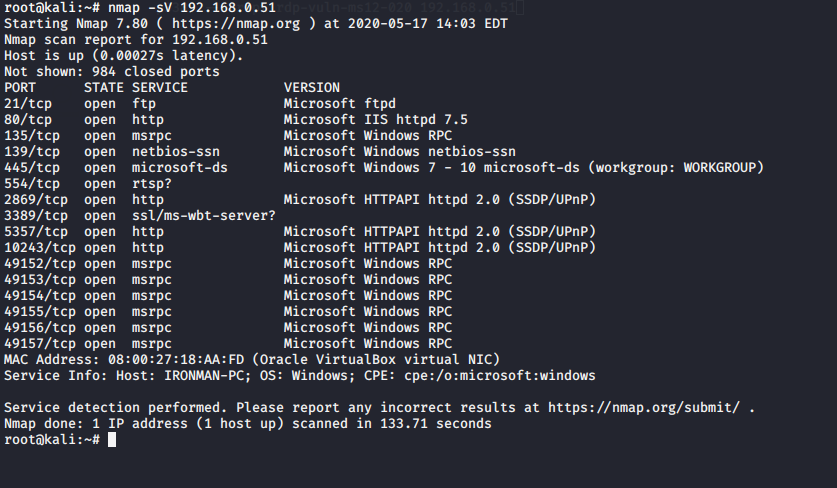


Figure 28: Port Scanning Using NMAP

**Step 3:** Using Metasploit to exploit

Execute “**service postgresql start**” and “**msfconsole**” commands in kali Linux to run database services and Metasploit.

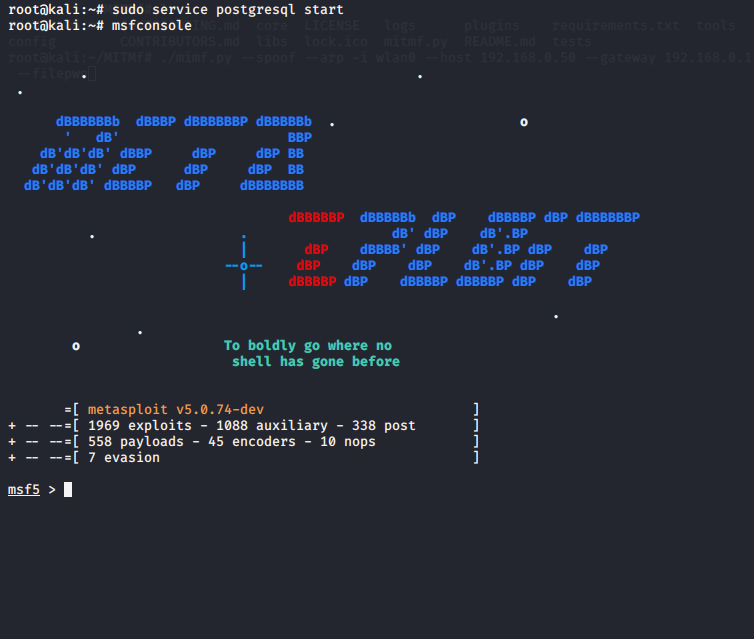


Figure 29: Running msfconsole

**Step 4:** Checking potential vulnerabilities within the Metasploit

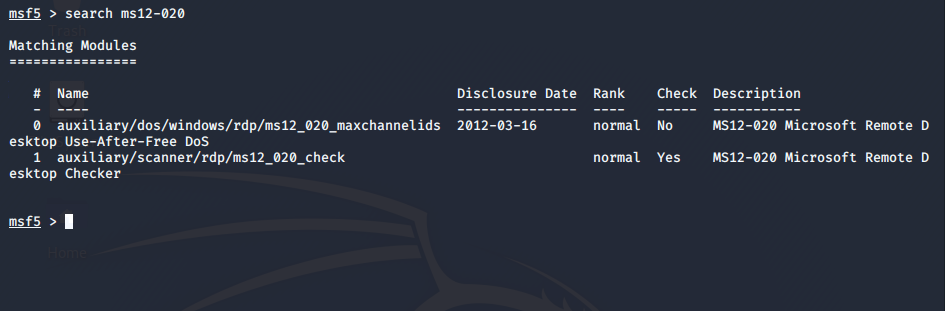


Figure 30: Setting up the host

Two vulnerabilities found for the MS12-020

**Step 5: configuring options**

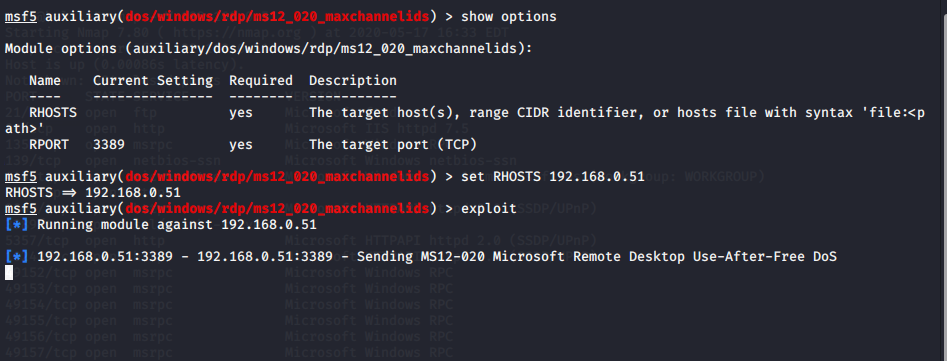


Figure 31: Exploiting

The targeted machine is known as the remote host (RHOST)

The exploit command is like trying to pull the trigger. The target machine will be fully operated with one click by the attacker

**Step 6: Crashing the Client Machine**

The client system was crashed after a successful attack, and reboots on its own

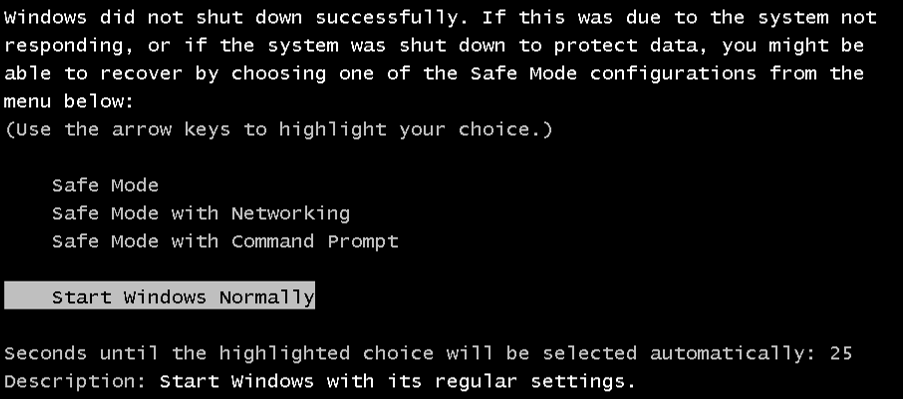


Figure 32: Client System Crashed

### Countermeasures

Configure remote property in system and security section and change the "Allow connexion from running all RDP versions" to "Allow connexion from computer running Remote Desktop with network level authentication only."

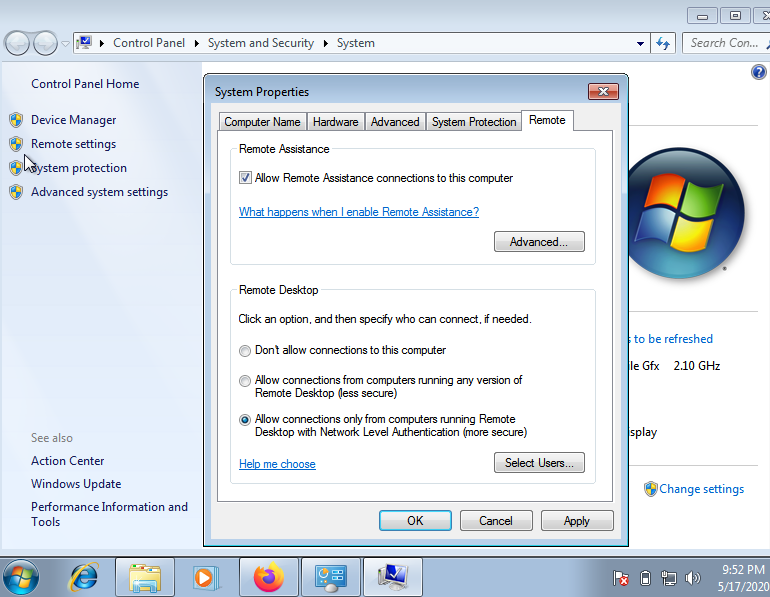


Figure 33: Configuring the Vulnerability

## Attack 4: Phishing User Credentials with BlackEye

# 

Phishing is a digital assault that utilizations masked email as a weapon. The objective is to fool the email beneficiary into accepting that the message is something they need or need a solicitation from their bank, for example, a note from somebody in their organization and to click a connection or download a connection. Social media accounts are the most loved objective for hackers and the best strategies for assaulting accounts on sites. These secret key taking assaults depend on fooling clients into entering their passwords into a persuading counterfeit website page.

**OS Guidance:**

Use **Parrot OS** as Attacker

**Windows7** as Victim

### 

### Steps to perform Attack

**Step 1: Downloading BlackEye in Parrot OS**

In the first place, clone the source from BlackEye's GitHub archive.

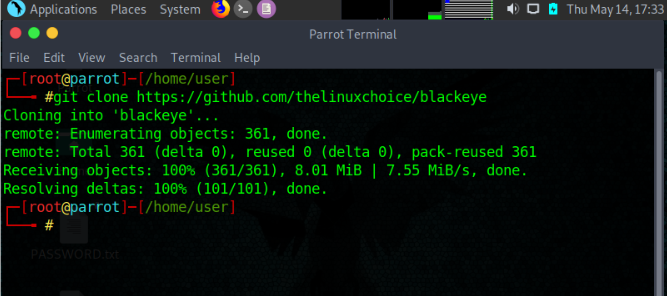


Figure 34: Installing BlackEye

**Step 2: Explore the options of phishing page**

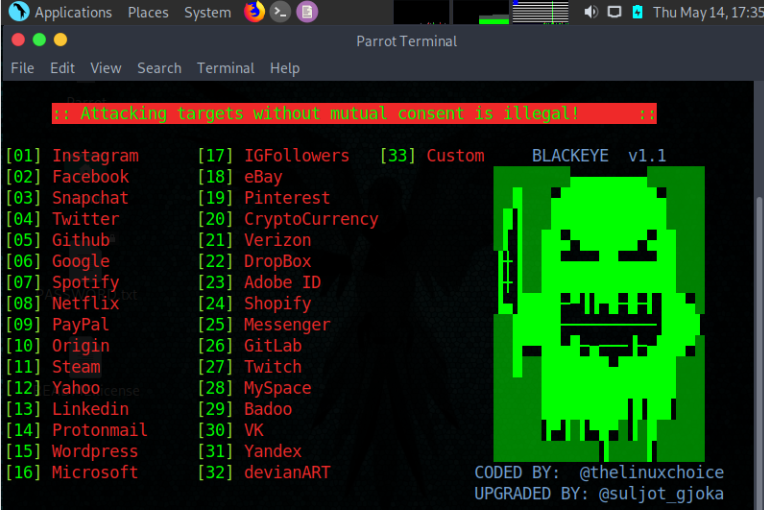


Figure 35: Options provided by Tool

To begin a phishing page, open a terminal window and explore to the blackeye organizer and select any one module.

**Step 3: Configuring the Module**

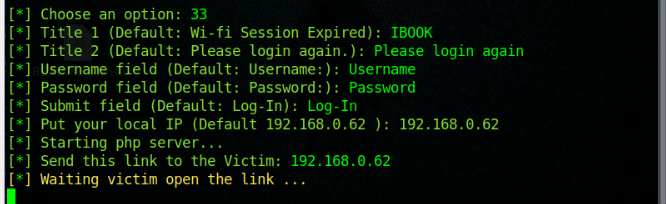


Figure 36: Configuring

Subsequent to doing social engineering assailant will know the interests of the person and do phishing appropriately. For instance, Consider IBOOK as an acclaimed web-based life application. The assailant will make a phony login page equivalent to the first one and steel the username and secret phrase of the casualty as appeared in the above figure.

**Step 4: Creating an application to send Anonymous email**

Make an Anonymous email sender application with PHP and HTML codes and a Server to host the site/application.

PHP code:



Figure 37: Code for creating application

At long last anonymous email sending application was created

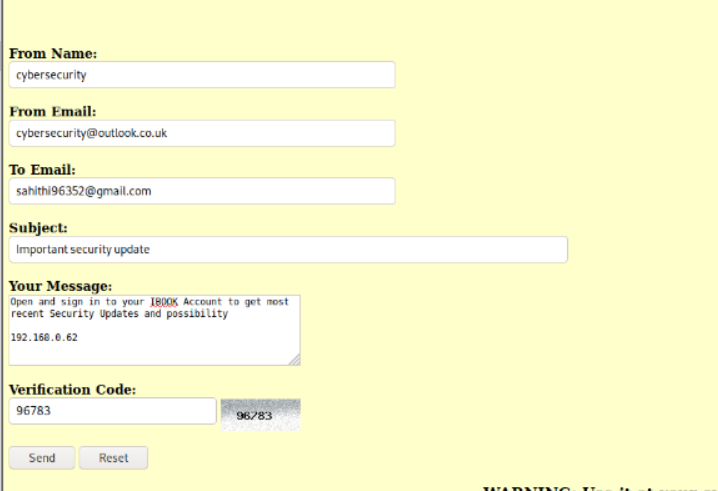


Figure 38: Application That Sends Anonymous Email

**192.168.0.62** is the phishing link attached to mail with a message.

**Step 5: The Victim received the mail send by the Attacker.**



Figure 39: Email received by Client

“Open and sign in to your IBOOK account to get most recent security updates and possibilities” was the message send by the attacker.

Figure 31 is the output when the Victim click the link send by the Attacker.

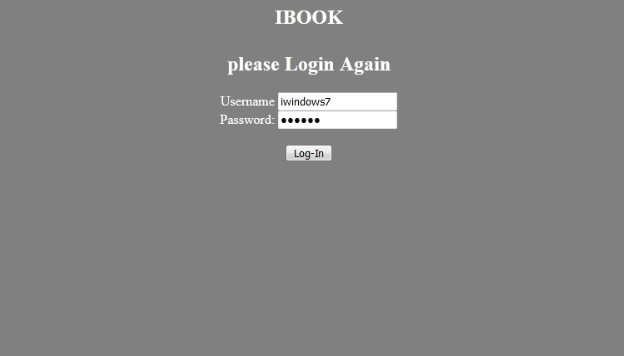


Figure 40: Entering Username and Password

Opening the connexion causes the script to return information about the type of devices currently accessing the phishing page

If the target enters credentials and clicks on login, the web page is redirected to the actual IBOOK website, creating the impression of a productive login.

**Step 6: Exploiting Credentials**

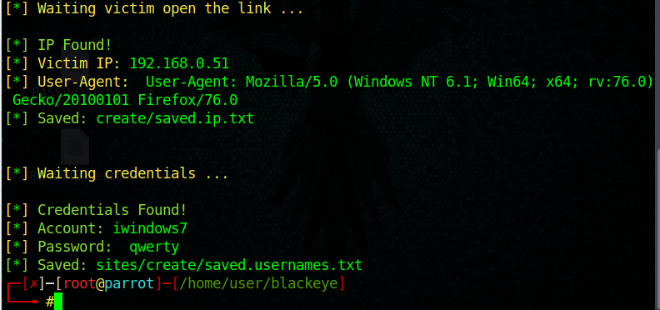


Figure 41: Exploiting

BlackEye tool provide the user credentials when the victim enters the username and password through phishing link

### Countermeasures:

Enable two-factor account login authentication and use a hardware security key to allow new devices to use key to log in.

## References

adminVRT, 2016. *100+ Free Hacking Tools To Become Powerful Hacker*.

Amir, S, 2017. *Penetration Testing of an FTP Server*.

DRD\_, 2019. *Gain SSH Access to Servers by Brute-Forcing Credentials*.

# PART-B

**DNS Attack at GitHub**

## ****Abstract****

The paper focuses on cyber-attack at GitHub, which was due to a denial of service (DNS). The focal point of the report depends on the executed systems and strategies for the disposal of difficulties and control of negative effects as required. Strategically, the report focuses on analytical perspectives of the case and the issues associated with the attacks. Also, the countermeasures that the organization took to challenge the situation was implemented in a better way to assist in the control of the challenges. Based on the applied policies of the company, the report is focused on the elimination of challenges associated with the DNS attacks and measures implemented to reduce the chances of occurrence and other issues that may challenge the occurrence and negative impacts as well.

## ****Introduction****

GitHub, as a company, has faced a number of security challenges that lead to deterioration of the services that they offer. The worst security compromise was the 2018 February cyber-attack that led to the denial of services (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). As a security compromise, the challenge led to slowed services and poor processing power of the information hence compromising the quality and effective measures identified for the promotion and execution of the services. The following report is based on the denial of service (DNS) attack and how it occurred in the organization. Additionally, the focus is laid on the adverse consequences of the attack and the challenges that reduced the quality strategies and compliance with the services as recommended (Burnton 2019, pp. 1-25). Strategically, the attacks were good, and additional measures were necessary to assist in combating crime.

The scope of the cyber-attack report is an exploration of the severity of the attacks based on the challenges that the company experienced and the issues that inspired the attackers to execute the evil act (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). As a strategy, the promotion of better services as required to assist in the diagnosis of the challenge in the serves of the company to reduce the challenge. Also, the selection of the attack is based on the technique, which is hacking and channeling of data hence denying essential services. DNS attacks are common, and as a technique of cyber-attack, it can be considered a significant challenge that existed, and the issue led to adversity and contrary to what was expected (Burnton 2019, pp. 1-25). Negativity was the consequence of the entire attack and led to the adversities reported in the company in February 2018. The following is a critical analysis of the negative impacts of the DNS attack and the countermeasures that were implemented to rescue the organization from the negative issue.

## ****The DNS Attack at GitHub****

As a company, GitHub is renowned for online code management for developers in computer technology (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). The company deals with data traffic and manages requests from various sources and individuals who need services for quality operations as required. Strategically, the company has been focused on a number of years to total and quality services to assist in the regulation of challenges and control of adversities. GitHub is a company that has been stable for years when it comes to services of code management, and the security has been robust.

The DNS attack occurred in February 2018 and compromised the operations since there was sudden traffic of data at a rate of 1.3 Tbsp (Cekerevac et al., 2017, pp. 166-172). In the servers that were anomalous. In the history of server data traffic, the case of GitHub was unique and resulted in issues that were difficult to explain hence the challenge as difficult. As a strategy to reduce the adversity, it was good to ensure that essential approaches are implemented for control of the traffic (Burnton 2019, pp. 1-25). At the time of the attack, there was a data packet flow each second of 126.9 million that exhausted the servers and altered the usual operation and compromised the required services. The challenge was adverse and led to the consequences that were observed (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). Management of the services by the company was difficult, and it could not satisfy the needed requests hence the adversity that was seen. Denial of service was experienced since the company as shut down, and no requests could be processed. There was an announcement that GitHub was unavailable for some time since there was an excessive flow of data traffic that rendered the services useless, and the challenges were adverse (Cekerevac et al., 2017, pp. 166-172). Unavailability as a result of the malicious parties who hacked and started a high-frequency data flow and compromised the systems hence reducing the effectiveness of the techniques and strategies as recommended.

## ****Critical Discussion, analysis, and reflection****

DNS attacks are rare, but when they occur, challenges occur, and adversities are reported hence reducing the competence of the affected companies (Burnton 2019, pp. 1-25). As a result, there are challenges and issues that compromise the quality and operational techniques required. Based on the techniques required for sending information in specific media, it becomes a bigger problem inevitably to solve the situation. For the case of GitHub, there was distributed denial of service due to large data traffic originating from different sources and causing adverse impacts contrary to what was expected (Burnton 2019, pp. 1-25). The company was at a standstill since the critical online code service management was blocked, and requests from legitimate customers were blocked. Deliberately, it was important to follow a decent approach and guarantee that vital mediations are followed for the disposal of difficulties and the advancement of a decent methodology fundamental for the decrease of afflictions as suggested.

An attack is originating from a single source is easy to identify and bloom for operations to proceed as normal (Cekerevac et al., 2017, pp. 166-172). GitHub experienced distributed denial-of services, and the challenge was adverse, making the issues adverse and poor-quality techniques led to a poor-quality strategy. Basically, there was a need to follow a strategic intervention to intercept the perpetrators and reduce the rate and incidence of attacks. Denial of Service is the worst complication in the servers since the usual processing speed is hampered, and alternative techniques have resorted that reduce the quality and the techniques that are required for quality and strategic interventions.

The cyber-attack was due to spoofing and a channeled attack that reduced the quality and compliance strategy as recommended (Burnton 2019, pp. 1-25). Based on the strategies of the attackers, it was difficult to detect the course of action and take a good measure. There was an amplified traffic flow that was channeled through the servers and limited the organizational strategy to mitigate the risks. Denial of service (DNS) attack so far remains a challenge and an issue that must be effectively applied to assist in the elimination of challenges and reduction of adversities to amply the strategic measures of control. Basically, the needed policies are good and effective measures necessary for the elimination of adversity in the information systems.

Critically, the processing of requests was delayed, and there was temporary sabotage in the company since the attackers targeted critical services that relate to the customers' services (Cekerevac et al., 2017, pp. 166-172). In the best interest of the organization, it was difficult to discern a good course of action and reinforce strategic measures to control the challenges. A good server must have a quality of speedy processing power to assist in the resource acquisition and elimination of adversities. As an intervention, it was difficult to apply the best service and ensure that challenges are controlled and better approaches implemented in the DNS attack control.

Based on the incident, the company was down for 20 minutes without any meaningful operational techniques (Cekerevac et al., 2017, pp. 166-172). There was a need to successfully implement strategies and follow a good policy in the reduction of challenges and promotion of better measures as require. The DNS services blocked all the spots of data processing in the website, making the organization to be sluggish. A policy to ensure that the challenges were reduced was the implementation of an analytical plan to reinforce the basic avenues and policies for the elimination of spoofing and DNS attacks. The congestion of the websites was regarded as the most fundamental issue that reduced the competence of information processing and compelled the drastic change (Burnton 2019, pp. 1-25). Since a number of processes slowed down and had to come to a halt, it was more difficult for the organization to work normally.

DNS attack at GitHub led to losses of billions of shilling since a number of crucial and vital services were put to a halt (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). Challenges are resulting from poor strategies and reduced approaches to the offered clients reduced. Strategically, there was a need to ensure that basic approaches were applied to reduce the challenges and ensure that competent strategies are applied as required. Sabotage was also among the challenges that reduced the competence and capacity of the information system to hold the required data within the desired time. Among the challenges affecting the critical infrastructure were the issues of strategic importance and regarded quality that was necessary for solving the challenges and reduction of the approaches for control of the bad strategies as well. Distributed denial of access also lowered the competence of the organization to focus on the reinforcement of better services hence limited the necessary quality for control of the challenges as recommended.

## Methodology

Secondary data has been gathered for the examination to comprehend issues of cyber-attacks at GitHub and the techniques for alleviating. Auxiliary information will be gathered through journals, news articles. Valid, reliable, and accurate information have been gathered for the examination to get an appropriate conclusion.

## ****Countermeasures for DNS attack at GitHub****

A team of competent information system analysts were deployed by the company to check the issue and worked to resolve the challenge within the shortest time possible (Medvedovsky and Aviv, Radware Ltd, 2019, 1-8). Since there were a number of weaknesses in the information system, it was possible to detect the source of malicious parties and work to resolve the challenge in a more critical way. Substantial strategies are recommended for eliminating adversity and reduction of the challenges to promote better services and required approaches for the elimination of adverse situations (Cekerevac et al., 2017, pp. 166-172). DNS attack was planned, and the countermeasures focused on the reduction of the consequences as well as finding the best solution to provide temporary but necessary service delivery.

Another option was the installation of firewalls to assist in the elimination of challenges and control of adversities as recommended (MALISENCU 2019, 1-2). Based on the applied principles, it was good to strategically employ the best intervention and control the challenges of porosity to the network and servers. As a security architecture plan, firewall implementation was put into effect to control the adverse effects and ensure that quality interventions are applied for control of the challenges as required (Masuda, Segawa and Mori, 2019, pp. 34-40). A blocking chain of attack was a good strategy employed by the company to reverse the situation and control the bad outcomes.

Surveillance was also implemented whereby spyware programs were implemented to check for the presence of any personnel or individual who could have breached the required information system (Cekerevac et al., 2017, pp. 166-172). Recommended strategies focused on policy implementation and reduction of challenges to assist in the elimination of challenges. Based on the applied policies, it was good to follow an effective implementation so that surveillance programs could work as recommended (Cekerevac et al., 2017, pp. 166-172). Based on the applied policies, it was necessary to work on a strategy of execution whereby the better programs are followed for effective implementation and reduction of negativity in a bid to control the adversity (Mahjabin and Xiao, 2019, pp. 1-2). The company was focused on delivering the right security as recommended to reduce the chances of bad consequences and the challenges that could cause negative concerns.

Reinforcing the network security status of GitHub was a good policy that was implemented to control the adversity and ensure that the challenges are effectively mitigated (Burnton 2019, pp. 1-25). Some of the major issues that led to control of the challenges included an adjustment of the security system to counteract DNS at all levels and ensure that the best interventions are applied for the reduction of the challenges associated with security.

## ****Conclusion****

The DNS attack at GitHub is among the challenges that affected the company in 2018 since it led to alteration of the services and reduction of the quality services as recommended. Based on the issues that were applied, it was good enough for strategic control and elimination of challenges as required. In a better way, there was a strategic policy to ensure that the issues were effectively applied and better policies implemented as recommended. The DNS reduced the effectiveness of the services offered by the company since most of the customers were locked out.

## References

Burton, R., 2019. Characterizing Certain DNS DDoS Attacks. *arXiv preprint arXiv:1905.09958*. 1-25.

Cekerevac, Z., Dvorak, Z., Prigoda, L. and Cekerevac, P., 2017. Techno-Economic Aspect of the Man-in-the-Middle Attacks. Communications-Scientific letters of the University of Zilina, 19(2), pp.166-172.

Mahjabin, T. and Xiao, Y., 2019, January. Mitigation process for DNS flood attacks. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-2). IEEE. 1-2.

MALISENCU, D., 2019. Attacks analyze in the computer networks. 1-2.

Masuda, H., Segawa, S. and Mori, M., 2019. Proposal and Prototype of DNS Server Firewall with Flexible Response Control Mechanism. *International Journal of Networked and Distributed Computing*, *8*(1), pp.34-40.

Medvedovsky, L. and Aviv, D., Radware Ltd, 2019. *Techniques for defense against domain name system (dns) cyber-attacks*. U.S. Patent Application 15/940,371. 1-8