Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Cyber Threats

A **Cyber threat**

- is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.

- refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.

- **Most common cyber threats**: Social Engineered Trojans, Unpatched Software, Phishing, Network worms, etc.

Cyber Threats Sources

- Anyone with a motive and the needed technology can create cyber threats.

- Cyber threats can come from a wide variety of sources, some notable examples include:
    - National governments.
    - Terrorists.
    - Industrial secret agents.
    - Rogue employees.
    - Hackers.
    - Business competitors.
    - Organization insiders.

Cyber Threat Classifications

- Threats can be classified by multiple criteria:
    - Attacker's Resources
    - Attacker's Organization
    - Attacker's Funding

- On basis of these criteria, threats are of 3 types:
    - Unstructured Threats
    - Structured Threats
    - Highly Structured threats

Unstructured Cyber Threats

- **Resources:** Individual or small group.
- **Organization:** Little or no organization.
- **Funding:** Negligible.
- **Attack:** Easy to detect and make use of freely available cyberattack tool.
- Exploitation based on documented vulnerabilities.

Structured Cyber Threats

- **Resources:** Well trained individual or group.
- **Organization:** Well planned.
- **Funding:** Available.
- **Attack:** Against particular individual or organizations.

❖

- Exploitation based on information Gathering.

Highly Structured Cyber Threats

- Extensive organization, resources and planning over time.

- Attack: Long term attack on particular machine or data.

- Exploitation with multiple methods:
    - Technical, social and insider help.

Cyber Security Threat Index Level

- Cyber threats are evaluated daily by the CTU (counter threat unit) and associated with a threat index level.
- The indicator shows the current level of malicious cyber activity and reflects the potential for, or actua damage.
- The threat index levels are:
  - Low
  - **Blue or Guarded**
  - **Elevated**
  - **High**
  - **Severe**

Cyber Security Threat Index Level

- **Green or Low:** indicates a low risk

- **Blue or Guarded:** Indicates a **general risk** of increased hacking, virus or other malicious activity.
  - The potential exists for malicious cyber activities,
    - but no known exploits have been identified or
    - known exploits have been identified but no significant impact has occurred.
- **Yellow or Elevated:** Indicates a significant risk
- There are known vulnerabilities that are being exploited wit a moderate level of damage/disruption or
- The potential for significant damage or disruption is high.

Cyber Security Threat Index Level

Orange or High: Indicates a high risk of increased hacking, or any other malicious cyber activity which

- targets or compromises core infrastructure,
- causes multiple service outages, multiple system compromises or compromises critical infrastructure
- At this level, vulnerabilities are being exploited with high level of damage or disruption or the potential for severe damage or disruption is high.

Cyber Security Threat Index Level

Red or Severe: Indicates a severe risk of increased hacking, virus or any other malicious cyber activity which

- results in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or weakens one or more critical infrastructure sectors.
- At this level, vulnerabilities are being exploited with severe level or wide spread level of damage or disruption of Critical Infrastructure Assets.

Offensive Security & Defensive Security: Labs

Resource:
https://tryhackme.com/

Offensive Security?

- The process of **breaking into** computer systems, exploiting software bugs, and finding loopholes in applications to gain **unauthorized access** to them.

- To beat a hacker, you need to behave like a hacker,
  - **finding** vulnerabilities and **recommending** patches before a cybercriminal does!

- Red Teams

Defensive Security?

- The process of **protecting** an organization's network and computer systems by **analyzing** and **securing** any potential digital threats;

- **Investigating** infected computers or devices to understand
  - how it was hacked,
  - tracking down cybercriminals, or
  - monitoring infrastructure for malicious activity.
- Blue teams

First Hack

- to hack a fake bank application called FakeBank
- use a command-line application called "GoBuster" to brute-force FakeBank's website
  - to find hidden directories and pages
- GoBuster takes a list of potential page or directory names and tries accessing a website with each of them
  - If page exists, it informs

First Hack

1. **Open terminal** on the machine
2. Find hidden website pages

```
gobuster -u http://fakebank.com -w wordlist.txt dir
```

```
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wo
rdlist.txt dir

===============================================================
Gobuster v2.0.1                OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://fakebank.com/
[+] Threads      : 10
[+] Wordlist     : wordlist.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
===============================================================
2024/01/21 04:50:27 Starting gobuster
===============================================================
/images (Status: 301)

/bank-transfer (Status: 200)

===============================================================

2024/01/21 04:50:36 Finished
```

First Hack

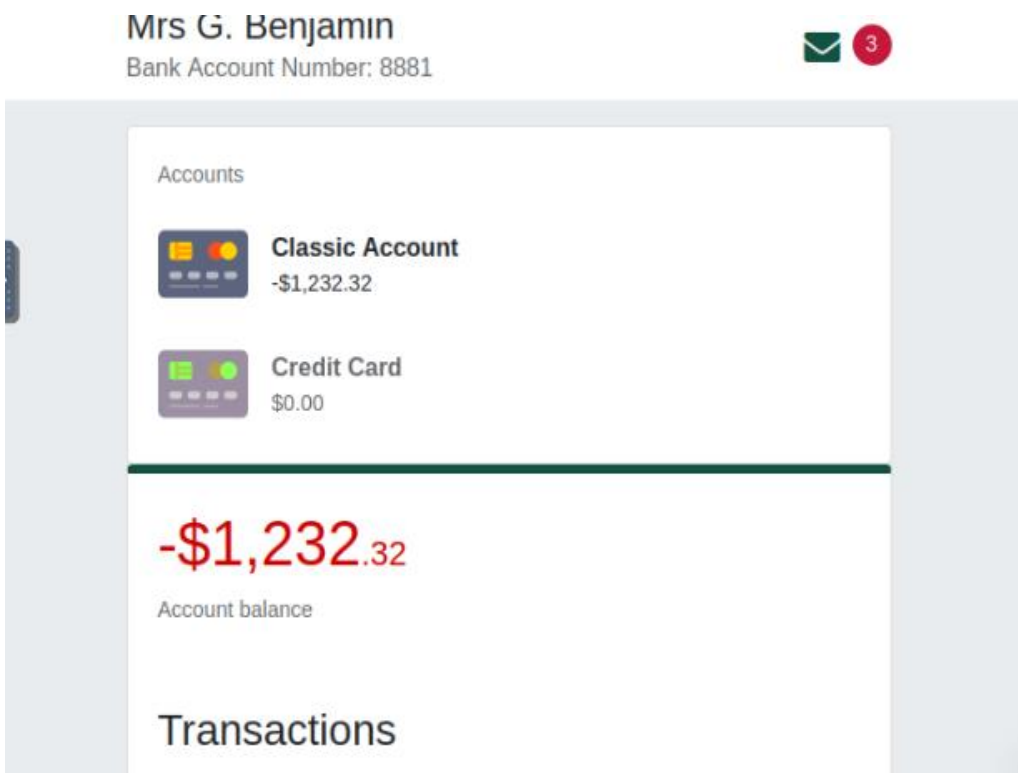
- **-u** is used to state the website we're scanning,
- -w takes a list of words to iterate through to find hidden pages.
- GoBuster scans the website with each word in the list
  - finding pages that exist on the site
- GoBuster will have told you the pages it found in the list of page/directory names (indicated by Status: 200).

First Hack

- a secret bank transfer page that allows you to transfer money between accounts at the bank (/bank-transfer) is found

- **Hack the Bank:** Type the hidden page into the FakeBank website on the machine.

Fakebank.com/bank-transfer



Defensive Security

it is concerned with two main tasks:

- Preventing intrusions from occurring
- Detecting intrusions when they occur and responding properly

- Blue teams

Defensive Security Tasks

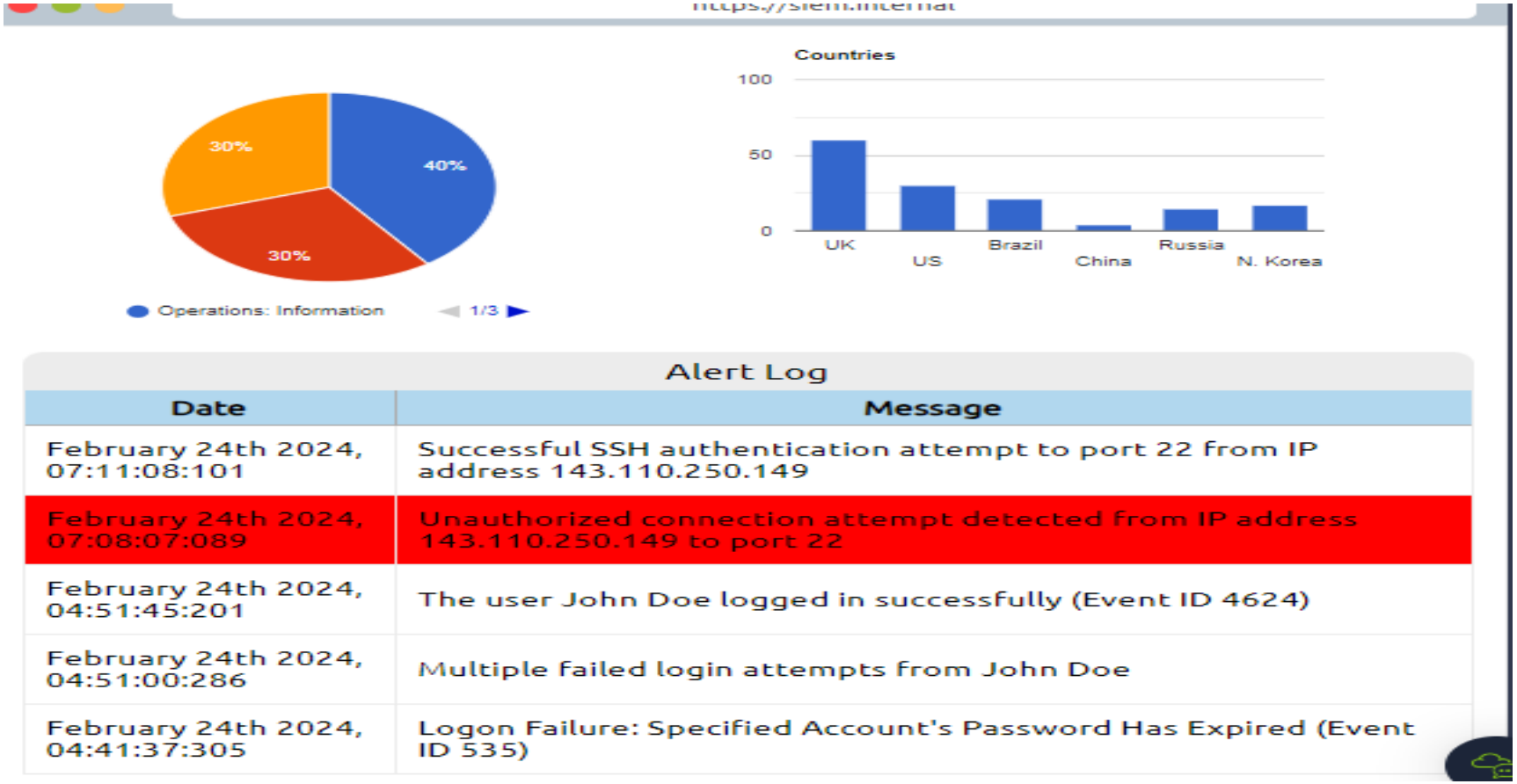
- **User cyber security awareness:** Training users about cyber security helps protect against various attacks that target their systems.
- **Documenting and managing assets:** We need to know the types of systems and devices that we have to manage and protect properly.
- **Updating and patching systems:** Ensuring that computers, servers, and network devices are correctly updated and patched against any known vulnerability (weakness).

Defensive Security Tasks

- **Setting up preventative security devices:** firewall and intrusion prevention systems (IPS) are critical components of preventative security.
  - Firewalls control what network traffic can go inside and what can leave the system or network.
  - IPS blocks any network traffic that matches present rules and attack signatures.
- **Setting up logging and monitoring devices:** Without proper logging and monitoring of the network, it won't be possible to detect malicious activities and intrusions. If a new unauthorized device appears on our network, we should be able to know.

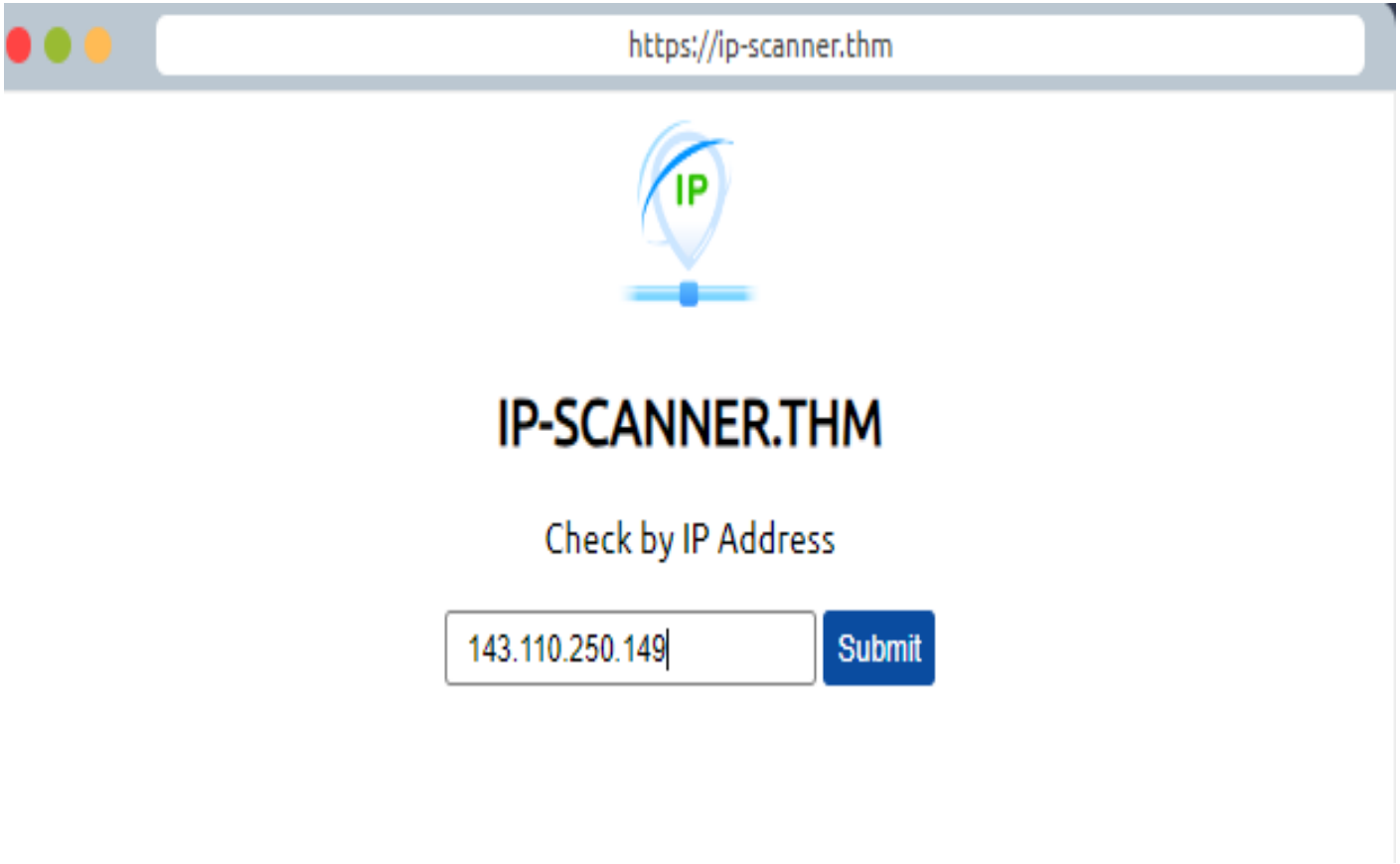
Defensive Security: Example

Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make a note of it, and then click on the alert to proceed.



Defensive Security: Example

There are websites on the Internet that allow you to check the reputation of an IP address to see whether it's malicious or suspicious.



Defensive Security: Example

There are many open-source databases out there, like AbuseIPDB, and Cisco Talos Intelligence, where you can perform a reputation and location check for the IP address. Most security analysts use these tools to aid them with alert investigations. You can also make the Internet safer by reporting the malicious IPs, for example, on AbuseIPDB.

Defensive Security: Example

Now that we know the IP address is malicious, we need to escalate it to a staff member!

We shouldn't worry too much if it was a failed authentication attempt, but you probably noticed the successful authentication attempt from the malicious IP address. Let's declare a small incident event and escalate it. There is some great staff working at the company, but you wouldn't want to escalate this to the wrong person who is not in charge of your team or department.

Sales Executive

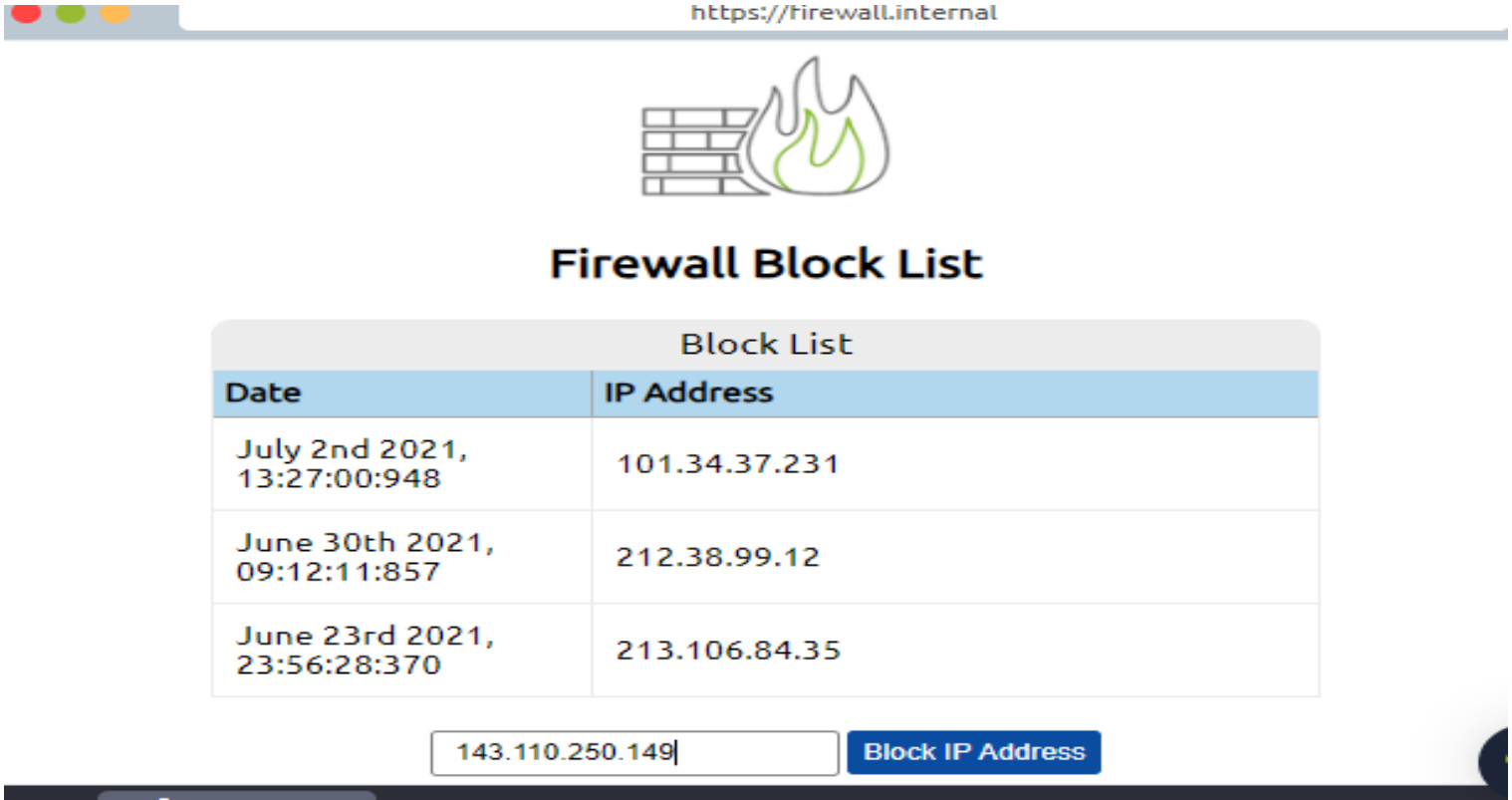
Security Consultant

Information Security Architect

SOC Team Lead

Defensive Security: Example

You got the permission to block the malicious IP address, and now you can proceed and implement the block rule. Block the malicious IP address on the firewall and find out what message they left for you.



Defensive Security: Example

Challenge Complete

You blocked the malicious IP address!

THM{THREAT-BLOCKED}