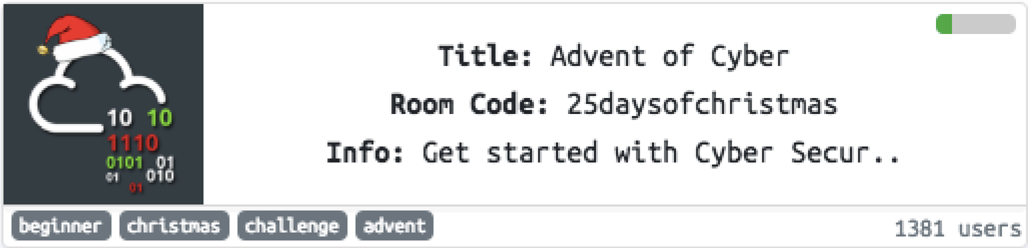
14 DECEMBER 2019 / CHRISTMAS

Local File Inclusion

This blog post will explain what local file inclusion is and how we can use it to exploit a machine. Use this post to solve challenge 14 of the Christmas Advent of Cyber!



Title: Advent of Cyber
Room Code: 25daysofchristmas
Info: Get started with Cyber Secur..

Advent of Cyber Room Image

https://tryhackme.com/room/25daysofchristmas

Some web applications include the contents of other files, and prints it to a web page. Or the application can include it into the document and parse it as part of the respective language.

For example if a web application has the following request:

```
https://example.com/?include_file=file1.php
```

This would take the contents from **file1.php** and display it on the page. If an application doesn't whitelist which files can be included, a user would be able to request the file /etc/shadow, showing all users hashed passwords on the system running the web application.

/When the web application includes a file, it will read it with the permissions of the user running the web server. For example, if the user *joe* runs the web server, it will read the file with joe's permissions, if its running as root, it will have the root users permissions. Take this into account when trying to include files - try first including a file you know the web server has permission to read (such as robots.txt if the web server has it), to see if its vulnerable to including other files.

With local file inclusion, you can try and view the following files to assist you in taking over a machine.

- /etc/shadow - View hashes passwords of all users on the system
- server.js or index.js - If the application was written in NodeJS, these are common file names that contain the main

exposed upon reading the file.

- /etc/hosts - Perhaps the web server machine is communicating with other devices on the network.
- /uploads/evil.php - If you manage to upload your own web shell onto the web server at some point, you can have it executed by including the file.

Challenge Tip

Some web servers will take every slash (/) as making a request to a new directory.. but what if we want to include a file such as /etc/shadow. Take the following request:

```
https://example.com/notes/?include=/etc/shadow
```

The server will think its going to /notes/include/etc/shadow. You can't include a slash in the URL as the web server will think its making a request to a different directory.

The solution is to use URL encoding. URL encoding replaces unsafe ASCII characters with '%' followed by two hexadecimal digits. A slash (/) can be URL encoded as **%2F**. This means we can change the request we previously had to:

```
https://example.com/notes/?include=%2Fetc%2Fshadow
```

This new request will be made to /notes/ and then convert the %2F to a slash! Removing any ambiguity in where the request is made and the file we're including.

Decoder/Encoder you can use.

Happy Hacking!

Ben Spring

Read more posts by this author.

Read More

— TryHackMe Blog —

christmas

Hydra

Metasploit: Basics

Linux Privilege Escalation: SUID

See all 3 posts →

Dumping Router Firmware - WriteUp

Dumping Router Firmware is a room at TryHackMe and can be accessed by using the below link! https://tryhackme.com/room/rfirmwareWe will move step by step i.e. from downloading the sample

6 MIN READ

METASPLOIT

Metasploit: Basics

Exploiting Struts2 with Metasploit Check our Christmas Challenge out! https://tryhackme.com/christmasThis blog post will go through using Metasploit. We will use this security tool to compromise a web server running Struts2.

6 MIN READ