Day 4: Web Exploitation – Santas Watching

Tools used: Kali Linux, Firefox, Terminal, SQLMap, Burpsite

Solution/walkthrough:

Question 1

Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

Ans: wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

Question 2

Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

Ans: site-log.php

Question 3

Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

Ans: THM{D4t3_AP1}

Thought Process/Methodology:

Having accessed the target machine, we input the URL given from THM. Once the URL has been input, the entire wfuzz command looks like to query the “breed” parameter using the wordlist “big.txt”. From there we will get the answer to the first question. After that access, GoBuster to find the API directory and from there get the answer for the second question. After that, you will get the flag displayed.

Day 5: Web Exploitation – Someone stole Santa’s gift list!

Tools used: Kali Linux, Firefox, Terminal, SQLMap, Burpsuite

Solution/walkthrough:

Question 1

Without using directory brute forcing, what's Santa's secret login panel?

Ans: /santapanel

Question 2

How many entries are there in the gift database?

Ans: 22

Question 3

What did Paul ask for?

Ans: Github Ownership

Question 4

What is the flag?

Ans: thmfox{All_I_Want_for_Christmas_Is_You}

Question 5

What is admin's password?

Ans: EhCNSWzzFP6sc7gB

Thought Process/Methodology:

Deploy the machine and use the IP address given. For us to bypass the login page, we have to utilize UNION SQL to gather the gift. To get the flag we utilize BurpSuite and SQLMap. Open BurpSuite and check that out proxy is turned on then get a request from the website. After that, we formulate the SQLMap. Once we run that we will be able to get the flag and admins password.

Day 6: Web Exploitation – Be Careful with what you wish on Christmas night

Tools used: Kali Linux, Firefox, Zap

Solution/walkthrough:

Question 1

What vulnerability type was used to exploit the application?

Ans: Stored cross-site scripting

Question 2

What query string can be abused to craft a reflected XSS?

Ans: q

Question 3

Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts are in the scan?

Ans: 2

Thought Process/Methodology:

By using the IP address given, we use zap to test the website. We then copy the URL into Zap and run the application. Once the attack is done, we will be able to see some vulnerabilities which are in XSS and cross-site scripting we then copy the code and paste it into the search query.

Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

Question 1

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Ans: 10.11.3.2

Question 2

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

Ans: http.request.method == GET

Question 3

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

Ans: reindeer-of-the-week

Question 4

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

Ans: plaintext_password_fiasco

Question 5

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

Ans: SSH

Question 6

What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Ans: Rubber ducky

Thought Process/Methodology:

Day 8: Networking – What's Under the Christmas Tree?

Tools used: Kali Linux, Firefox, Terminal, Nmap

Solution/walkthrough:

Question 1

When was Snort created?

Ans: 1998

Question 2

Using Nmap on MACHINE_IP , what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)

Ans: 80,2222,3389

Question 3

Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

Ans: Ubuntu

Question 4

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Ans: Blog

Thought Process/Methodology:

Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox, Terminal, FTP

Solution/walkthrough:

Question 1

Name the directory on the FTP server that has data accessible by the "anonymous" user

Ans: public

Question 2

What script gets executed within this directory?

Ans: backup.sh

Question 3

What movie did Santa have on his Christmas shopping list?

Ans: The Polar Express

Question 4

Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

Ans: THM{even_you_can_be_santa}

Thought Process/Methodology:

Day 10: Networking –Don’t be sELfish!

Tools used: Kali Linux, Firefox, Terminal, enum4linux, smbclient

Solution/walkthrough:

Question 1

Using enum4linux, how many users are there on the Samba server (MACHINE_IP)?

Ans: 3

Question 2

Now, how many "shares" are there on the Samba server?

Ans: 4

Question 3

Use *smbclient* to try to login to the shares on the Samba server (MACHINE_IP). What share doesn't require a password?

Ans: tbfc-santa

Question 4

Log in to this share, what directory did ElfMcSkidy leave for Santa?

Ans: jingle-tunes