Introduction To Hacking/CTF

The word “hacking” must have caught your attention.

What is a CTF

CTF (Capture The Flag) is an information security competition. It involves solving challenges based on different areas of cybersecurity. CTF’s can help beginners get an idea about the world of cybersecurity and help experts practice their skills. Flags are a string which are generally in the form of flag{*.?} with regex as flag{th1s_15_a_f4k3_fl4g!@#$}

Categories in CTFs are:

Binary Exploitation

Binary exploitation is the art of triggering vulnerabilities and redirecting code execution to perform functions that are unintended by the developer and hence executing malicious code on the system. Exploitation vulnerabilities are often found in C, C++, asm etc. Various type of binary exploitation methods are: Buffer overflow, return oriented programming(ROP), heap exploitation, v8 pwn(browser), kernel pwn.

Resources for Binary exploitation:

- https://ctf101.org/binary-exploitation/overview/
- Live overflow’s bin exp series
- John hammond’s bin exp series
- https://github.com/welchbj/ctf/blob/master/docs/binary-exploitation.md

Web exploitation

Web exploitation is the art of exploiting vulnerabilities in the webserver/website to execute remote code or exploit bad configuration in the website. Common vulnerability in this ctf category are: SQL injection(sqli), remote code execution(rce), directory traversal, cross site scripting(xss), server side request forgery(ssrf), cross site request forgery(csrf)

Resources for Web exploitation:

- https://github.com/payloadbox/command-injection-payload-list
- https://github.com/payloadbox/xss-payload-list
- https://github.com/payloadbox/xxe-injection-payload-list
- https://github.com/payloadbox/sql-injection-payload-list
- https://github.com/payloadbox/rfi-lfi-payload-list

- https://github.com/payloadbox/open-redirect-payload-list
- https://ctf101.org/web-exploitation/overview
- Live overflow's web series

Forensics

Forensics is the art of finding hidden files or data in a dump or another file. It is the analysis of files and data to find more clues about the flag.
It also includes recovering deleted files or finding traces of it. Right tools are needed for quality of life like: steghide, stegsnow, stegsolve, binwalk, foremost, exiftool, ghex, wireshark, volatility. Various types of forensics methods are: Steganography, embedded files, corrupted files, network dump analysis, memory dump analysis

Resources for Forensics:

- https://ctf101.org/forensics/overview/
- John hammond's forensics series
- https://aperisolve.fr/
- https://champdfa-ccsc-sp20.ctfd.io/

Cryptography

Cryptography is the reason we are able to talk online or do banking over the web. It is the method in which only the sender and recipient can only read the data shared. It's main purpose is to protect our privacy. However in CTFs we are required to break these encryption methods which are improperly implemented. The math may seem daunting, but more often than not, a simple understanding of the underlying principles will allow you to find flaws and crack the code. Types of cryptography are: XOR, caesar cipher, vigenere cipher, hashing functions, block ciphers, stream ciphers, RSA, AES etc

Resources for Crypto:

- https://ctf101.org/cryptography/overview/
- John hammond's bin crypto series
- https://macs358.org/chapters/frontmatter.html

Reverse engineering

It is typically the process of taking compiled program and converting it back into human format and understanding the flow of program code. It is mainly used in malware analysis and crackme(s). You need to have a knowledge of Assembly, C lang, Disassemblers, compilers/decompilers like ida freeware, binary ninja, gdb.

Resources for Crypto:

- https://ctf101.org/reverse-engineering/overview/
- John hammond's bin rev series
- https://pwn.college/

Interesting and useful CTF links:

- John hammond youtube channel
- Live overflow youtube channel
- Ippsec youtube channel
- Xct youtube channel
- Ctf101
- Bi0s wiki
- https://github.com/firmianay/CTF-All-In-One/tree/master/doc

For any queries regarding the topic contact:

Tarush Sonakya
Email: tsonakya@protonmail.com
Insta: @**anonimbus31337**
Discord: Anonimbus#6691