CTF CHALLENGE

Types of Challenges and Tools

WEB

This type of challenges focus on finding and exploiting the vulnerabilities in web application. The maybe testing the participants' knowledge on SQL Injection, XSS (Cross-Site Scripting), Command Injection and many more.

- SQL Injection is a vulnerability where an application takes input from a user and doesn't vaildate that the user's input doesn't contain additional SQL
- Cross Site Scripting or XSS is a vulnerability where on user of an application can send JavaScript that is executed by the browser of another user of the same application.

  This is a vulnerability because JavaScript has a high degree of control over a user's web browser.

  For example JavaScript has the ability to:

  Modify the page (called the DOM)
  Send more HTTP requests
  Access cookies
  By combining all of these abilities, XSS can maliciously use JavaScript to extract user's cookies and send them to an attacker controlled server. XSS can also modify the DOM to phish users for their passwords. This only scratches the surface of what XSS can be used to do.

  XSS is typically broken down into three categories:

  Reflected XSS
  Stored XSS
  DOM XSS

- Command Injection is a vulnerability that allows an attacker to submit system commands to a computer running a website. This happens when the application fails to encode user input that goes into a system shell. It is very common to see this vulnerability when a developer uses the system() command or its equivalent in the programming language of the application.

Forensics

Participants need to investigate some sort of data, like do a packet analysis on .pcap file, memory dump analysis, and so on. Forensics is the art of recovering the digital trail left on a computer. There are plently of methods to find data which is seemingly deleted, not stored, or worse, covertly recorded.

Cryptography

Cryptography is the reason we can use banking apps, transmit sensitive information over the web, and in general protect our privacy. However, a large part of CTFs is breaking widely used encryption schemes 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.

Reverse Engineering

Reverse Engineering in a CTF is typically the process of taking a compiled (machine code, bytecode) program and converting it back into a more human readable format. Very often the goal of a reverse engineering challenge is to understand the functionality of a given program such that you can identify deeper issues

Binary Exploitation

Binaries, or executables, are machine code for a computer to execute. For the most part, the binaries that you will face in CTFs are Linux ELF files or the occasional windows executable. Binary Exploitation is a broad topic within Cyber Security which really comes down to finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

Tools for CTF Challenges

CTF Frameworks or All-In One Tools for CTF

PwnTools – a CTF framework and exploit development library used by Gallopsled in every CTF

ctf-tools – a Github repository of open source scripts for your CTF needs like binwalk and apktool

Metasploit Framework – aside from being a penetration testing framework and software, Metasploit has modules for automatic exploitation and tools for crafting your exploits like find_badchars.rb, egghunter.rb, patter_offset.rb, pattern_create.rb, etc.

ROPgadget – used for ROP exploitation

Peda – Python Exploit Development Assistance for GDB

Google – where you can ask some questions

Reverse Engineering Tools, Decompilers and Debuggers

Immunity Debugger – a debugger similar to OllyDbg that has some cool plugins with the use of Python

OllyDbg – the most disassembly-based and GUI debugger for Windows

SWFScan – allows you to decompile Flash files

gdb – GNU Debugger

IDA Pro – Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger

WinDbg – Windows Debugger distributed by Microsoft

Tools for Static Code Analysis

RIPS – a static code analyzer for auditing vulnerabilities in PHP applications

HP Fortify Static Code Analyzer – also known as Fortify SCA which is a commercial software that is a multi-language auditor for vulnerabilities

OWASP Code Crawler – a static code review tool for .NET and J2EE/JAVA code which supports the OWASP Code Review Project

OWASP LAPSE Project – security auditing tool for detecting vulnerabilities in Java EE Applications

Flawfinder – a static source code analyzer that examines C/C++ source code and reports possible security weaknesses

Forensics

Strings – allows you to search and extract ASCII and UNICODE strings from a binary

SANS SIFT – SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu Live CD

ProDiscover Basic – evidence analyzer and data imaging tool

Volatility – memory forensics framework

The Sleuth Kit – open source digital forensics tool

FTK Imager – data preview and imaging tool

IPhone Analyzer – used for iPhone Forensics but only supports iOS 2, iOS 3, iOS 4 and iOS 5 devices

Xplico – network forensics tool

Binwalk – firmware analysis tool which allows you to extract the firmware image

ExifTool – a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of file formats like EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP

and ID3, as well as the maker notes of many digital cameras by Canon, Casio, FLIR, FujiFilm, GE, HP, JVC/Victor, Kodak, Leaf, Minolta/Konica-Minolta, Nikon, Nintendo, Olympus/Epson, Panasonic/Leica, Pentax/Asahi, Phase One, Reconyx, Ricoh, Samsung, Sanyo, Sigma/Foveon and Sony

dd – a command line utility for Unix and Linux which allows you to copy and convert files

CAINE – Computer Aided INvestigative Environment is a Live GNU/Linux distribution which is aimed for digital forensics

Autopsy – GUI to the command line digital investigation analysis tools in The Sleuth Kit

Any Hex Editors will do

DEFT Linux – Digital Evidence & Forensics Toolkit Linux distribution

Windows Sysiternals – consist of Windows system utilities that contain various useful programs

Cryptography

Hashdump

Sage

John The Ripper – is a free and fast password cracker available for many flavors of Unix, Windows, DOS, BeOS, and OpenVMS

Cryptool – open source e-learning tool illustrating cryptographic and cryptanalytic concepts

crypo.in.ua – online decoder and encoder for crypto and most people who are joining CTF competitions have this website opened while playing

Steganography

Steghide – a stega tool that can be used for embedding or extracting data in various kinds of image and audio files

Ffmpeg – cross-platform software to record, convert and stream audio and video

Gimp – GNU Image Manipulation Program

Audacity – free audio auditor and recorder

Stepic – python image steganography

Pngcheck – PNG tester and debugger which verifies the integrity of PNG, JNG and MNG files (by checking the internal 32-bit CRCs [checksums] and decompressing the image data)

OpenStego – free steganography solution

OutGuess

For Web Vulnerability Hunting or Web Exploitation

Burp Suite – commonly used for web application security testing and usually for finding manual web vulnerabilities which has an intercepting proxy and customizable plugins

OWASP ZAP – an Open Web Application Security Project similar to Burp but free and open source

WPScan – a blackbox WordPress Vulnerability Scanner

W3af – open source web application security scanner

OWASP Dirbuster – directory bruteforce or discovery tool

Bizploit – open source ERP Penetration Testing framework

Networking

aircrack-ng Suite – an open source WEP/WPA/WPA2 cracking tool which is usually bundled in most pentesting distributions

reaver – WiFi Protected Setup attacker tool

Kismet – 802.11 layer2 wireless network detector, sniffer, and intrusion detection system

Pixiewps – a tool used to bruteforce offline the WPS pin exploiting the low or non-existing entropy of some APs (pixie dust attack)

Nmap – an open source port scanner which has plugins for vulnerability assessment and net discovery

Wireshark – network sniffer and network protocol analyzer for Unix and Windows

Netcat -the TCP/IP swiss army

Captipper – a python tool to analyze, explore, and revive HTTP malicious traffic

Scapy – a powerful interactive packet manipulation program

For Your Protection in Attack in Defend

Snort – lightweight and free network intrusion detection system for UNIX and Windows

Iptables

Any Antivirus and Two-Way firewall will do

Chellam – Wi-Fi IDS/Firewall for Windows which detect Wi-Fi attacks, such as Honeypots, Evil Twins, Mis-association, and Hosted Network based backdoors etc., against a Windows based client without the need of custom hardware or drivers

peepdf – Python tool to explore PDF files in order to find out if the file can be harmful or not

Android IMSI-Catcher Detector – Android app for detecting IMSI-Catchers

Some Linux Distributions Ideal for CTF

Santoku Linux – GNU/Linux distribution or distro designed for helping you in every aspect of your mobile forensics, mobile malware analysis, reverse engineering and security testing needs

Kali Linux – a fully packed penetration testing Linux distribution based on Debian

BackBox Linux – a simplistic penetration testing distro based on Ubuntu

CAINE – Computer Aided INvestigative Environment is a Live GNU/Linux distribution which is aimed for digital forensics

DEFT Linux – Digital Evidence & Forensics Toolkit Linux distribution