CLOSE X

Loading Image...

DIARIUM

VNIVERSIDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

Pablo Gallardo's Blog

My professional web log about IT, Project Management & SAP

About

List of Tools featured in CEH iLabs by Hacking Phases

by Pmgallardo on 13 DECEMBER 2020 in CYBERSECURITY, IT, SECURITY

According to some people that have performed Certified Ethical Hacker (CEH) Practical exam, they say that most of the scenarios are based on exercises presented on CEH iLabs, that are included in the official CEH iLearn Course. So for CEH Practical exam candidates, it is important to know and handle all tools that are featured in these labs.

This post tries not to be just a plain list of all tools as they appear in the course, but I have tried to organized them according to the phase of hacking where they would belong. The phases of hacking, according to CEH, are:

1. Reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access
5. Clearing tracks

Nevertheless, some exercises fall out of any of these phaes. That would be the case for DoS attack or defensive actions; if this is the case they are listed separated from the others.

This post pretends to be a guide so, when a hacking challenge is presented during CEH exam, exam candidate has a list of available tools to complete it. It wants to be useful also to check exam candidate readiness before the exam.

CEH tools by attack/defense phase

Penetration Attack Phases

In a penetration attack, or standard hacking attack, the aim is to control

1. Reconnaissance

a. Ping a target

a. *ping* (Windows command)

b. Calculate TTL

a. *tracert* (Windows command)

c. Network Mapping

a. *Path Analyzer Pro* (Windows app)

d. Web Mirroring

a. *HTTTrack* (Windows app)
b. Social Engineering Tool (SET) (Linux command line)

2. Scanning

a. Sniffing / Packet Capture
a. *Wireshark* (Windows, Linux app)
Traffic Analyzer

a. *Capsa Network Analyzer* (Windows)
b. Network Scanning
a. *MegaPing* (Windows app)
b. *NetScanTools Pro* (Windows app)
c. *Solar Network Topology Mapper* (Windows app)
d. *Angry IP Scanner* (Windows app)
e. *Global Network Inventory* (Windows app)
f. *Softperfect Network Scanner* (Windows app)
g. *Metasploit > nmap* (Linux command line)
h. Metasploit > smb_versions (Linux command line)
c. Packet Crafting / Port Scanning
a. *nmap (Linux command)*
b. *Zenmap* (Windows app; GUI for nmap)
c. *hping3* (Linux command)
d. *ping* (Windows command)
e. *ping* (Ubuntu command)
f. *Cola Soft Packet Builder* (Windows app)
g. *IP-Tools* (Windows app)
d. NetBIOS Enumeration
a. *Advanced IP Scanner* (Windows app)
b. *SuperScan* (Windows app)
c. *NetBIOS Enumerator* (Windows app)
d. *nbtstat* (Windows command)
e. SNMP Enumeration
a. *nmap*
b. *Metasploit*
f. LDAP Enumeration
a. *ADExplorer* (Windows app)
g. Host Characteristics Enumeration
a. *enum4linux* (Linux command)
h. Host Resources Enumeration
a. *Hyena* (Windows app)
i. Vulnerability Scanning
a. *Nessus* (Windows app)
b. *Nikto* (Linux app)
j. WebServer Vulnerability Scanner
a. N-Stalker Tool (M15e02)
b. Acunetix Website Vulnerability Server (WVS) (M14e05)
c. Vega (M14e04)

- k. Webserver footprinting
  - a. *Netcat / nc* (Linux command line)
  - b. *Skipfish* (Linux command line)
  - c. *Uniscan* (LInux command line
  - d. *httprecon* (Windows app)
  - e. *ID Serve* (Windows app)
- l. Find hidden content in web servers
  - a. *OWASP dirbuster* (Linux app)

3. Gaining Access

- a. Bypass firewall
  - a. nmap -sI (zombie attack) (Linux)
  - b. HTTHost / HTTPort
- b. Dump Windows hash tables
  - a. *wmic* (Windows command line)
  - b. *PwDump7* (Windows app)
  - c. *metasploit > post/windows/gather/smart_hashdump* (Linux command line)

  Get dump hashes from LLMNR-NBTNS

  - a. *responder* (Linux command line)
- c. Generate rainbow tables
  - a. *Winrtgen* (Windows app)
- d. Crack Windows hash tables
  - a. *john* (Linux command line) (in combination with responder hashes)
  - b. *ophcrack* (Windows app) (in combination with PwDump7 hashes and tables made with another program)

  Compare rainbow tables with hashes

  - a. *RainbowCrack* (Windows app)
- e. Control from command line shell
  - a. *metasploit > reverse_tcp*
- f. Backdoor Creator
  - a. *msfvenom* (Linux command line) (controled by metasploit > reverse_tcp)
  - b. *TheFatRat* (Linux command line) (controled by metasploit > reverse_tcp)
  - c. *HTTP RAT* (Windows app) (controlled by HTTP RAT server)
  - d. *MoSucker* (Windows app)
  - e. *njRAT Builder* (Windows app) (controlled by njRAT Manager)
  - f. SwayzCryptor (Windows app) (controlled by njRAT Manager)
  - g. ProRat (Windows)
  - h. Theef Server (Windows app) (controlled by Theef Client)
- g. RAT
  - a. metaspoit > reverse_tcp and TightVNC
  - b. HTTP RAT
  - c. MoSucker
  - d. njRAT
  - e. ProRat
  - f. Theef Client
- h. Worm Maker
  - a. Internet Worm Maker Thing (Windows)
- i. Creater user
  - a. net (Windows command line)
- j. Spoof MAC Adress / ARP Poisoning
  - a. SMAC (Windows app)
  - b. Cain & Abel (Windows app)
- k. Session Hijacking Proxies to intercept or alter data/cookie
  - a. Burp proxy (Linux app)
  - b. OWASP Zed Attack Proxy (ZAP)
- l. FTP Password cracking
  - a. Hydra
- m. Web Server Attack
  - a. Armitage (Linux, app) (GUI for metasploit)
- n. Social Engineering

      a. Social Engineering Tool (SET) (Linux command line)
   o. Get WordPress Usernames
      a. WPScan (Linux command line)
   p. Crack WordPress Passwords
      a. metasploit > wordpress_login_enum
   q. SQL Injection Attack
      a. SQLMap (Linux command line) (M14e06)
      b. blast
   r. Dump Wireless data
      a. airodump-ng (Linux command line)
   s. Crack wireless
      a. aircrack-ng (Linux command line)

4. Maintaining Access

   a. Privilege Escalation
      a. *metasploit* > *bypassuac_foodhelper*
   b. SpyWare
      a. Spytech SpyAgent
      b. SpyWare
   c. Bypass password rules
      a. *HTTHost* (Windows app)
      b. *netsh* (Windows command line)

5. Clearing Tracks

   a. Hide files
      a. NTFS streams (Windows command line)
   b. Steganography
      a. *snow* (Windows app)
      b. *OpenStego* (Windows app)
      c. *QuickStego* (Windows app)
   c. Covert channels
      a. cover_tcp (Linux command line)
   d. Modify Windows audit policy
      a. *auditpol* (Windows command line)
   e. Logs
   f. Registry values

Denial-of-Service (DoS)

Denial-of-Service (DoS) is a type of attack that differs from the standard hacking attack, where the aim is to control the target system. In the case of DoS, the objective is to impact the availability of a system.
The reconnaissance and scanning phases seen on Penetration would apply as well to a DoS attack.

1. Reconnaissance
2. Scanning
3. DoS Attack
   a. SYN flood
      a. *metasploit* > *auxiliary/dos/tcp/synflood* (Linux command) M10e01
      b. *hping3* (Linux command), with –flood parameter
   b. Other
      a. High Orbit Ion Cannon (HOIC) (Windows app)

Information Security Aspects

This section covers the defensive tools seen on CEH.

Audit System Passwords

L0phtCrack (Windows)

Static Malware Analysis

IDA Disassembler

OllyDBg

Detect ARP Attacks

Wireshark (M08e05)

XARP Tool (M08e06)

Dynamic Malware Analysis / Detecting Trojans in your computer

TCPView (Windows app)

autoruns (Windows app)

CurrPorts (Windows app)

Startup program Monitoring

WinPatrol

Antivirus and antimalware

Windows Defender

j16 PowerTools (Windows app)

ClamWin Antivirus

Windows Registry Monitoring

regshot

Intrusion Detection System (IDS)

Snort

Honeypot

HoneyBOT (Windows)

Firewall

Windows Firewall

Windows command netsh

Server Configuration

Internet Information Service (ISS) / inetmgr (Windows)

Calculate hash

HashCalc

MD5 Calculator

Text/file encryptor

Cryptoforge (Windows app)

BCTextEncoder (Windows app)

CrypTool (Windows app)

Disk Encryption

VeraCrypt (Windows app)

Top apps

The top 5 applications that you need to master for CEH Practical exam, as they are ones of the most used, are the following:

1. nmap / Zenmap
2. Wireshark
3. Burp Suite
4. Cain
5. metasploit (it is very present in iLabs exercises, but I am not sure if it is requested during exam)

🏷 app, application, applications, apps, ceh, ceh practical, certified, certified ethical hacking, ethical, hacker, ilabs, labs, practical, software, tools, v10

← How to modify Windows Firewall Configuration from Command Prompt

Metasploit Framework in CEH Exam →

No comments yet.

Leave a Reply

You must be logged in to post a comment.