Guide-CEH-Practical-Master

Exame Details

- Exam Title: Certified Ethical Hacker (Practical)
- Number of Practical Challenges: 20
- Duration: 6 hours
- Availability: Aspen – iLabs
- Test Format: Cyber Range
- Passing Score: Min 15 Questions

Exam Tips

- Vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems, etc;
- System hacking, steganography;
- Network scanning to identify live and vulnerable machines in a network;
- OS banner grabbing, service, and user enumeration;
- Different types of cryptography attacks;
- SQL injection attacks;
- Packet sniffing;
- Computer Forensic;

Format

- Realized Test with Web Browser CyberQ
- One ParrotOS to perform the pentest and Windows 11 Machine
- Five machines to compromise on an isolated network from the internet
- Search in Google? (Yes!)
- Talk to someone during the race? (No!)
- Proctored Monitor

Tools

- Nmap
- Hydra

- Sqlmap
- Wpscan
- Nikto
- John
- Hashcat
- Metasploit
- Responder LLMNR
- Wireshark or Tcpdump
- Steghide
- OpenStego
- QuickStego
- Dirb
- OleView
- Dcomcnf
- RpcDump
- Gacutil
- Searchsploit
- sandfly-entropyscan
- Strings
- FTK Imager
- Malwoverview
- GDB or IDA
- Crunch
- Cewl
- LinPeas
- Aircrack-ng
- GTFOBINS
- Veracrypt
- Hashcalc
- Rainbow Crack
- Radare2
- Rockyou and SecList

Helps

- Reddit Exam Reviews
- Medium Exam Reviews

- Professionals Certificate
- Hack The Box (Challenges Steganography and Web) (https://www.hackthebox.eu/)
- Vulnhub (Machines Easy to Medium) (https://www.vulnhub.com/)
- Labs PenTest Brazil (CEH Course made in Major Eder ft ACADI-TI) (https://acaditi.com.br/ceh-v10-treinamento-certified-ethical-hacker/)
- TryHackMe (https://tryhackme.com/) / https://tryhackme.com/room/wirectf / https://tryhackme.com/room/wirectf / https://tryhackme.com/room/hydra / https://tryhackme.com/room/sqli / https://tryhackme.com/room/crackthehash / https://medium.com/@kyryloren/jack-writeup-by-kyryloren-tryhackme-e41cff4e1c55
- iLabs CEH (https://ilabs.eccouncil.org/ethical-hacking-exercises/)
- CEH Exam Guide (https://medium.com/techiepedia/certified-ethical-hacker-practical-exam-guide-dce1f4f216c9)

Examples Questions (There are the real issues)

- What is the IP of the Windows X machine?
- What is the version of the Linux Kernel?
- How many Windows machines are there?
- What is the password for user X of the FTP server?
- What is user X's IBAN number?
- Which user X's phone number?
- What is the password hidden in the .jpeg file?
- Rogue AP suspect, crack your password using capture.cap
- Discovery RAT in Network and acess computer to recovery secret.txt
- Identify IoT Message using capture.cap
- Identify FQDN of Domain Controller
- Perform deep scan on the elf and obtain hash of the file with highest entropy value.
- Find the executable's Entry point (Address)

Attacks Vector

https://www.upguard.com/blog/attack-vector

https://searchsecurity.techtarget.com/definition/attack-vector

https://www.balbix.com/insights/attack-vectors-and-breach-methods/

https://attack.mitre.org/

https://searchsecurity.techtarget.com/definition/attack-vector#:~:text=An%20attack%20vector%20is%20a,vulnerabilities%2C%20including%20the%20human%20element.

https://www.youtube.com/watch?v=LsuoJb7n3co

https://www.youtube.com/watch?v=rcB4EZLfi7I

https://www.youtube.com/watch?v=dz7Ntp7KQGA

Network Scanning

https://nmap.org/man/pt_BR/index.html

https://nmap.org/docs.html

https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

https://hackertarget.com/nmap-tutorial/

https://www.stationx.net/nmap-cheat-sheet/

https://media.x-ra.de/doc/NmapCheatSheetv1.1.pdf

https://www.100security.com.br/netdiscover

https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/

https://www.youtube.com/watch?v=PS677owUk-c

https://www.stationx.net/nmap-cheat-sheet/

https://redteamtutorials.com/2018/10/14/nmap-cheatsheet/

https://resources.infosecinstitute.com/nmap-cheat-sheet/#gref

https://medium.com/@infosecsanyam/nmap-cheat-sheet-nmap-scanning-types-scanning-commands-nse-scripts-868a7bd7f692

https://resources.infosecinstitute.com/network-discovery-tool/#gref

Enumeration

- https://null-byte.wonderhowto.com/how-to/enumerate-smb-with-enum4linux-smbclient-0198049/
- https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/

- https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html
- https://medium.com/@arnavtripathy98/smb-enumeration-for-penetration-testing-e782a328bf1b
- https://www.redsiege.com/blog/2020/04/user-enumeration-part-3-windows/
- https://nmap.org/nsedoc/scripts/smb-enum-users.html
- https://github.com/sensepost/UserEnum
- https://book.hacktricks.xyz/network-services-pentesting/pentesting-dns
- https://securitytrails.com/blog/dns-enumeration
- https://medium.com/@klockw3rk/back-to-basics-dns-enumeration-446017957aa3

Brute Force

https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux

https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/

https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/

https://redteamtutorials.com/2018/10/25/hydra-brute-force-https/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-passwords-with-tamper-data-thc-hydra-0155374/

https://laconicwolf.com/2018/09/29/hashcat-tutorial-the-basics-of-cracking-passwords-with-hashcat/

https://medium.com/@sc015020/how-to-crack-passwords-with-john-the-ripper-fdb98449ff1

https://www.varonis.com/blog/john-the-ripper/

Wordlists

http://www.phenoelit.org/dpl/dpl.html

https://datarecovery.com/rd/default-passwords/

https://github.com/Dormidera/WordList-Compendium

https://github.com/danielmiessler/SecLists

https://www.kaggle.com/wjburns/common-password-list-rockyoutxt

SQL Injection

- https://hackertarget.com/sqlmap-tutorial/
- https://www.binarytides.com/sqlmap-hacking-tutorial/
- https://www.hackingarticles.in/database-penetration-testing-using-sqlmap-part-1/
- https://medium.com/@rafaelrenovaci/dvwa-solution-sql-injection-blind-sqlmap-cd1461ad336e
- https://medium.com/hacker-toolbelt/dvwa-1-9-viii-blind-sql-injection-with-sqlmap-ee8d59fbdea7
- https://www.exploit-db.com/docs/english/13701-easy-methodblind-sql-injection.pdf
- https://gracefulsecurity.com/sql-injection-filter-evasion-with-sqlmap/
- https://medium.com/@drag0n/sqlmap-tamper-scripts-sql-injection-and-waf-bypass-c5a3f5764cb3
- https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF
- https://www.1337pwn.com/use-sqlmap-to-bypass-cloudflare-waf-and-hack-website-with-sql-injection/

Types of SQL Injection

Union-based SQLi: This technique involves using the UNION SQL operator to combine the results of the original query with the results of an attacker-controlled query.

Error-based SQLi: This technique involves forcing the database to generate an error, which can reveal information about the database structure.

Blind SQLi: In this type of SQLi, the attacker doesn't get the results of the SQL query in the HTTP response. The attacker has to send a payload, and based on the application's response, he can infer if the payload was executed successfully or not.

Time-based Blind SQLi: This is a type of blind SQLi where the attacker can infer if the payload was executed successfully or not based on the time the server takes to respond.

Out-of-Band SQLi: In this type of SQLi, the attacker doesn't get the results of the SQL query in the HTTP response. Instead, the results are sent to an external server controlled by the attacker.

Second Order SQLi: In this type of SQLi, the payload is not directly injected into the SQL query, but it is stored by the application and used in a later SQL query.

Stored Procedure Attacks: This involves calling stored procedures from the SQL injection point.

Function Call Payloads: This involves calling database functions from the SQL injection point.

Boolean-based SQLi: This involves sending a SQL query that will return a different result depending on whether the condition in the query is true or false.

Content-based SQLi: This involves sending a SQL query that will return a different result depending on the content of the HTTP response.

Tools

SQLMap: SQLMap is a popular open-source penetration testing tool that automates the process of detecting and exploiting SQL Injection vulnerabilities.

Havij: Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities.

jSQL Injection: jSQL Injection is a lightweight application used to find database information from a distant server.

BBQSQL: BBQSQL is a blind SQL injection framework written in Python.

NoSQLMap: NoSQLMap is an open-source Python tool designed to audit for as well as automate injection attacks and exploit default configuration weaknesses in NoSQL databases.

SQLNinja: SQLNinja is a tool to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.

SQLiX: SQLiX is a SQL Injection scanner written in Perl.

SQLSentinel: SQLSentinel is an application-level firewall for MySQL that prevents SQL Injection attacks.

MyBatis: MyBatis is a Java persistence framework that includes a built-in SQL Injection scanner.

Blisqy: Blisqy is a tool to aid Web Security researchers to find Time-based Blind SQL injection on HTTP Headers and also exploitation of the same vulnerability.

Steganography

https://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref

https://flylib.com/books/en/1.36.1/steganography.html

https://blog.eccouncil.org/what-is-steganography-and-what-are-its-popular-techniques/

https://www.edureka.co/blog/steganography-tutorial

https://www.tutorialspoint.com/image-based-steganography-using-python

https://medium.com/@KamranSaifullah/da-vinci-stenography-challenge-solution-90122a59822

https://medium.com/@chrisdare/steganography-in-computer-forensics-6d6e87d85c0a

https://www.telegraph.co.uk/culture/art/art-news/8197896/Mona-Lisa-painting-contains-hidden-code.html

https://medium.com/write-ups-hackthebox/tagged/steganography

http://moinkhans.blogspot.com/2015/06/steghide-beginners-tutorial.html

https://www.2daygeek.com/easy-way-hide-information-inside-image-and-sound-objects/

System Hacking

https://www.notsosecure.com/pwning-with-responder-a-pentesters-guide/

https://www.ivoidwarranties.tech/posts/pentesting-tuts/responder/cheatsheet/

https://blog.rapid7.com/2017/03/21/combining-responder-and-psexec-for-internal-penetration-tests/

https://www.4armed.com/blog/llmnr-nbtns-poisoning-using-responder/

https://medium.com/@hninja049/how-to-easy-find-exploits-with-searchsploit-on-linux-4ce0b82c82fd

https://www.offensive-security.com/offsec/edb-searchsploit-update-2020/

https://www.youtube.com/watch?v=29GlfaH5qCM

https://www.hackingloops.com/maintaining-access-metasploit/

https://resources.infosecinstitute.com/information-gathering-using-metasploit/

https://www.youtube.com/watch?v=s6rwS7UuMt8

https://null-byte.wonderhowto.com/how-to/exploit-eternalblue-windows-server-with-metasploit-0195413/

https://www.youtube.com/watch?v=joT8NxlXxVY

https://attack.mitre.org/techniques/T1557/001/

https://www.youtube.com/watch?v=0TBCzaBklcE

https://www.youtube.com/watch?v=FfoQFKhWUr0

https://www.youtube.com/watch?v=Fg2gvk0qgjM

https://www.youtube.com/watch?v=rjRDsXp_MNk

https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

https://medium.com/@subhammisra45/llmnr-poisoning-and-relay-5477949b7bef

https://www.hackingarticles.in/get-reverse-shell-via-windows-one-liner/

Web Scanners

https://blog.clusterweb.com.br/?p=1297

https://hackertarget.com/nikto-tutorial/

https://geekflare.com/nikto-webserver-scanner/

https://www.youtube.com/watch?v=K78YOmbuT48

https://blog.sucuri.net/2015/12/using-wpscan-finding-wordpress-vulnerabilities.html

https://www.hackingtutorials.org/web-application-hacking/hack-a-wordpress-website-with-wpscan/

https://linuxhint.com/wpscan_wordpress_vulnerabilities_scan/

https://www.youtube.com/watch?v=SS991k5Alp0

https://www.youtube.com/watch?v=MtyhOrBfG-E

https://www.youtube.com/watch?v=sQ4TtFdaiRA

https://www.exploit-db.com/docs/english/45556-wordpress-penetration-testing-using-wpscan-and-metasploit.pdf?rss

https://www.wpwhitesecurity.com/strong-wordpress-passwords-wpscan/

https://www.youtube.com/watch?v=BTGP5sZfJKY

https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-5-creating-custom-wordlist-with-cewl-0158855/

https://medium.com/tech-zoom/dirb-a-web-content-scanner-bc9cba624c86

https://www.hackingarticles.in/comprehensive-guide-on-dirb-tool/

Sniffers

https://www.youtube.com/watch?v=TkCSr30UojM

https://www.varonis.com/blog/how-to-use-wireshark/

https://hackertarget.com/wireshark-tutorial-and-cheat-sheet/

https://www.lifewire.com/wireshark-tutorial-4143298

https://www.comparitech.com/net-admin/wireshark-cheat-sheet/

https://medium.com/hacker-toolbelt/wireshark-filters-cheat-sheet-eacdc438969c

https://github.com/security-cheatsheet/wireshark-cheatsheet

https://www.cellstream.com/resources/2013-09-10-11-55-21/cellstream-public-documents/wireshark-related/83-wireshark-display-filter-cheat-sheet/file

https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

https://www.youtube.com/watch?v=4_7A8Ikp5Cc

https://www.guru99.com/wireshark-passwords-sniffer.html

https://danielmiessler.com/study/tcpdump/

https://hackertarget.com/tcpdump-examples/

https://opensource.com/article/18/10/introduction-tcpdump

Malware Analysis

Static Analysis:

Header Examination: Look at the headers of the executable file. Common executable file formats include PE (Portable Executable) for Windows and ELF (Executable and Linkable Format) for Linux. Disassembly: Disassemble the binary code using a disassembler such as IDA Pro, Ghidra, or Radare2. These tools can help you navigate the assembly code and identify the entry point.

Dynamic Analysis:

Debugger: Use a debugger like OllyDbg, WinDbg, or GDB to run the executable in a controlled environment. Set breakpoints and step through the code until you reach the entry point. Monitoring Tools: Use tools like Process Monitor (ProcMon) on Windows or strace on Linux to monitor system calls and identify when the executable is loaded and starts executing. Strings and Signatures:

String Analysis: Look for strings within the executable that may indicate the entry point. Some malware authors leave identifiable strings. Signature-Based Detection: Use antivirus or anti-malware tools that might have signature databases to identify known malware and their entry points. Code Emulation and Analysis:

Sandboxing: Execute the executable in a controlled environment, often called a sandbox, and monitor its behavior. Analyze the log or output for indications of the entry point.

Tools

Cuckoo Sandbox: An open-source automated malware analysis system.

FireEye: A platform for detecting, preventing, and resolving advanced malware.

Joe Sandbox: A malware analysis platform that provides both static and dynamic analysis.

OllyDbg: A 32-bit assembler level analyzing debugger for Microsoft Windows.

IDA Pro: A multi-processor disassembler and debugger for Windows, Linux, and macOS.

Ghidra: A software reverse engineering framework developed by the NSA.

Radare2: A portable reversing framework that supports a wide range of architectures.

Process Monitor: A monitoring tool for Windows that shows real-time file system, registry, and process/thread activity.

Wireshark: A network protocol analyzer that lets you capture and interactively browse network traffic.

YARA: A tool for identifying and classifying malware based on patterns.

Volatility: A memory forensics framework for incident response and malware analysis.

The Sleuth Kit: A collection of command-line tools for digital investigation and analysis.

Autopsy: A digital forensics platform that provides a graphical interface for The Sleuth Kit.

Mandiant Redline: A free tool for host investigations and memory analysis.

Regshot: A utility that takes a snapshot of your system's registry and compares it to a second one.

PEiD: A tool that can detect the compiler/packer/cryptor of PE executables.

PEview: A lightweight and portable tool for viewing PE files.

PEStudio: A free tool that performs malware assessments on executable files.

Dependency Walker: A utility that scans any 32-bit or 64-bit Windows module and builds a hierarchical tree diagram of all dependent modules.

VirusTotal: A service that analyzes suspicious files and URLs to detect malware.

Reviews and Details CEH Practical

https://www.linkedin.com/pulse/my-jouney-ceh-practical-joas-antonio-dos-santos (My Review)

https://forums.itpro.tv/topic/2604/ceh-practical/2

https://www.linkedin.com/pulse/considera%C3%A7%C3%B5es-sobre-o-exame-ceh-practical-leandro-cortiz/

https://infayer.com/archivos/65

https://medium.com/@jonaldallan/passed-ec-councils-certified-ethical-hacker-practical-20634b6f0f2

https://www.reddit.com/r/CEH/comments/c69fou/passed_ceh_practicalpost_exam_writeup/

https://www.reddit.com/r/CEH/comments/eeu3cx/ceh_practical_handson_exam_passed_with_2020_score/

https://www.reddit.com/r/CEH/comments/8wk2ve/ceh_vs_ceh_practical/

https://www.reddit.com/r/CEH/comments/dfa1y8/passed_ceh_practical/

https://www.reddit.com/r/CEH/comments/b1wgbs/ceh_v10_practical/

https://www.youtube.com/watch?v=ZYEo2AQdgcg

https://www.youtube.com/watch?v=MEYjyr65bJE

https://www.reddit.com/r/CEH/comments/ek0gzp/ceh_practical_passed_2020/

https://www.reddit.com/r/CEH/comments/evuztj/ceh_practical/

https://www.reddit.com/r/CEH/comments/f6t80r/can_ceh_practical_be_regarded_as_a/

https://www.reddit.com/r/CEH/comments/g6z6vn/just_passed_ceh_practical_1920/

https://medium.com/@jonathanchelmus/c-eh-practical-exam-review-42755546c82e

https://www.reddit.com/r/CEH/comments/hk6880/passing_ceh_practical/

https://www.reddit.com/r/CEH/comments/f629zk/ceh_practical_vs_ejpt_vs_ecppt/

https://www.youtube.com/watch?v=o1u69KvSFmQ&list=PLmQBbrHGk7jQbsvF3_xJp720yaUgeYCkj

https://www.youtube.com/watch?v=oYgtePf0z44

https://www.youtube.com/watch?v=9g5gdhoDotg&list=PLWGnVet-gN_kGHSHbWbeI0gtfYx3PnDZO

https://www.youtube.com/watch?v=LHU0OFcWSBk

https://medium.com/@mruur/ceh-practical-exam-review-918e76f831ff

https://www.youtube.com/c/XanderBilla/videos

https://www.youtube.com/watch?v=YZf5xmeaU58

https://newhorizons.com.sg/ceh-master/

https://www.iitlearning.com/certified-ethical-hacker-practical.php

https://medium.com/@anontuttuvenus/ceh-practical-exam-review-185ea4cef82a

https://www.cyberprotex.com/ceh.html

https://www.infosec4tc.com/product/ceh-master-exam1-exam2-practical/

https://sysaptechnologies.com/certified-ethical-hacker-ceh-v10-practical/

https://jensoroger.wordpress.com/2019/02/09/oscp-ceh-practical/

https://khroot.com/2020/06/20/certified-ethical-hacker-practical-review/

https://github.com/Samsar4/Ethical-Hacking-Labs

https://www.reddit.com/r/CEH/comments/jg0y6u/ceh_practical/

https://www.reddit.com/r/CEH/comments/dfa1y8/passed_ceh_practical/

https://www.reddit.com/r/CEH/comments/cgualo/ceh_practical_tell_me_about_it/

https://www.reddit.com/r/CEH/comments/c69fou/passed_ceh_practicalpost_exam_writeup/