My respositry

Hacker roadmap

This repository is an overview of what you need to learn penetration testing and a collection of hacking tools, resources and references to practice ethical hacking. Most of the tools are UNIX compatible, free and open source.

Before you start

If you're new to information security, forget everything you know about hacking.

Don't start using tools without reading about pen testing and how it works (see Additional resources section).

Don't download or use tools if you haven't audited its code.

Don't use these tools to do stupid things like investigating/hacking without consent on your friends, or worst, your recruiter.

Read books, manuals, articles, be curious and not just a script kiddie.

I wish you don't use these tools for illegal purposes, but if you do, I sure hope you know what you're doing.

Practice using challenges, not real targets!

Table of Contents

Introduction

What is penetration testing?

Want to become a penetration tester?

Some vocabulary

Difference between hacking and ethical hacking

Languages

Content Management Systems

Basic steps of pen testing

Tools by category

🕵‍♂ Information Gathering

🔒 Password Attacks

📝 Wordlists

🌐 Wireless Testing

🔧 Exploitation Tools

👥 Sniffing & Spoofing

🚀 Web Hacking

🎉 Post Exploitation

📦 Frameworks

Additional resources

Books / Manuals

Discussions

Security Advisories

Challenges

License

(TOC made with nGitHubTOC)

Introduction

What is penetration testing?

Penetration testing is a type of security testing that is used to test the security of an application. It is conducted to find a security risk which might be present in a system.

If a system is not secure, then an attacker may be able to disrupt or take unauthorized control of that system. A security risk is normally an accidental error that occurs while developing and implementing software. For example, configuration errors, design errors, and software bugs, etc. Learn more

Want to become a penetration tester?

Knowing about risks on the internet and how they can be prevented is very useful, especially as a developer. Web hacking and penetration testing is the v2.0 of self-defense! But is knowing about tools and how to use them really all you need to become a pen tester? Surely not. A real penetration tester must be able to proceed rigorously and detect the weaknesses of an application. They must be able to identify the technology behind and test every single door that might be open to hackers.

This repository aims first to establish a reflection method on penetration testing and explain how to proceed to secure an application. And secondly, to regroup all kind of tools or resources pen testers need. Be sure to know basics of programming languages and internet security before learning pen testing.

Also, this is important to inform yourself about the law and what you are allowed to do or not. According to your country, the computer laws are not the same. First, check laws about privacy and surveillance: Nine eyes countries, Five eyes and Fourteen Eyes. Always check if what you're doing is legal. Even when it's not offensive, information gathering can also be illegal!

(Table of Contents)

Some vocabulary

Infosec: Information security, which is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Infosec can also be a person who practices ethical security. Wikipedia

Opsec: Operations security, which is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. Wikipedia

Black/grey/white hat hacker: Someone who uses bugs or exploits to break into systems or applications. The goal and the method differs depending if they're a black, grey or white hat hacker. A black hat is just someone malicious that does not wait permission to break into a system or application. A white hat is usually a security researcher who practice ethical hacking. A grey hat is just in the middle of these two kind of hackers, they might want to be malicious if it can be benefit (data breach, money, whistleblowing ...).

Red team: According to Wikipedia, a red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view. It is particularly effective in organizations with strong cultures and fixed ways of approaching problems. The United States intelligence community (military and civilian) has red teams that explore alternative futures and write articles as if they were foreign world leaders. Little formal doctrine or publications about Red Teaming in the military exist. In infosec exercises, Red teamers are playing the role of attackers. Wikipedia

Blue team: A blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation. As a result, blue teams were developed to design defensive measures against red team activities. In infosec exercises, Blue teamers are playing the role of defenders. Wikipedia

Penetration tester: An ethical hacker who practices security, tests applications and systems to prevent intrusions or find vulnerabilities.

Security researcher: Someone who practices pen testing and browses the web to find phishing/fake websites, infected servers, bugs or vulnerabilities. They can work for a company as a security consultant and are most likely a Blue teamer.

Reverse engineering: Reverse engineering, also called back engineering, is the process by which a man-made object is deconstructed to reveal its designs, architecture, or to extract knowledge from the object. Similar to scientific research, the only difference being that scientific research is about a natural phenomenon. Wikipedia

Social engineering: In the context of information security, it refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. The term "social engineering" as an act of psychological manipulation of a human, is also associated with the social sciences, but its usage has caught on among computer and information security professionals. Wikipedia

Threat analyst: A threat hunter, also called a cybersecurity threat analyst, is a security professional or managed service provider (MSP) that proactively uses manual or machine-assisted techniques to detect security incidents that may elude the grasp of automated systems. Threat hunters aim to uncover incidents that an enterprise would otherwise not find out about, providing chief information security officers (CISOs) and chief information officers (CIOs) with an additional line of defense against advanced persistent threats (APTs). SearchCIO

(Table of Contents)

Difference between hacking and ethical hacking

A black hat is practicing penetration testing, but unlike a white hat, this is not ethical hacking. Ethical hacking is about finding vulnerabilities and improve the security of a system. An ethical hacker is the ultimate security professional. Ethical hackers know how to find and exploit vulnerabilities and weaknesses in various systems, just like a malicious hacker (a black hat hacker). In fact, they both use the same skills; however, an ethical hacker uses those skills in a legitimate, lawful manner to try to find vulnerabilities and fix them before the bad guys can get there and try to break in. An ethical hacker is basically a white hat hacker.

(Table of Contents)

Languages

Learning programming is the very first way to start learning about security. There's a lot of languages, most people start with Python, it's the easiest and the most popular one. PHP and Go are the less popular to write security-related stuff, but any of these can still be used in such context. Bash and Powershell are mostly about scripting and writing simple CLI applications.

Since not all languages work the same way, you need to look at how they work and what you want to learn. For example, C++ and Java compile, PHP and Python do not, they are interpreted languages. This definitely changes what you should use them for. Each language also has its own design patterns.

Scripting

Bash

Powershell

Software & mobile apps

Java

Swift

C / C++ / C#

General purpose

Python

Ruby

Perl

PHP

Go

(Table of Contents)

Content Management Systems

Wordpress

Joomla

Drupal

SPIP

These are the most used Content Management Systems (CMS). See a complete list here.

(Table of Contents)

Basic steps of pen testing

Source: tutorialspoint

Read more about pen testing methodology

(Table of Contents)

Tools by category

A more complete list of tools can be found on Kali Linux official website.

🕵‍♂ Information Gathering

Information Gathering tools allows you to collect host metadata about services and users. Check informations about a domain, IP address, phone number or an email address.

Tool Language Support Description

theHarvester Python Linux/Windows/macOS E-mails, subdomains and names Harvester.

CTFR Python Linux/Windows/macOS Abusing Certificate Transparency logs for getting HTTPS websites subdomains.

Sn1per bash Linux/macOS Automated Pentest Recon Scanner.

RED Hawk PHP Linux/Windows/macOS All in one tool for Information Gathering, Vulnerability Scanning and Crawling. A must have tool for all penetration testers.

Infoga Python Linux/Windows/macOS Email Information Gathering.

KnockMail Python Linux/Windows/macOS Check if email address exists.

a2sv Python Linux/Windows/macOS Auto Scanning to SSL Vulnerability.

Wfuzz Python Linux/Windows/macOS Web application fuzzer.

Nmap C/C++ Linux/Windows/macOS A very common tool. Network host, vuln and port detector.

PhoneInfoga Go Linux/macOS An OSINT framework for phone numbers.

🔒 Password Attacks

Crack passwords and create wordlists.

Tool Language Support Description

John the Ripper C Linux/Windows/macOS John the Ripper is a fast password cracker.

hashcat C Linux/Windows/macOS World's fastest and most advanced password recovery utility.

Hydra C Linux/Windows/macOS Parallelized login cracker which supports numerous protocols to attack.

ophcrack C++ Linux/Windows/macOS Windows password cracker based on rainbow tables.

Ncrack C Linux/Windows/macOS High-speed network authentication cracking tool.

WGen Python Linux/Windows/macOS Create awesome wordlists with Python.

SSH Auditor Go Linux/macOS The best way to scan for weak ssh passwords on your network.

📝 Wordlists

Tool Description

Probable Wordlist Wordlists sorted by probability originally created for password generation and testing.

🌐 Wireless Testing

Used for intrusion detection and wifi attacks.

Tool Language Support Description

Aircrack C Linux/Windows/macOS WiFi security auditing tools suite.

bettercap Go Linux/Windows/macOS/Android bettercap is the Swiss army knife for network attacks and monitoring.

WiFi Pumpkin Python Linux/Windows/macOS/Android Framework for Rogue Wi-Fi Access Point Attack.

Airgeddon Shell Linux/Windows/macOS This is a multi-use bash script for Linux systems to audit wireless networks.

Airbash C Linux/Windows/macOS A POSIX-compliant, fully automated WPA PSK handshake capture script aimed at penetration testing.

🔧 Exploitation Tools

Acesss systems and data with service-oriented exploits.

Tool Language Support Description

SQLmap Python Linux/Windows/macOS Automatic SQL injection and database takeover tool.

XSStrike Python Linux/Windows/macOS Advanced XSS detection and exploitation suite.

Commix Python Linux/Windows/macOS Automated All-in-One OS command injection and exploitation tool.

Nuclei Go Linux/Windows/macOS Fast and customisable vulnerability scanner based on simple YAML based DSL.

👥 Sniffing & Spoofing

Listen to network traffic or fake a network entity.

Tool Language Support Description

Wireshark C/C++ Linux/Windows/macOS Wireshark is a network protocol analyzer.

WiFi Pumpkin Python Linux/Windows/macOS/Android Framework for Rogue Wi-Fi Access Point Attack.

Zarp Python Linux/Windows/macOS A free network attack framework.

🚀 Web Hacking

Exploit popular CMSs that are hosted online.

Tool Language Support Description

WPScan Ruby Linux/Windows/macOS WPScan is a black box WordPress vulnerability scanner.

Droopescan Python Linux/Windows/macOS A plugin-based scanner to identify issues with several CMSs, mainly Drupal & Silverstripe.

Joomscan Perl Linux/Windows/macOS Joomla Vulnerability Scanner.

Drupwn Python Linux/Windows/macOS Drupal Security Scanner to perform enumerations on Drupal-based web applications.

CMSeek Python Linux/Windows/macOS CMS Detection and Exploitation suite - Scan WordPress, Joomla, Drupal and 130 other CMSs.

🎉 Post Exploitation

Exploits for after you have already gained access.

Tool Language Support Description

TheFatRat C Linux/Windows/macOS Easy tool to generate backdoor and easy tool to post exploitation attack like browser attack, dll.

📦 Frameworks

Frameworks are packs of pen testing tools with custom shell navigation and documentation.

Tool Language Support Description

Operative Framework Python Linux/Windows/macOS Framework based on fingerprint action, this tool is used to get information on a website or a enterprise target with multiple modules.

Metasploit Ruby Linux/Windows/macOS A penetration testing framework for ethical hackers.

cSploit Java Android The most complete and advanced IT security professional toolkit on Android.

radare2 C Linux/Windows/macOS/Android Unix-like reverse engineering framework and commandline tools.

Wifiphisher Python Linux The Rogue Access Point Framework.

Beef Javascript Linux/Windows/macOS The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Mobile Security Framework (MobSF) Python Linux/Windows/macOS Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

Burp Suite Java Linux/Windows/macOS Burp Suite is a leading range of cybersecurity tools, brought to you by PortSwigger. This tool is not free and open source

(Table of Contents)

Additional resources

Devbreak on Twitter

The Life of a Security Researcher

Find an awesome hacking spots in your country

Awesome-Hacking Lists

Crack Station

Exploit Database

Hackavision

Hackmethod

Packet Storm Security

SecLists

SecTools

Smash the Stack

Don't use VPN services

How to Avoid Becoming a Script Kiddie

2017 Top 10 Application Security Risks

Starting in cybersecurity ?

Books / Manuals

Warning : I haven't read them all so do not consider I am recommending as I liked them. They just seem to provide useful resources.

Penetration Testing: A Hands-On Introduction to Hacking (2014)

Kali Linux Revealed - PDF (2017)

Blue Team Field Manual (BTFM) (2017)

Cybersecurity - Attack and Defense Strategies (2018)

NMAP Network Scanning : Official Discovery (2009)

Social Engineering : The Art of Human Hacking (2010)

Incognito Toolkit: Tools, Apps, and Creative Methods for Remaining Anonymous (2013)

Discussions

Reddit/HowToHack Learn and ask about hacking, security and pen testing.

Reddit/hacking Discuss about hacking and web security.

ax0nes Hacking, security, and software development forum.

0Day.rocks on discord Discord server about the 0day.rocks blog for technical and general InfoSec/Cyber discussions & latest news.

Reddit/AskNetsec Discuss about network security, ask professionals for advices about jobs and stuff.

Security Advisories

CVE

CWE

NVD

Challenges

Vulnhub - Has a lot of VMs to play with. Some are beginner friendly, some aren't.

Itsecgames - bWAPP or buggy web app is a deliberately insecure web application.

Dvwa - Damn Vulnerable Web Application is another deliberately insecure web application to practice your skills on.

Hackthissite - A site which provides challenges, CTFs, and more to improve your hacking skills.

Defend the Web - Defend the Web is an interactive security platform where you can learn and challenge your skills.

Root-me - Another website which hosts challenges to test your hacking skills.

HackTheBox - An online platform to test and advance your skills in penetration testing and cyber security.

Overthewire - Learn and practice security concepts in the form of fun-filled games.

Ctftime - The de facto website for everything CTF related.

TryHackMe - TryHackMe is a free online platform for learning cyber security, using hands-on exercises and labs.

PicoCTF - Provides you with fun CTF challenges of varying levels of difficulty to practice on.

(Table of Contents)

License

This repository is under MIT license.

(Table of Contents