Home › Hacking › Hacking Cheat Sheet for Pro Hackers/Security Professionals 2020

Hacking

Hacking Cheat Sheet for Pro Hackers/Security Professionals 2020

By **Shaheer** - October 7, 2019 0

f Facebook | Twitter | Pinterest | in Linkedin

Hacking Cheat Sheet for Pro Hackers and Security Professionals 2020

Today the field of cybersecurity is spreading is vast dimensions. One needs to learn a lot of new techniques and get a hold on a lot of tools to execute. For a hacker, a lot of

Follow SecuredYou

| 35 Fans | 749 Followers | 13 Followers |

Latest Articles

How to Permanently Delete your Skype Account 2020 (2 Methods)
October 12, 2019

AndroRAT APK Free Download 2019 – Android Hacking App
October 12, 2019

THC Hydra Free Download 2019 – Best Password Brute Force Tool
October 12, 2019

Top 13 Ways on How to Secure your Windows Server from Hackers
October 10, 2019

How to Format your Hard Drive (HDD) Securely using DBAN 2020
October 10, 2019

things must be there on his mind from the early stages of information gathering to post-exploitation cleaning up. If he makes one single mistake, then that can lead his success to failure within minutes. It, however, can be a little daunting for all of us.

In this **hacking cheat sheet 2020**, we are going to provide you with information that is going to be important for everyone from a beginner to an expert. He shall need this for offensive and defensive hacking.

Contents [hide]

How To Remove Malware from your Windows 10/8/7 PC in 2020

October 10, 2019

Hacking Cheat Sheet – Do you have one?

The tool kit that you have is of prior importance. It is going to be both your weapon and your shield. This is the most challenging asset that you are going to have, second only to actual hand-on experience. Following are the tool that you must have in your toolbox:

- **File search utility:** This is the File Locator
- **Web application vulnerability scanning software:** This is the Acunetix Web Vulnerability Scanner, AppSpider
- **Database security scanners:** SQLPing3
- **Exploit software:** Metasploit
- **Password cracking software:** Ophcrack, Proactive Password Auditor
- **Network scanners:** Nmap, NetScanTools
- **Network vulnerability scanning software:** LanGuard, Nexpose
- **Network analyzing:** Cain & Abel, CommView
- **Wireless network analyzers:** Aircrack-ng, CommView for WiFi

This is, however, just the guideline and not the complete list. These are only the standard tools that one refers to again and again.

Common Hacking Attack Vectors to know

All the hackers and penetration testers out there have different ways of doing things, but they usually are different colors of the same wheel. Consider the following items that are common attack vectors:

- Often people tend to get lazy and then choose passwords that are weal
- Most of us get annoyed with update notifications and close them frequently thus leaving them with potentially vulnerable software
- As a user, you will never expect to be open to an attack. Due to this belief, it does happen to them

It all makes sense that you need to begin your test with the most common vulnerabilities. Whenever you are carrying out a penetration test, the following security flaws must be there at the top of your checklist:

- Overly trusting users and Gullible

- Unsecured computer room entrances
- Unsecured building entrances
- Hard disks and pen drives that are the most common storage devices are not securely erased of the sensitive data
- There is no firewall protection in the network perimeters
- There is a lack of intrusion detection systems
- Default passwords
- The file and share access controls are either weak, inappropriate or entirely missing
- Online access portals have a soft authentication mechanism
- Have unpatched systems which could be easily exploited by using popular tools like Metasploit
- The password storage methods are either insufficient or outdated like the MD5 hash
- Carry insecure routers
- Consist of guest wireless networks that give access to the public to connect to a corporate network environment
- The employee hardware lacks full disk encryption
- The mobile devices have little to no mandatory protection
- Have weak or no passwords for applications, database, and operating systems

Most Commonly Hacked Ports

Today almost everyone knows how to secure standard ports like TCP port 80 (HTTP), but other ports might get overlooked and hence be open to attacks. Whenever you are testing for security you need to check these commonly hacked UDP and TCP ports according to Dummies:

- TCP port 443 — HTTP(Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
- TCP port 110 — POP3(Post Office Protocol version 3)
- TCP and UDP port 135 — Windows RPC
- TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP
- TCP port 1433 and UDP port 1434 — Microsoft SQL Server
- TCP port 21 — FTP(File Transfer Protocol)
- TCP port 22 — SSH(Secure Shell)
- TCP port 23 — Telnet
- TCP port 25 — SMTP(Simple Mail Transfer Protocol)
- TCP and UDP port 53 — DNS(Domain Name System)

SEE ALSO: SAMInside Free Download – Windows Logon Recovery Tool.

Best Practices with Port Security

Whenever you are dealing with ports, you need to keep the following points in your mind:

- You need to avoid using default ports like 22 for SSH whenever it is possible
- You need to flag and block attempts for bulk port scanning. A professional user is not going to ping every single port at one time sequentially. This might not be enough to prevent the attack (a smart hacker is one that can query ports in random order from different IP addressed), but at least you shall be alerted.
- According to the rule of thumb, all the ports (except 80 and 443, i.e. HTTP and HTTPS) must require authentication to allow connection unless and until there is an excellent reason not to.

Top Hacking Tips for Beginners in Hacking

If you are a hacker, then the following tips are going to be very handy for you:

- Before you get started with anything you need to define your goals and develop your plan
- Whatever you are trying to do, you must have permission for that otherwise there is a thin boundary between doing things legally

and illegally

- You must use the right tools for the task you are going to do
- You need to keep in mind that it is nearly impossible to check for every security vulnerability on every system, but when you have a plan this becomes easy as well
- You should not overlook the non-technical security issues as they are exploited first. For example social engineering in an insecure server room
- You need to treat the other people's confidential information as you treat yours as a violation of privacy is not a game.

SEE ALSO: Wfuzz Free Download – #1 Web Application Hacking Tool.

Ethical Hacking Tips for Security Analysts

If you are a professional security analyst, then the following tips are going to be very handy for you:

- You need to make sure that you are not interfering in the work of your clients when you are pen testing for them.
- You need to know and be aware that the attacks can come from inside as well as from outside

- When you are testing you need to keep the key players in the loop
- Make sure to report for critical vulnerabilities
- As a security analyst, you must study malicious hackers and rogue inside behaviors and black hat tactics. The more you know, the more it gets more comfortable for you to test your systems for security vulnerabilities
- Your testing must be above board
- You should not treat vulnerability that is discovered in the same manner, as all weaknesses are not bad. You must evaluate the context of the issue
- You need to show customers and management that security testing is indeed a good job, and you are the right one to do it. Just find what matters most and do we repeat we do comply with the different laws and regulations.

This, however, is just a little cheat sheet with the help of which you shall be able to hack more efficiently and get successful quite often.

SEE ALSO: Ncrack Free Download – Network Hacking Tool.

Essential Security Guides

- How to Hack WPA-3 WiFi Networks using new Vulnerabilities.

- How to Secure your WiFi Router.
- How to Hack Any SQL Database Server.
- Kali Linux Hacking Tutorial for Beginners.
- How to Secure your Facebook Account from Hackers.
- How to Secure your Linux Server.
- How to Format your Hard Drive Securely and Permanently using DBAN.

TAGS ethical hacking cheat sheet ethical hacking guide hacking cheat sheet hacking tools hacking tutorials

Share Facebook Twitter Pinterest Linkedin

Shaheer

https://securedyou.com/

Shaheer is the founder of Secured You. He is a cybersecurity freak and loves anything related to Computers, Hacking, Artificial Intelligence and Technology. Apart from being a tech geek, he loves listening to music.

RELATED ARTICLES MORE FROM AUTHOR

Hacking

How to Hack Any SQL Database Password in 2019 – Cracking SQL

Hacking

How to Prevent SQL Injection Attacks 2019 – Protect Against SQL Hacking

Hacking

How to Hack WPA3 WiFi Passwords – Side-channel Attack Method

Hacking

Commando VM Download – Free Windows-based Hacking Distribution

Hacking

Top 9 Best Microsoft Windows CMD Hacking Commands 2019 (New)

Hacking

Cybersecurity and Ethical Hacking Terms 2019 – (Lingo, Acronym, Slang)

‹ ›

LEAVE A REPLY

Comment:

Name:*

Email:*

Website:

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment