PENTEST WITH METASPLOIT - OVERVIEW

JOAS ANTONIO

DETAILS

- This PDF was created to help PenTest professionals and those who are starting to use the Metasploit tool
- https://www.linkedin.com/in/joas-antonio-dos-santos

INTRODUCTION

WHAT IS

- The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.
- Creator – H.D Moore in 2003
- Acquired by Rapid7
- Written in Ruby

WHAT IS

- Penetration testing, often called “pentesting”, “pen testing”, "network penetration testing", or “security testing”, is the practice of attacking your own or your clients’ IT systems in the same way a hacker would to identify security holes. Pen testing tries to gain control over systems and obtain data. The person carrying out a penetration test is called a penetration tester or pen tester. For the rest of the article, we will refer to it as a pen test or pen testing.
-

WHAT IS - PENTEST

- A pen test is designed to detect openings in your security. Simulating an attack on yourself is a great way to make sure you are prepared for a breach and learn where you are exposed.

PENTEST STEPS

Each pen test might have different steps, but a pen test generally has the following:

- Set the scope
- Reconnaissance
- Discovery
- Exploitation
- Brute Forcing
- Social Engineering
- Take Control
- Pivoting
- Gather Evidence
- Cleanup
- Report
- Remediation

GLOSSARY

Auxiliary Module

An auxiliary module does not execute a payload and perform arbitrary actions that may not be related to exploitation. Examples of auxiliary modules include scanners, fuzzers, and denial of service attacks.

Bind Shell Payload

A bind shell attaches a listener on the exploited system and waits for the attacking machine to connect to the listener.

GLOSSARY

Database

The database stores host data, system logs, collected evidence, and report data.

Discovery Scan

A discovery scan is a Metasploit scan that combines Nmap and several Metasploit modules to enumerate and fingerprint targets.

Email Template

An email template contains predefined HTML content that you can insert into an email.

Exploit

An exploit is a program that takes advantage of a specific vulnerability and provides an attacker with access to the target system. An exploit typically carries a payload and delivers it to a target. For example, one of the most common exploits is windows/smb/s08-067_netapi, which targets a Windows Server Service vulnerability that could allow remote code execution.

GLOSSARY

Exploit Module

An exploit module executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit module takes advantage of a vulnerability to provide access to the target system. Exploit modules include buffer overflow, code injection, and web application exploits.

Executable

An executable file that automatically runs when a human target opens the file. The executable runs a payload that creates a connection from the exploited machine back to the attacking machine.

File Format Exploit

A file format exploit targets a vulnerability in a specific application, such as Microsoft Word or Adobe PDF.

Human Target

A human target is the person who receives the social engineering attack or is part of a campaign.

GLOSSARY

Listener

A listener waits for an incoming connection from either the exploited target or the attacking machine and manages the connection when it receives it.

Meterpreter

Meterpreter is an advanced multi-function payload that provides you an interactive shell. From the Meterpreter shell, you can do things like download a file, obtain the password hashes for user accounts, and pivot into other networks. Meterpreter runs on memory, so it is undetectable by most intrusion detection systems.

Module

Most of the tasks that you perform in Metasploit require the use of a module, which is a standalone piece of code that extends the functionality of the Metasploit Framework. A module can be an exploit, auxiliary or post-exploitation module. The module type determines its purpose. For example, any module that can open a shell on a target is considered an exploit module. A popular exploit module is MS08-067.

GLOSSARY

Payload

A payload is the shell code that runs after an exploit successfully compromises a system. The payload enables you to define how you want to connect to the shell and what you want to do to the target system after you take control of it. A payload can open a Meterpreter or command shell. Meterpreter is an advanced payload that allows you to write DLL files to dynamically create new features as you need them. A payload can be a reverse shell payload or a bind shell payload. The major difference between these payloads is the direction of the connection after the exploit occurs.

Phishing Attack

A phishing attack is a form of social engineering that attempts to acquire sensitive information, such as usernames, passwords, and credit card information, from a human target. During a phishing attack, a human target receives a bogus email disguised as an authentic email from a trusted source, like the bank. Generally, the email contains a link that opens a fake web page that looks nearly identical to the official site. The style, logo, and other images may appear exactly as they are on the real website.

GLOSSARY

Portable File

A generated executable file that you can attach to an email or save to a USB key. When the victim opens the file, the executable runs the payload, starts a session on the victim's machine, and connects back to your machine.

Project

All work in Metasploit Pro must be done inside of a project. A project is a container for the targets, tasks, reports, and data that are part of a penetration test. A project contains the workspace that you use to create a penetration test and configure tasks. Every penetration test runs from within a project.

Post-Exploitation Module

A post-exploitation module enables you to gather more information or to gain further access to an exploited target system. Examples of post-exploitation modules include hash dumps and application and service enumerators.

Resource File

A resource file refers to a web page template, email template, or target list. It is a reusable file that you can use in a campaign. Each project has its own set of resource files. The resource files are not shareable between projects.

GLOSSARY

Reverse Shell Payload

A reverse shell connects back to the attacking machine as a command prompt.

Shell

A shell is a console-like interface that provides you with access to a remote target.

Shellcode

Shellcode is the set of instructions that an exploit uses as the payload.

Target List

A target list defines the targets that you want to include in the social engineering campaign. You use the target list to specify the recipients that you want to email the social engineering attack.

Task

A task is an action that Metasploit Pro can perform. Examples of tasks include performing a scan, running a bruteforce attack, exploiting a vulnerable target, or generating a report.

GLOSSARY

Tracking Link

A tracking link consists of a URL path to a web page and a tracking string. When a target clicks on the URL, the system sets a cookie to track the visit and any subsequent visits.

Tracking GIF

A tracking GIF sets a browser cookie when a human target opens an email.

Tracking String

A tracking string is a 64-bit string that encodes the target and email IDs. Campaigns use tracking strings to monitor the activity of a target.

Vulnerability

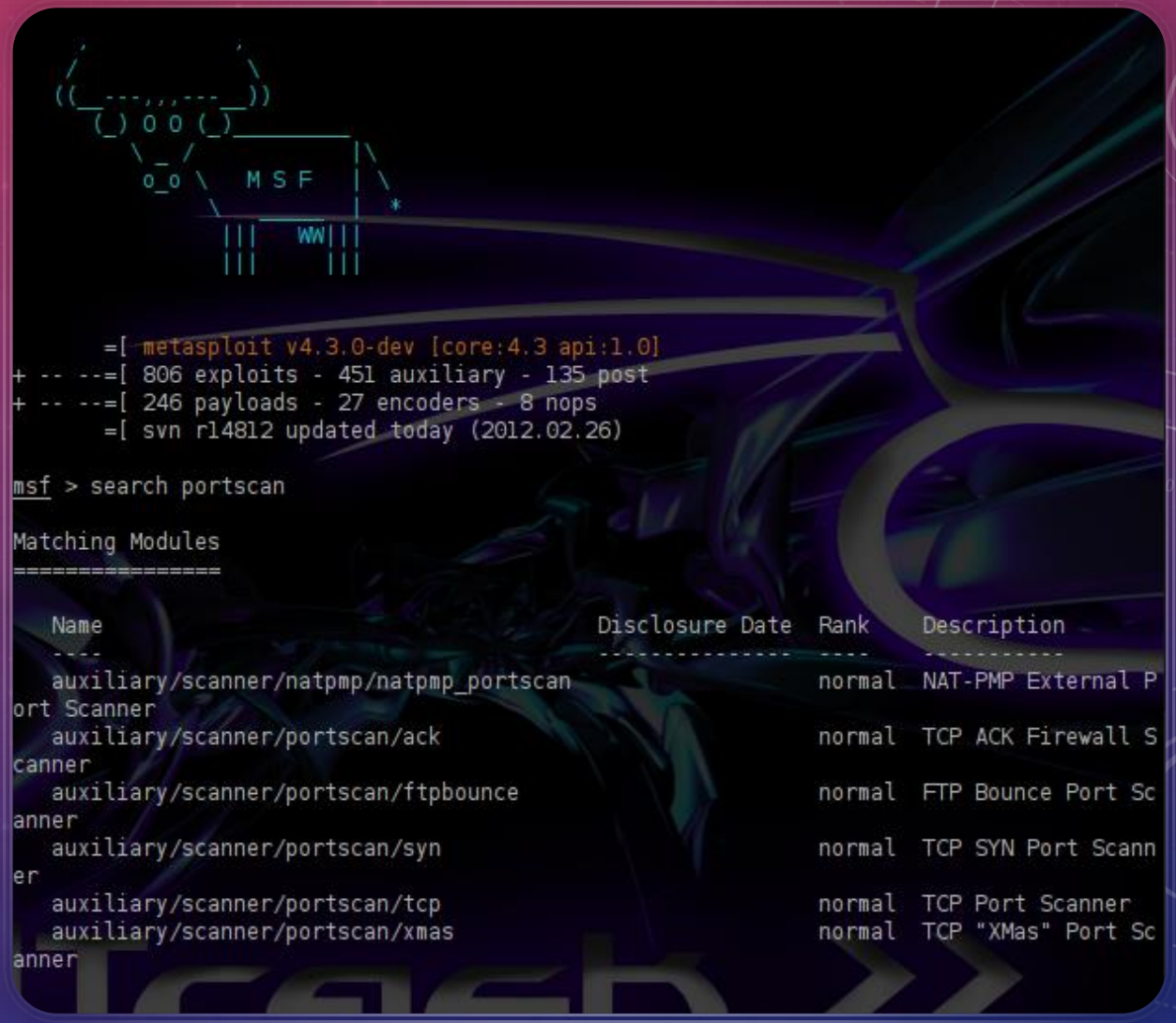
A vulnerability is a security hole in a piece of software, hardware or operating system that provides a potential angle to attack the system. A vulnerability can be as simple as weak passwords or as complex as buffer overflows or SQL injection vulnerabilities. A compromised system can result in privilege escalation, denial-of-service, unauthorized data access, stolen passwords, and buffer overflows.

https://docs.rapid7.com/metasploit/metasploit-basics

PRACTICE

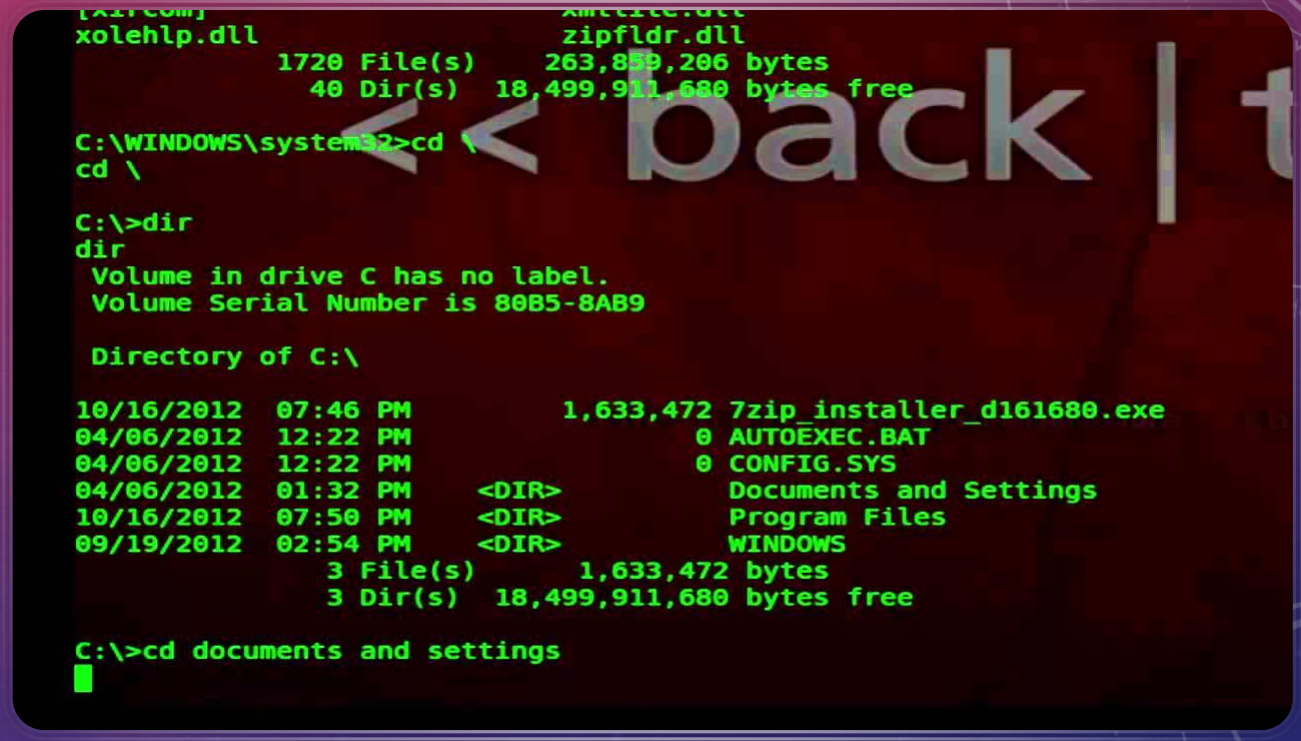
PORTSCAN

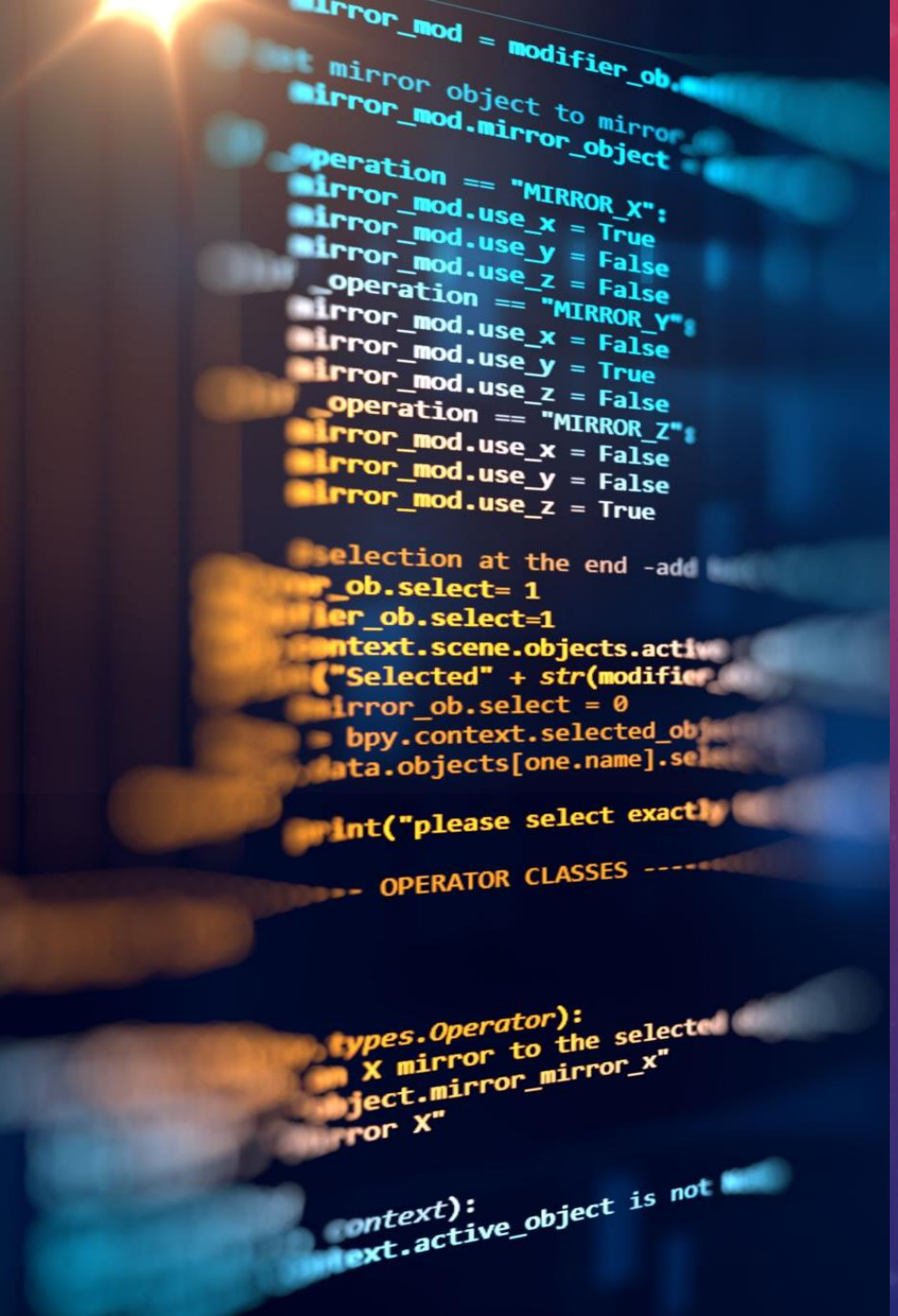
- https://securityonline.info/ports-scanning-using-metasploit/
- https://www.offensive-security.com/metasploit-unleashed/port-scanning/
- https://pentestlab.blog/2012/02/26/port-scanning-with-metasploit/
- https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities
- https://null-byte.wonderhowto.com/how-to/discover-open-ports-using-metasploits-built-port-scanner-0186829/
- https://www.youtube.com/watch?v=L3ZWsYapxus&ab_channel=LimJetWee



RPC DCOM

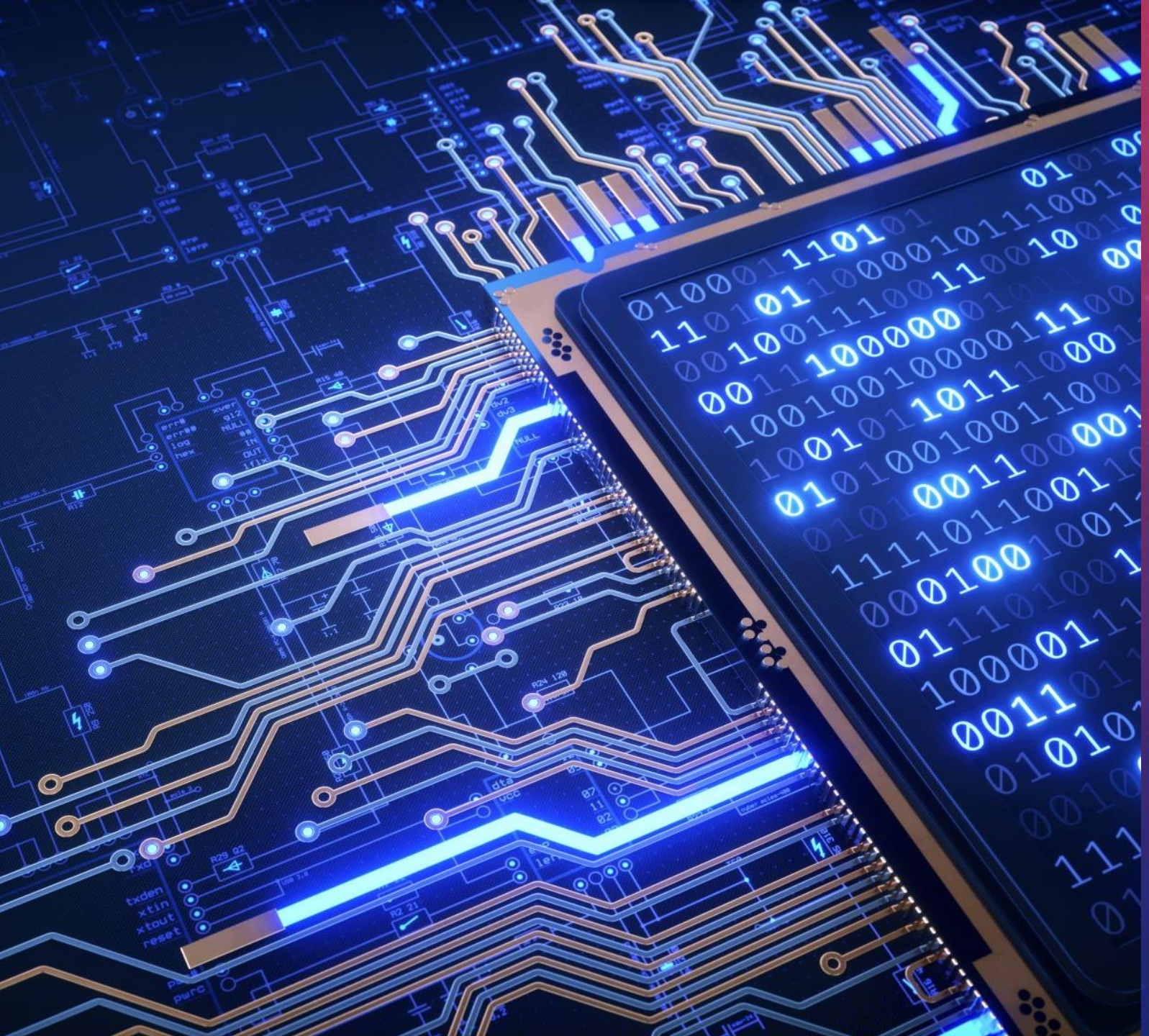
- https://www.rapid7.com/db/modules/exploit/windows/dcerpc/ms03_026_dcom/
- https://www.youtube.com/watch?v=oavnHMNsebo&ab_channel=AngelosVasilopoulos
- https://www.youtube.com/watch?v=gAlGRlf_fDY&ab_channel=MarufParkar
- https://security.stackexchange.com/questions/76889/ms03-026-rpc-dcom-exploit-not-working-on-metasploit
- https://www.exploit-db.com/exploits/66
- https://pentestlab.blog/tag/dcom-exploit/





PAYLOAD CONFIG

- https://docs.rapid7.com/metasploit/working-with-payloads/
- https://docs.rapid7.com/metasploit/the-payload-generator/
- https://www.offensive-security.com/metasploit-unleashed/generating-payloads/
- https://www.offensive-security.com/metasploit-unleashed/exploits/
- https://hatching.io/blog/metasploit-payloads/
- https://netsec.ws/?p=331
- https://www.tutorialspoint.com/metasploit/metasploit_payload.htm



MSFCONSOLE COMMANDS

- https://www.hackingtutorials.org/metasploit-tutorials/metasploit-commands/
- https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/
- https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
- https://pentestlab.blog/2012/03/13/msfconsole-commands-cheat-sheet/
- https://www.youtube.com/watch?v=gWKyFYMY_Pk&ab_channel=Hak5

PAYLOAD TYPES

- https://www.offensive-security.com/metasploit-unleashed/payloads/#:~:text=A%20payload%20in%20Metasploit%20refers,across%20numerous%20types%20of%20scenarios.
- https://www.offensive-security.com/metasploit-unleashed/payload-types/
- https://www.sciencedirect.com/topics/computer-science/payload-module
- https://www.helloitsliam.com/2016/02/10/understanding-metasploit-payloads/
- https://hackmag.com/security/metasploit-guide/

METASPLOIT CONFIG

- https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
- https://tools.kali.org/exploitation-tools/metasploit-framework
- https://computingforgeeks.com/install-and-run-metasploit-framework-on-kali-linux/
- https://www.youtube.com/watch?v=s08FVeHY6qw&ab_channel=HackerSploit
- https://github.com/scriptjunkie/msfgui
- https://www.offensive-security.com/metasploit-unleashed/metasploit-guis/
- https://www.gitmemory.com/issue/scriptjunkie/msfgui/2/497212034

ARMITAGE

- https://www.offensive-security.com/metasploit-unleashed/armitage/
- https://www.offensive-security.com/metasploit-unleashed/armitage-exploitation/
- https://www.youtube.com/watch?v=RtAhCwe5-7g&ab_channel=WorldGurukul
- https://www.youtube.com/watch?v=EACo2q3kgHY&ab_channel=RaphaelMudge
- https://www.youtube.com/watch?v=JALmoY4LuT8&ab_channel=HackerSploit
- http://www.fastandeasyhacking.com/manual
- https://seginfo.com.br/2011/09/12/armitage-ferramenta-de-gerenciamento-de-ataques-para-o-metasploit-2/
- https://under-linux.org/entry.php?b=3031
- https://www.vivaolinux.com.br/artigo/Armitage-a-nova-interface-grafica-do-Metasploit
- https://en.wikipedia.org/wiki/Armitage_(computing)

INITIAL ACCESS

- https://www.youtube.com/watch?v=NTdthBQYa1k&ab_channel=Hak5
- https://www.youtube.com/watch?v=JUDkziT2tAw&ab_channel=Hak5
- https://www.youtube.com/watch?v=gWKyFYMY_Pk&ab_channel=Hak5
- https://www.youtube.com/watch?v=TCPyoWHy4eA&ab_channel=Hak5
- https://labs.f-secure.com/blog/attack-detection-fundamentals-initial-access-lab-4/
- https://resources.infosecinstitute.com/topic/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/
- https://www.dailymotion.com/video/x37bbea
- https://www.offensive-security.com/metasploit-unleashed/generating-payloads/
- https://www.youtube.com/watch?v=hollnezbeus&ab_channel=zSecurity
- https://www.youtube.com/watch?v=WNKr2TgJsGc&ab_channel=TheSolutionHub
- https://docs.rapid7.com/metasploit/best-practices-for-social-engineering/
- https://www.tutorialspoint.com/metasploit/metasploit_social_engineering.htm
- https://www.youtube.com/watch?v=gKykLr59LW8&ab_channel=CryptoCat
- https://www.youtube.com/watch?v=QU2l36LQQFU&ab_channel=PacktVideo
- https://shehackske.medium.com/creating-a-backdoor-using-social-engineering-toolkit-set-c5ce486aab5

SEARCH EXPLOITS

- https://www.offensive-security.com/metasploit-unleashed/searching-content/
- https://medium.com/quiknapp/how-to-load-and-use-exploit-in-metasploit-61b4f10ceb9d
- https://medium.com/swlh/intro-to-metasploit-19e3d07ff725
- https://www.blackmoreops.com/2015/11/03/how-to-search-exploits-in-metasploit/
- https://www.exploit-db.com/searchsploit

EXPLOITS

- https://www.offensive-security.com/metasploit-unleashed/using-exploits/
- https://docs.rapid7.com/metasploit/using-exploits/
- https://ironlinux.com.br/explorando-vulnerabilidade-metasploit/
- https://www.exploit-db.com/
- https://www.infosecmatter.com/list-of-metasploit-windows-exploits-detailed-spreadsheet/
- https://www.youtube.com/watch?v=8lR27r8Y_ik&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=TieUDcbk-bg&ab_channel=LoiLiangYang
- https://www.youtube.com/watch?v=kIkfCNO904w&ab_channel=CrazyNet

CREATE MODULES

- https://www.youtube.com/watch?v=YQj8FaQ8B5w&ab_channel=KacperSzurekEN
- https://www.offensive-security.com/metasploit-unleashed/writing-an-exploit/
- https://github.com/rapid7/metasploit-framework/wiki
- https://www.rapid7.com/blog/post/2012/07/05/part-1-metasploit-module-development-the-series/
- https://linuxhint.com/writing_exploit_metasploit/
- https://www.offensive-security.com/metasploit-unleashed/building-module/
- https://www.offensive-security.com/metasploit-unleashed/creating-auxiliary-module/
- https://www.youtube.com/watch?v=SOy87RUjsoU&ab_channel=Hak5
- https://www.youtube.com/watch?v=YQj8FaQ8B5w&ab_channel=KacperSzurekEN
- https://subscription.packtpub.com/book/networking-and-servers/9781788624480/7/ch07lvl1sec57/writing-your-own-metasploit-module
- https://teamrot.fi/how-to-metasploit-exploit-development/
- https://docs.rapid7.com/metasploit/modules/

PRIVILEGE ESCALATION

- https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/
- https://medium.com/@cmpbilge/privilege-escalation-with-meterpreter-3e3f999d9978
- https://www.youtube.com/watch?v=xsyeL6xWWy4&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=BAndD6a4wA0&ab_channel=MotasemHamdan
- https://www.youtube.com/watch?v=ajFvcCaiIOA&ab_channel=GusKhawaja
- https://null-byte.wonderhowto.com/how-to/get-root-with-metasploits-local-exploit-suggester-0199463/
- https://www.rapid7.com/db/modules/exploit/windows/local/service_permissions/
- https://www.exploit-db.com/exploits/47307
- https://www.exploit-db.com/docs/english/18229-white-paper--post-exploitation-using-meterpreter.pdf
- https://ethicalhackingblog.com/practical-privilege-escalation-using-meterpreter/
- https://hackerculture.com.br/?p=1211
- https://bugtestlab.com/?p=794
- https://www.infosecmatter.com/metasploit-android-modules/
- https://labs.f-secure.com/advisories/metasploit-pro-root-privilege-escalation/
- https://pentestlab.blog/category/privilege-escalation/

POST EXPLOITATION

- https://www.offensive-security.com/metasploit-unleashed/post-module-reference/
- https://www.offensive-security.com/metasploit-unleashed/msf-post-exploitation/
- https://www.youtube.com/watch?v=o89WoOnIzT4&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=fZzmpb_x0Cg&ab_channel=PacktVideo
- https://www.youtube.com/watch?v=3A7fJUGfNtk&ab_channel=PentesterAcademyTV
- https://docs.rapid7.com/metasploit/about-post-exploitation/
- https://www.infosecmatter.com/post-exploitation-metasploit-modules-reference/
- https://linuxhint.com/meterpreter_post_exploitation/
- https://subscription.packtpub.com/book/networking_and_servers/9781788990615/8/ch08lvl1sec47/basic-post-exploitation-commands
- https://pentestlab.blog/2013/01/04/post-exploitation-in-linux-with-metasploit/
- https://sushant747.gitbooks.io/total-oscp-guide/content/getting_meterpreter_shell.html
- https://labs.bishopfox.com/industry-blog/9-post-exploitation-tools-for-your-next-penetration-test

PIVOTING

- https://www.offensive-security.com/metasploit-unleashed/pivoting/
- https://blog.pentesteracademy.com/network-pivoting-using-metasploit-and-proxychains-c04472f8eed0
- https://www.tutorialspoint.com/metasploit/metasploit_pivoting.htm
- https://medium.com/swlh/metasploit-pivoting-281636b23279
- https://www.youtube.com/watch?v=MeSql-3aOsM&ab_channel=Hak5
- https://www.youtube.com/watch?v=bHEGzRInMPQ&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=0lJ0a3E4lWc&ab_channel=SecuriumSolutions
- https://medium.com/@viniciuskmax/conhe%C3%A7a-o-packet-pivoting-t%C3%A3o-aguardado-novo-recurso-do-metasploit-fd33c6d8f414
- https://www.ivoidwarranties.tech/posts/pentesting-tuts/pivoting/meterpreter/

METERPRETER

- https://medium.com/canivete-sui%C3%A7o-hacker/metasploit-dismistificado-ii-5-b6d3dc47b83c#:~:text=O%20Meterpreter%20%C3%A9%20uma%20payload,completion%2C%20canais%20e%20outras%20fun%C3%A7%C3%B5es.
- https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
- https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/
- https://danieldonda.com/metasploit-framework-meterpreter/
- https://ironlinux.com.br/msfvenom-cheatsheet/
- https://docs.rapid7.com/metasploit/use-meterpreter-locally-without-an-exploit/
- https://www.offensive-security.com/metasploit-unleashed/custom-scripting/
- https://www.offensive-security.com/metasploit-unleashed/writing-meterpreter-scripts/
- https://www.hackers-arise.com/post/2018/06/27/metasploit-basics-part-12-creating-rc-scripts
- https://www.oreilly.com/library/view/metasploit/9781593272883/ch16s04.html
- https://www.blueliv.com/downloads/Meterpreter_cheat_sheet_v0.1.pdf
- https://subscription.packtpub.com/book/networking_and_servers/9781788623179/4/ch04lvl1sec62/meterpreter-resource-scripts
- https://rubyfu.net/module-0x5-or-exploitation-kung-fu/metasploit/meterpreter/meterpreter-scripting
- https://github.com/CyberSecurityUP/First-Script-Meterpreter

LATERAL MOVEMENT

- https://pentestlab.blog/2020/07/21/lateral-movement-services/
- https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f
- https://www.mindpointgroup.com/blog/lateral-movement-with-psexec
- https://labs.f-secure.com/blog/attack-detection-fundamentals-discovery-and-lateral-movement-lab-4/
- https://www.offensive-security.com/metasploit-unleashed/pivoting/
- https://www.hackingarticles.in/lateral-movement-pass-the-hash-attack/
- https://www.hackingarticles.in/lateral-movement-wmi/
- https://nv2lt.github.io/windows/smb-psexec-smbexec-winexe-how-to/
- https://blog.palantir.com/restricting-smb-based-lateral-movement-in-a-windows-environment-ed033b888721

CLEAR TRACKS

- https://www.offensive-security.com/metasploit-unleashed/event-log-management/
- https://www.hackingarticles.in/delete-firewall-log-remote-pc-using-metasploit/
- https://null-byte.wonderhowto.com/how-to/clear-logs-bash-history-hacked-linux-systems-cover-your-tracks-remain-undetected-0244768/
- http://index-of.es/Varios-2/Clear%20Logs%20!.pdf
- https://www.youtube.com/watch?v=TgquV_OA-lU&ab_channel=HackerSploit
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/

DATA EXFILTRATION

- https://www.linkedin.com/pulse/data-exfiltration-metasploit-meterpreter-dns-tunnel-alexey-sintsov/
- https://www.pentestpartners.com/security-blog/data-exfiltration-techniques/
- https://sudonull.com/post/64015-Metasploit-exfiltration-DNS-tunnel-for-Meterpreter
- https://www.rapid7.com/db/modules/auxiliary/server/icmp_exfil/
- https://www.hacktoday.io/t/data-exfiltration-with-metasploit-meterpreter-dns-tunnel/512
- https://cyberlab.pacific.edu/courses/comp178/labs/lab-5-exploitation
- https://blog.gaborszathmari.me/data-exfiltration-with-wordpress-xss/
- http://masshackers.pbworks.com/w/file/fetch/53013655/ohdae-beacon2012.pdf
- https://www.defensive-security.com/blog/meterpreter-payload-delivery-using-dns-axfr-poc

BACKDOOR AND PERSISTENCE

- https://www.offensive-security.com/metasploit-unleashed/meterpreter-backdoor/
- https://apprize.best/security/penetration/8.html
- https://www.hackingu.com.br/2019/03/10/backdoor-persistente-com-o-metasploit/?utm_source=rss&utm_medium=rss&utm_campaign=backdoor-persistente-com-o-metasploit
- https://github.com/Screetsec/Vegile
- https://www.sciencedirect.com/topics/computer-science/backdoors
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-hijack-software-updates-install-rootkit-for-backdoor-access-0149225/
- https://sectechno.com/vegile-tool-for-setting-up-backdoors-and-rootkits/
- https://www.darkoperator.com/blog/2009/12/31/meterpreter-persistance.html
- https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/
- https://pentestlab.blog/2012/03/17/metasploit-persistent-backdoor/
- https://pentestlab.blog/2020/02/04/persistence-waitfor/
- https://www.darkoperator.com/blog/2009/12/31/meterpreter-persistance.html
- https://secnhack.in/technique-to-persistence-on-windows-10-with-metasploit/
- https://sushant747.gitbooks.io/total-oscp-guide/content/persistence.html

RUBY FOR METASPLOIT

- https://www.reddit.com/r/netsec/comments/ikebb/metasploit_is_it_worth_the_time_to_learn_ruby/
- https://rubyfu.net/module-0x5-or-exploitation-kung-fu/metasploit
- https://subscription.packtpub.com/book/networking_and_servers/9781788624596/14/ch14lvl1sec90/ruby-the-heart-of-metasploit
- https://hub.packtpub.com/ruby-and-metasploit-modules/
- https://github.com/rapid7/metasploit-framework
- https://www.darkoperator.com/blog/2017/10/22/switching-ruby-version-in-rvm-for-metasploit-development

AUTOMATE EXPLOIT

- https://www.youtube.com/watch?v=ycKLeh2KgGw&ab_channel=MotasemHamdan
- https://www.youtube.com/watch?v=qj3-3ZKixiM&ab_channel=EthicalHackingandDigitalForensicsTutorial
- https://www.youtube.com/watch?v=zaE6_9sNLvM&ab_channel=HackerAssociate
- https://www.rapid7.com/blog/post/2011/12/08/six-ways-to-automate-metasploit/
- https://docs.rapid7.com/metasploit/auto-exploitation
- https://kalilinuxtutorials.com/exploitivator-metasploit-scanning-exploitation/
- https://thedarksource.com/easysploit-metasploit-automation-tool/
- https://medium.com/swlh/metasploit-framework-basics-part-1-manual-to-automatic-exploitation-8182d0917193

MSFVENOM AND ENCODING

- https://www.offensive-security.com/metasploit-unleashed/generating-payloads/
- https://ironlinux.com.br/msfvenom-cheatsheet/
- https://medium.com/@PenTest_duck/offensive-msfvenom-from-generating-shellcode-to-creating-trojans-4be10179bb86
- https://securitytutorials.co.uk/creating-a-payload-with-msfvenom/
- https://www.guiadoti.com/2018/06/metasploit-framework-de-cabo-a-rabo-parte-6/
- https://security.stackexchange.com/questions/154245/encode-an-executable-file-multiple-time-using-msf-venom
- https://ethicaldebuggers.com/msfvenom-create-your-own-payload/
- https://medium.datadriveninvestor.com/creating-windows-os-backdoor-with-msfvenom-ba56567eb088
- https://securityboulevard.com/2020/02/evading-antivirus-with-better-meterpreter-payloads/
- https://failingsilently.wordpress.com/2017/08/05/msfvenom-encoders-and-formats/
- https://book.hacktricks.xyz/shells/shells/msfvenom

CUSTOM BINARIES

- https://www.ired.team/offensive-security/defense-evasion/av-bypass-with-metasploit-templates
- https://www.offensive-security.com/metasploit-unleashed/binary-payloads/
- https://www.offensive-security.com/metasploit-unleashed/binary-linux-trojan/
- https://securityboulevard.com/2020/02/evading-antivirus-with-better-meterpreter-payloads/
- https://docs.rapid7.com/metasploit/the-payload-generator/
- https://netsec.ws/?p=331
- https://subscription.packtpub.com/book/networking_and_servers/9781788623179/5/ch05lvl1sec82/backdooring-windows-binaries
- http://insecurety.net/injecting-arbritary-metasploit-payloads-into-windows-executables/
- https://www.passeidireto.com/arquivo/52931774/the-hacker-playbook-3-practical-guide-to-penetration-testing/47

DLL INJECTION

- https://pentestlab.blog/2017/04/04/dll-injection/
- https://www.youtube.com/watch?v=yKoD5Oy8CKQ&ab_channel=TheRedTeam
- https://www.youtube.com/watch?v=O_bX0I9hF1s&ab_channel=EricRomang
- https://www.youtube.com/watch?v=DjewBjJR0HA&ab_channel=EricRomang
- https://www.drchaos.com/post/malicious-dll-infection-thru-metasploit-smb-exploit
- https://blog.cobaltstrike.com/2012/09/17/delivering-custom-payloads-with-metasploit-using-dll-injection/
- https://www.ired.team/offensive-security/code-injection-process-injection/reflective-dll-injection

WEB SERVER AND APPLICATIONS

- https://www.offensive-security.com/metasploit-unleashed/wmap-web-scanner/
- https://www.offensive-security.com/metasploit-unleashed/scanner-http-auxiliary-modules/
- https://www.youtube.com/watch?v=7K7kcLJ2sBI&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=fsQ38Xg_U0k&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=YQUcyQ4WT6w&ab_channel=PentesterAcademyTV
- https://www.hackers-arise.com/post/2019/05/06/metasploit-basics-for-hackers-part-26-web-delivery-with-linuxunixosx
- https://www.offensive-security.com/metasploit-unleashed/web-application-exploit-development/
- https://linuxhint.com/metasploit_vurnerability_scanner_linux/
- https://hydrasky.com/network-security/metasploit-for-pentest-web-application/
- https://null-byte.wonderhowto.com/how-to/use-metasploits-wmap-module-scan-web-applications-for-common-vulnerabilities-0187572/

NESSUS AND NMAP

- https://www.offensive-security.com/metasploit-unleashed/nessus-via-msfconsole/
- https://www.offensive-security.com/metasploit-unleashed/working-with-nessus/
- https://pt-br.tenable.com/blog/using-nessus-and-metasploit-together?tns_redirect=true
- https://www.youtube.com/watch?v=3gtVySv4vsk&ab_channel=AlpineSecurity
- https://www.youtube.com/watch?v=hMKIIRhfk74&ab_channel=BhargavTandel
- https://www.youtube.com/watch?v=HHPXDQ-Y2J0&ab_channel=ChuckMoore
- https://www.youtube.com/watch?v=AOkgACXYEmw&ab_channel=OffensiveHacks
- https://www.youtube.com/watch?v=8de06mhTLIA&ab_channel=Caf%C3%A9comC%C3%B3digo-Hacker
- https://www.youtube.com/watch?v=WYhGVPia_Xk&ab_channel=MotasemHamdan
- https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities
- https://www.gdatasoftware.com/blog/2021/05/36810-perform-simple-security-tests-yourself-using-metasploit-framework-and-nmap
- https://linuxhint.com/metasploit_and_nmap_in_kali_linux_2020-1/
- https://motasemhamdan.medium.com/using-metasploit-and-nmap-to-enumerate-and-scan-for-vulnerabilities-ce420c0ce580
- https://null-byte.wonderhowto.com/how-to/use-metasploits-web-delivery-script-command-injection-pop-shell-0189130/