

Previously on Cyber Clinic:

- Linux
 - Navigating through folders, **ifconfig**, **ls**, **cd**, **pwd**
- Nmap
 - Scanning **ports** and **services** on a computer we don't have access to
- Metasploit
 - Using a pre-made script to **exploit** an unpatched vulnerability

DARKNET DIARIES

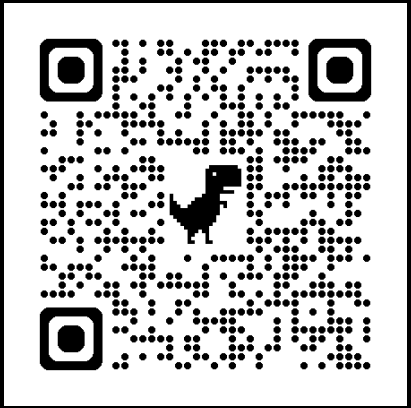
**Last session involved Metasploit.
Episode 114 of Darknet Diaries covers 'HD Moore',
the inventor of Metasploit.**

**You can listen to it on Spotify or
<https://darknetdiaries.com/episode/114/>**

True stories from the dark side of the Internet

This is a podcast about hackers, breaches, shadow government activity, hacktivism, cybercrime, and all the things that dwell on the hidden parts of the network. This is Darknet Diaries.

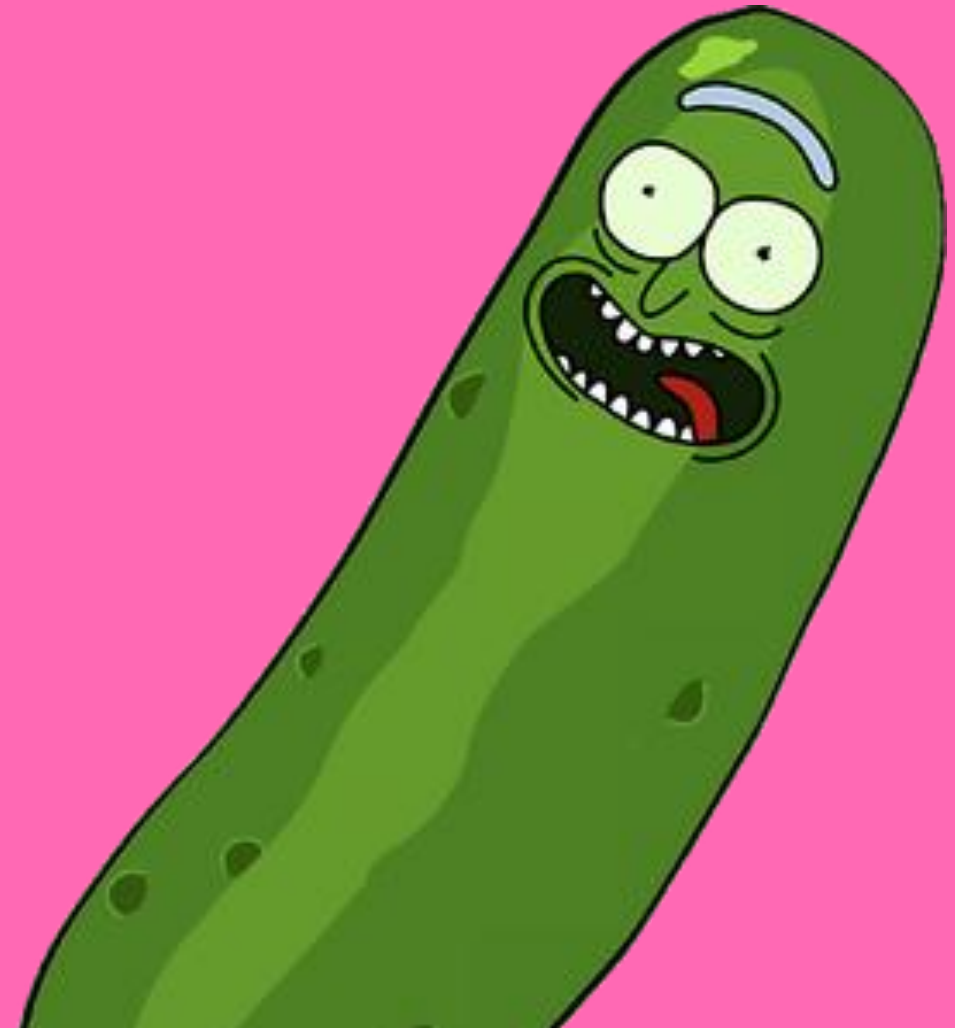
HD: So, I got this alert saying the machine was basically shut down, it crashed. We're capturing all the traffic going in in that machine just fine to start with, but by doing that, we were able to carve out the initial exploit.



Welcome to Cyber Clinic

Session 2

- *Linux file system*
- *Web servers*
- *Domain enumeration*
- *Exploiting Pickle Rick*



What is Cyber Clinic?

(again)

- *Weekly workshops on all kinds of cybersecurity*
- *Not very sequential*
- *Different things every week. Last year included a workshop on lockpicking in the curriculum*
- ***Feel free to suggest topics***
 - *For us to talk about*
 - *For you to give a talk on*

What's the plan?



If we want to hack into a website (web server)

- We have to know how web servers work
 - Ports, domains, structure
- We have to know (*how they run on*) Linux
 - User accounts, linux filesystem
- We have to know the tools at our disposal
 - Vulnerability scanners, domain enumeration

Web Servers



What is a web server?

- A computer that runs web server software and hosts the website files
Apache, NGINX **.html, .css, .js, .php**
They allow access to these website files through a **port**

Ports

- A port is just a number within a message (packet) that lets the server know where the messages you're sending are going
- Web servers typically use ports **80 (HTTP)** and **443 (HTTPS)** but can be hosted on any other port
unencrypted traffic **encrypted traffic**
- There are 65,533 other ports for servers to use – remote desktop, email, file transfer...
- Scanning ports (*sending a sample message to every port and looking for a response*) lets you see everything that server is providing.

How does it work?

Your computer connects to the web server through a web browser.





- All computers have an IP address.
- Typing in '**https://google.com**' is the same as typing in '**172.253.117.100:443**' (the hosting computer's IP and port)
- The prefix of **https://** expects port 443, and **http://** expects port 80 so it's not required to add at the end.

Web Servers

What do web servers actually do???

- A webserver in the simplest terms exposes part of a computer to the internet
- Its down to your web browser how its displayed and web admin on what's reachable

Index of /blog/images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	13-Oct-2006 22:24	-	
 activity-icon.gif	01-Aug-2002 13:52	1k	
 adesso-keyboard.jpg	19-Jan-2006 09:40	10k	
 amazon-uk-dvd-rental..>	21-Aug-2006 00:39	27k	
 american_red_cross.gif	31-Aug-2005 17:15	5k	

Why's this important ?

- Sometimes a web admin may expose more then they want
- We can exploit this using tools like
Gobuster, OWASP Zap, Nikto

Domain enumeration

- Using word lists we can pivot to new subdomains we don't know about
- Webservers have no rate limit like logins do so we can spam the hell out of them



















Remember not all website use /xx try /xx.php and /xx.txt



LINUX FILESYSTEM

Linux File Systems

ByteByteGo.com

/bin		Essential command binaries
/boot		System boot loader files
/dev		Device files
/etc		Host-specific system-wide configuration files
/home		User home directory
/lib		Shared library modules
/media		Media file such as CD-ROM
/mnt		Temporary mounted filesystems
/opt		Add-on application software packages
/proc		Automatically generated file system
/root		Home directory for root user
/run		Run-time program data
/sbin		System binaries
/srv		Site-specific data served by this system
/sys		Virtual directory providing information about the system
/tmp		Temporary files
/usr		Read-only user files
/var		File that is expected to continuously change

Note:

/home/user/myfile
IS NOT the same as
/home/user/myfile/

If there is a slash at the end, it means
'myfile' is a FOLDER (directory) not a
file. No slash = file

```
[root@desktop /root] # ls -l
```

total 558414									
d	rwxr-xr-x	5	root	root	1024	Dec 23 13:48	GNUstep		
-	rw-r--r--	1	root	root	331	Feb 11 10:19	Xrootenv.0		
-	rw-rw-r--	1	root	root	490	Jan 6 15:07	audio.cddb		
-	rw-r--r--	1	root	root	45254876	Jan 6 15:08	audio.wav		
d	rwxr-xr-x	2	root	root	1024	Feb 20 16:41	axhome		
-	rw-r--r--	1	root	root	900	Jan 18 20:15	conf		
d	rwxr-xr-x	2	root	root	1024	Dec 25 10:03	corel		
-	rw-r--r--	1	root	root	915	Jan 18 20:57	firewall		
d	rwxrwxr-x	2	root	root	1024	Jan 6 15:42	linux		
d	rwx-----	2	root	root	1024	Jan 4 02:19	mail		
d	rwxr-xr-x	3	root	root	1024	Jan 4 01:49	mirror		
-	rwxr--r--	1	root	root	29	Dec 27 15:07	openn		
d	rwxr-xr-x	3	root	root	1024	Dec 26 13:24	scan		
d	rwxrwxr-x	3	root	root	1024	Jan 4 02:34	sniff		
type	access modes	# of links	owner	group	size (bytes)	modification date and time	name		

The .html files for a web server would
be stored in
/var/www/html/