Services

UBNetDef, Spring 2024
Week 7

Lead Presenters:
Ethan Viapiano
Ben Juliano

Learning Goals

- Explore the applications of remote and local services
- Introduction to LAMP stack
- Initially configured a MySQL database
- Initialize MediaWiki setup
- Utilize application layer network protocols
- Learn how to use network reconnaissance tools
- Review log files
- Linux Threat Hunting

Agenda

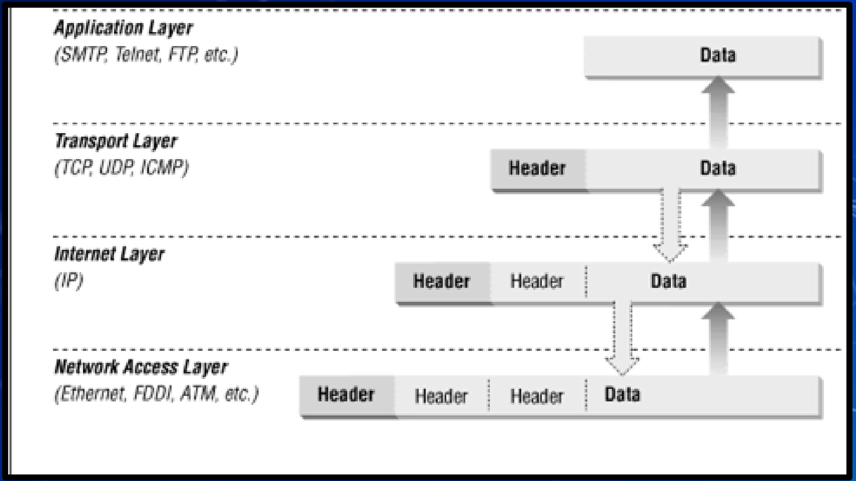
- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Client vs Server

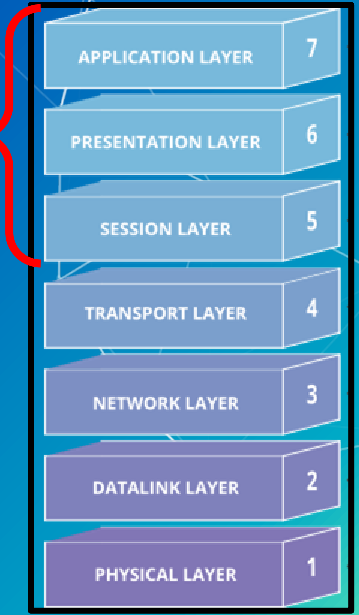
- Client
  - Runs a bunch of services for a limited amount of users
  - Ex: `Win10Client`, `UbuntuClient`
- Server
  - Runs a limited amount of services for a larger number of users
  - Ex: `ServerAD` (Active Directory), `RockyDB` (SQL), `UbuntuWebServer` (Apache)

Application Layer

- Specifies shared protocols for communication between devices



“Application Layer”



Agenda

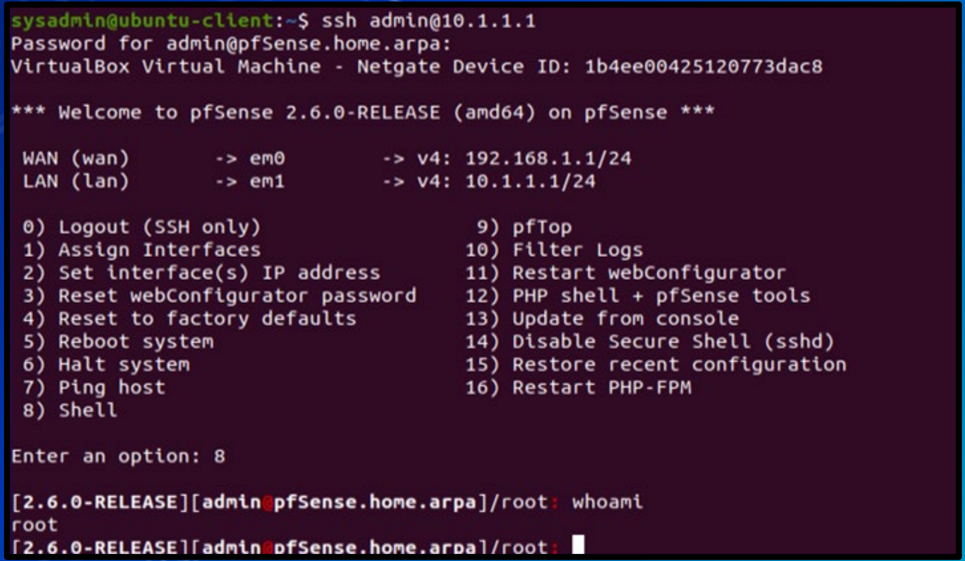
- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Protocols

- Protocol
  - Set of rules or procedures for transmitting data between devices
- Most protocols have “standard” ports
- What are some protocols you have used in this class?

Recall SSH

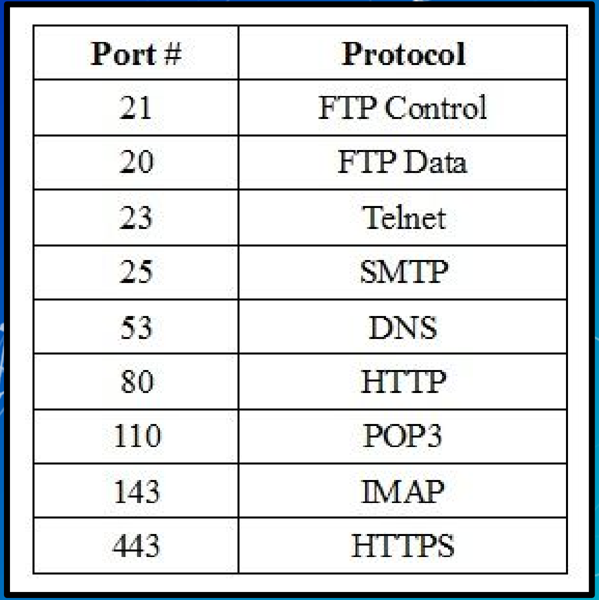
- SSH is a remote access protocol for encrypted client-server connection.
- Access is provided to the shell through a command line interface.
- The common port for SSH is 22.



```
sysadmin@ubuntu-client:~$ ssh admin@10.1.1.1
Password for admin@pfSense.home.arpa:
VirtualBox Virtual Machine - Netgate Device ID: 1b4ee00425120773dac8

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 192.168.1.1/24
 LAN (lan)       -> em1        -> v4: 10.1.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 8

[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: whoami
root
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: 
```

Types of Protocols

- Domain Name System (DNS)
- Email:
  - Simple Mail Transfer Protocol (SMTP)
  - Post Office Protocol (POP3)
- Remote access:
  - Remote Desktop Protocol (RDP)
  - Secure Shell (SSH)
- File Transfer:
  - File Transfer Protocol (FTP)
  - Secure Copy Protocol (SCP)
- Web:
  - Hypertext Transfer Protocol (HTTP)
  - Hypertext Transfer Protocol Secure (HTTPS)



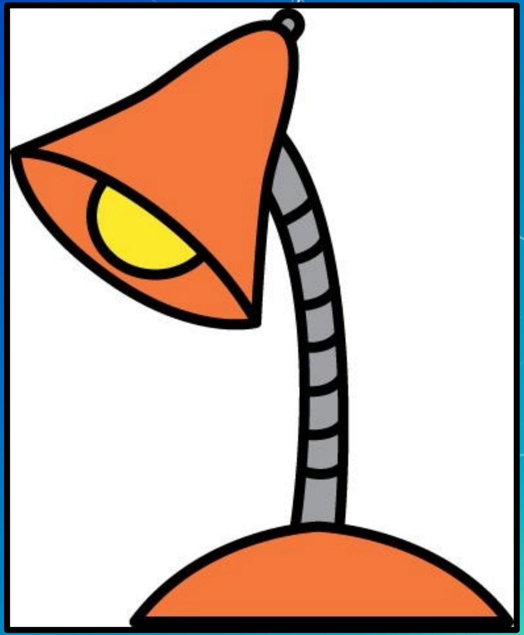
Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

LAMP Stack

- Tech stack of four different software technologies used for:
  - Web applications
  - Web servers
- Key aspects of LAMP stack
- Linux, Apache, MySQL, PHP/python
  - Open source
  - Compatibility/customization
  - Similar (bring in windows)



Agenda

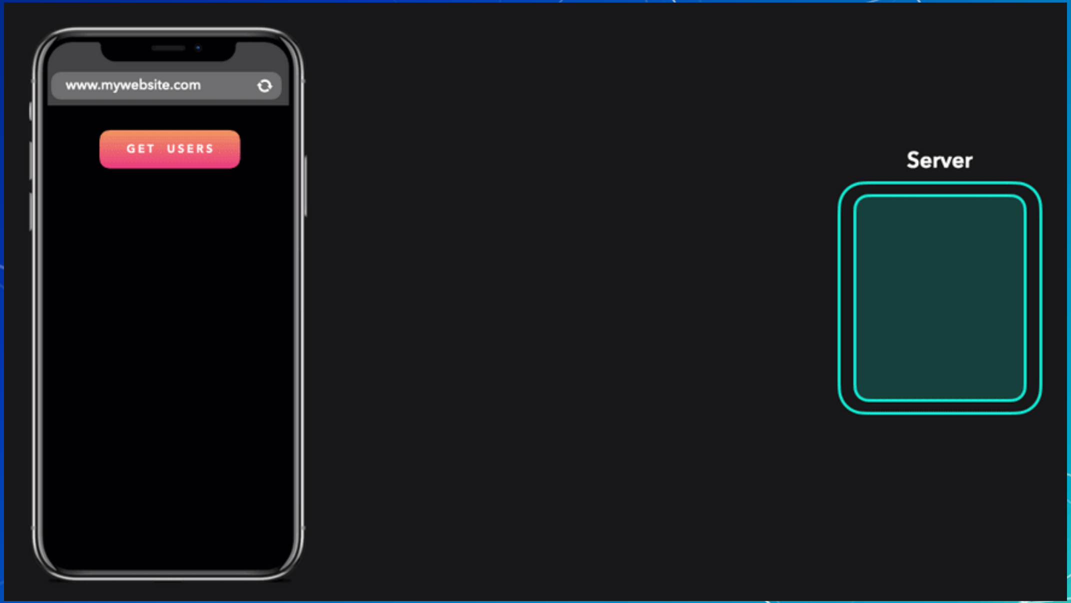
- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Web (Apache)

- Web Servers process incoming requests from clients to web over protocols
  - Web resources are identified by a **U**niform **R**esource **L**ocator (URL)
- Common protocols
  - **H**yper**T**ext **T**ransfer **P**rotocol (HTTP)
    - Unencrypted communication
    - Port 80
  - **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure (HTTPS)
    - Encrypted communication
    - Client is able to authenticate the server
    - Port 443

How we get to our website

- Website: `https://ubnetdef.org/`
- Get an IP address, gateway, etc.
- Resolve "`ubnetdef.org`" to an IP address
- Send an HTTP GET request to `128.205.44.157` asking for host ubnetdef.org and path "`/`"
- Note that the above steps are simplified: a lot more happens

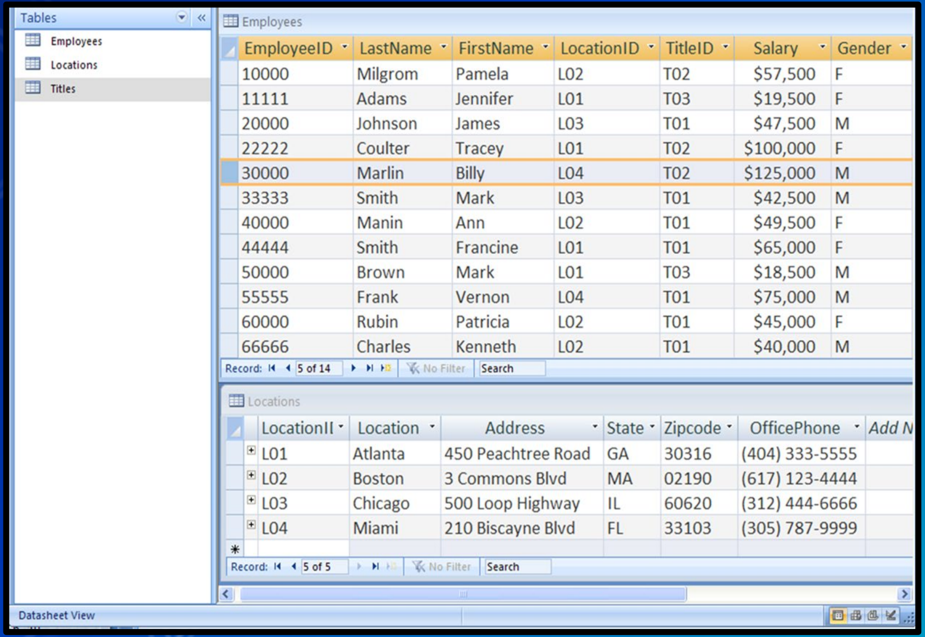


Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Databases (MySQL)

- Collection of data that allows access, retrieval and use of that data
  - Phone book, filing cabinet
  - SQLite, PostgreSQL, Oracle, Microsoft SQL Server, Microsoft Access, MariaDB
- Store structured data in tables made of fields (columns) and records (rows)

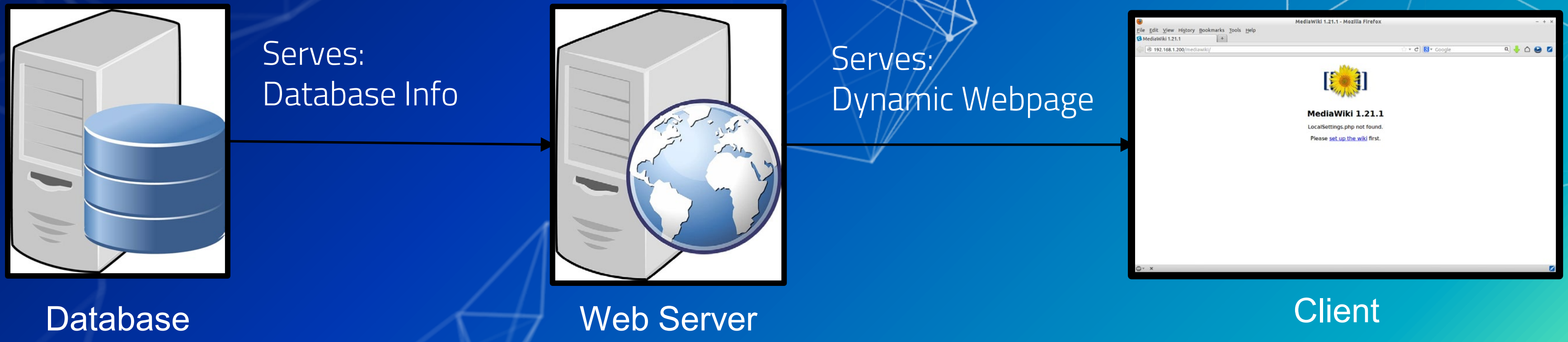


EmployeeID	LastName	FirstName	LocationID	TitleID	Salary	Gender
10000	Milgrom	Pamela	L02	T02	$57,500	F
11111	Adams	Jennifer	L01	T03	$19,500	F
20000	Johnson	James	L03	T01	$47,500	M
22222	Coulter	Tracey	L01	T02	$100,000	F
30000	Marlin	Billy	L04	T02	$125,000	M
33333	Smith	Mark	L03	T01	$42,500	M
40000	Manin	Ann	L02	T01	$49,500	F
44444	Smith	Francine	L01	T01	$65,000	F
50000	Brown	Mark	L01	T03	$18,500	M
55555	Frank	Vernon	L04	T01	$75,000	M
60000	Rubin	Patricia	L02	T01	$45,000	F
66666	Charles	Kenneth	L02	T01	$40,000	M

LocationII	Location	Address	State	Zipcode	OfficePhone	Add N
L01	Atlanta	450 Peachtree Road	GA	30316	(404) 333-5555	
L02	Boston	3 Commons Blvd	MA	02190	(617) 123-4444	
L03	Chicago	500 Loop Highway	IL	60620	(312) 444-6666	
L04	Miami	210 Biscayne Blvd	FL	33103	(305) 787-9999	

What is a Database Driven Website?

- Web resource curated by its own audience using a web browser.
- Service requirements of a wiki
    - Web server
    - Database server



Serves:
Database Info

Serves:
Dynamic Webpage

Database

Web Server

Client

MediaWiki 1.21.1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MediaWiki 1.21.1
192.168.1.200/mediawiki/
Google

MediaWiki 1.21.1

LocalSettings.php not found.

Please set up the wiki first.

MariaDB

- Database client and server software
- Relational database management system (DBMS)
- Option for a backend database for many web applications.
  - MediaWiki
  - WordPress
  - Wiki.js

Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

In Class Demo

Using MariaDB

MariaDB Demo

- Command Line Interface (CLI)
- Logging in
  - `sudo mysql -u root -p`
- List all available databases
  - `SHOW DATABASES;`
- Interact with specific database
  - `USE <DATABASE NAME>;`
- Show all available tables
  - `SHOW TABLES;`
- Show all values in a table
  - `SELECT * FROM <TABLE NAME>;`

QUESTIONS?

In Class Activity

RockyDBServer Setup

RockyDBServer Setup

- Database Setup on RockyDBServer:
  - Use netstat to check if SQL is running, It’s on port 3306

    -
      ```
      ss -tlp
      ```
  - Check the Status of MariaDB

    -
      ```
      sudo systemctl status mariadb
      ```
  - Start the MariaDB Service if necessary

    -
      ```
      sudo systemctl start mariadb
      ```
  - Enable the Service for Automatic Start

    -
      ```
      sudo systemctl enable mariadb
      ```
  - Verify that MariaDB is enabled and running

    -
      ```
      sudo systemctl status mariadb
      ```

RockyDBServer Setup

Database Setup on `RockyDBServer`:

- Improve the security of MariaDB
  - `sudo mysql_secure_installation`
- Verify that MariaDB is listening on the correct port
  - `ss -tlp`
- View current firewalls on your RockyDBServer firewal
  - `sudo firewall-cmd --list-all`
- Verify that the Public Zone is currently active on your RockyDBServer firewall
  - `sudo firewall-cmd --get-active-zones`
- Permanently whitelist the port in the “public” zone in your RockyDBServer Firewall
  - `sudo firewall-cmd --permanent --zone=public --add-port=3306/tcp`
- Reload the firewall
  - `sudo firewall-cmd --reload`

In Class Activity

Web Server Setup

Web Server Setup

Web Server Setup on `UbuntuWebServer`:

- Move to tmp directory
  - `cd /tmp`
- Use `wget` to download MediaWiki
  - `wget https://releases.wikimedia.org/mediawiki/1.41/mediawiki-1.41.0.tar.gz`
- Extract the archive
  - `tar -xvzf /tmp/mediawiki-1.41.0.tar.gz`
- Make a mediawiki directory
  - `sudo mkdir /var/lib/mediawiki`
- Move the contents of the extracted mediawiki to var/lib/mediawiki
  - `sudo mv mediawiki-1.41.0/* /var/lib/mediawiki`
- Create symbolic link from /var/lib/mediawiki to /var/www/html/mediawiki/
  - `sudo ln -s /var/lib/mediawiki /var/www/html/mediawiki`

Symlink

- Create a shortcut to another directory or file inside of a directory or file.
- Similar to the process of making a shortcut in Windows. (Desktop apps don’t live on the Desktop they live in the Program Files folder)

Break

Please return in 10 minutes

Agenda

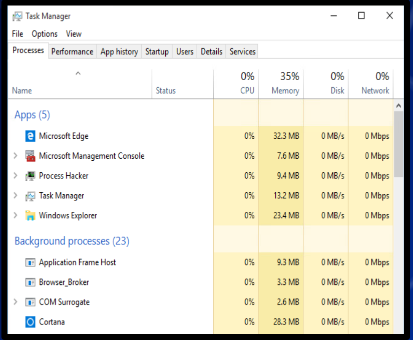
- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Recall Services And Processes

- Services and Processes
  - Common processes are instances of a program
    - Often initiated and terminated by user action
    - notepad.exe, mspaint.exe, Rocket League
  - Active services are persistent processes
    - Often run in the background
    - Xbox Live Game Service, Windows Update manager
  - Services are known to the OS whether they are running or not
- Typically manage things that make the system work

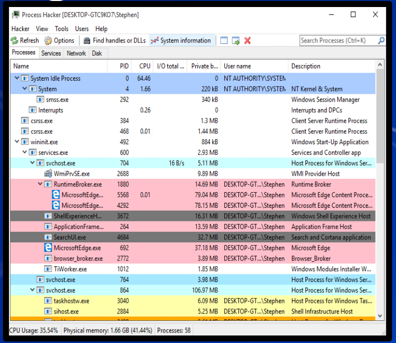
How can I see my machine’s processes?

- Process Managers:


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

		0%	35%	0%	0%
Name	Status	CPU	Memory	Disk	Network
Apps (5)					
Microsoft Edge		0%	32.3 MB	0 MB/s	0 Mbps
Microsoft Management Console		0%	7.6 MB	0 MB/s	0 Mbps
Process Hacker		0%	9.4 MB	0 MB/s	0 Mbps
Task Manager		0%	13.2 MB	0 MB/s	0 Mbps
Windows Explorer		0%	23.4 MB	0 MB/s	0 Mbps
Background processes (23)					
Application Frame Host		0%	9.3 MB	0 MB/s	0 Mbps
Browser_Broker		0%	3.3 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.6 MB	0 MB/s	0 Mbps
Cortana		0%	28.3 MB	0 MB/s	0 Mbps

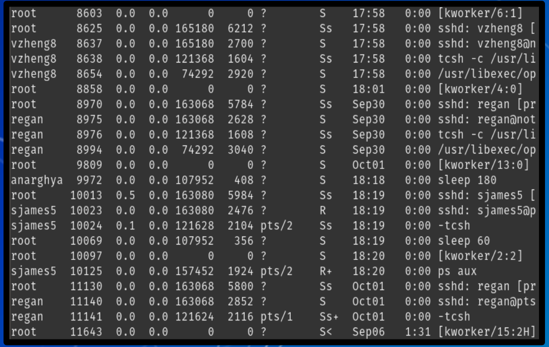
Windows Built-in


Process Hacker [DESKTOP-GTC9KO7\Stephen]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	64.46		0	NT AUTHORITY\SYSTEM	
System	4	1.66		220 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	292			340 kB		Windows Session Manager
Interrupts		0.26		0		Interrupts and DPCs
csrss.exe	384			1.3 MB		Client Server Runtime Process
csrss.exe	468	0.01		1.44 MB		Client Server Runtime Process
wininit.exe	492			884 kB		Windows Start-Up Application
services.exe	600			2.93 MB		Services and Controller app
svchost.exe	704		16 B/s	5.11 MB		Host Process for Windows Ser...
WmiPrvSE.exe	2688			9.89 MB		WMI Provider Host
RuntimeBroker.exe	1880			14.69 MB	DESKTOP-GT...\Stephen	Runtime Broker
MicrosoftEdge...	5568	0.01		79.04 MB	DESKTOP-GT...\Stephen	Microsoft Edge Content Proce...
MicrosoftEdge...	4292			78.15 MB	DESKTOP-GT...\Stephen	Microsoft Edge Content Proce...
ShellExperienceH...	3672			16.31 MB	DESKTOP-GT...\Stephen	Windows Shell Experience Host
ApplicationFrame...	264			13.59 MB	DESKTOP-GT...\Stephen	Application Frame Host
SearchUI.exe	4684			32.7 MB	DESKTOP-GT...\Stephen	Search and Cortana application
MicrosoftEdge.exe	692			37.18 MB	DESKTOP-GT...\Stephen	Microsoft Edge
browser_broker.exe	2772			3.89 MB	DESKTOP-GT...\Stephen	Browser_Broker
TiWorker.exe	1012			1.85 MB		Windows Modules Installer W...
svchost.exe	764			3.98 MB		Host Process for Windows Ser...
svchost.exe	864			106.97 MB		Host Process for Windows Ser...
taskhostw.exe	3040			6.09 MB	DESKTOP-GT...\Stephen	Host Process for Windows Tas...
sihost.exe	2884			5.25 MB	DESKTOP-GT...\Stephen	Shell Infrastructure Host

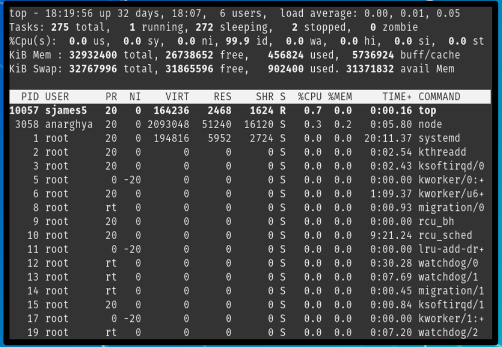
CPU Usage: 35.54% Physical memory: 1.66 GB (41.44%) Processes: 58

Process Hacker



```
root      8603  0.0  0.0      0     0 ?        S    17:58   0:00 [kworker/6:1]
root      8625  0.0  0.0 165180  6212 ?        Ss   17:58   0:00 sshd: vzheng8 [
vzheng8   8637  0.0  0.0 165180  2700 ?        S    17:58   0:00 sshd: vzheng8@n
vzheng8   8638  0.0  0.0 121368  1604 ?        Ss   17:58   0:00 tcsh -c /usr/li
vzheng8   8654  0.0  0.0  74292  2920 ?        S    17:58   0:00 /usr/libexec/op
root      8858  0.0  0.0      0     0 ?        S    18:01   0:00 [kworker/4:0]
root      8970  0.0  0.0 163068  5784 ?        Ss   Sep30   0:00 sshd: regan [pr
regan     8975  0.0  0.0 163068  2628 ?        S    Sep30   0:00 sshd: regan@not
regan     8976  0.0  0.0 121368  1608 ?        Ss   Sep30   0:00 tcsh -c /usr/li
regan     8994  0.0  0.0  74292  3040 ?        S    Sep30   0:00 /usr/libexec/op
root      9809  0.0  0.0      0     0 ?        S    Oct01   0:00 [kworker/13:0]
anarghya  9972  0.0  0.0 107952   408 ?        S    18:18   0:00 sleep 180
root     10013  0.5  0.0 163080  5984 ?        Ss   18:19   0:00 sshd: sjames5 [
sjames5  10023  0.0  0.0 163080  2476 ?        R    18:19   0:00 sshd: sjames5@p
sjames5  10024  0.1  0.0 121628  2104 pts/2    Ss   18:19   0:00 -tcsh
root     10069  0.0  0.0 107952   356 ?        S    18:19   0:00 sleep 60
root     10097  0.0  0.0      0     0 ?        S    18:20   0:00 [kworker/2:2]
sjames5  10125  0.0  0.0 157452  1924 pts/2    R+   18:20   0:00 ps aux
root     11130  0.0  0.0 163068  5800 ?        Ss   Oct01   0:00 sshd: regan [pr
regan    11140  0.0  0.0 163068  2852 ?        S    Oct01   0:00 sshd: regan@pts
regan    11141  0.0  0.0 121624  2116 pts/1    Ss+  Oct01   0:00 -tcsh
root     11643  0.0  0.0      0     0 ?        S<   Sep06   1:31 [kworker/15:2H]
```

$ps -aux

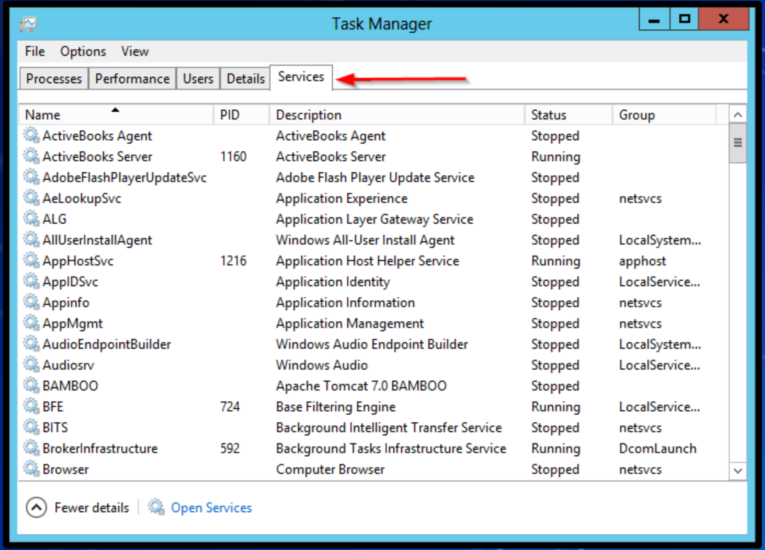


```
top - 18:19:56 up 32 days, 18:07,  6 users,  load average: 0.00, 0.01, 0.05
Tasks: 275 total,   1 running, 272 sleeping,   2 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni, 99.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 32932400 total, 26738652 free,   456824 used,  5736924 buff/cache
KiB Swap: 32767996 total, 31865596 free,   902400 used. 31371832 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
10057 sjames5   20   0  164236   2468   1624 R   0.7  0.0   0:00.16 top
 3058 anarghya  20   0 2093048  51240  16120 S   0.3  0.2   0:05.80 node
    1 root      20   0  194816   5952   2724 S   0.0  0.0  20:11.37 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:02.54 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:02.43 ksoftirqd/0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:+
    6 root      20   0       0      0      0 S   0.0  0.0   1:09.37 kworker/u6+
    8 root      rt   0       0      0      0 S   0.0  0.0   0:00.93 migration/0
    9 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
   10 root      20   0       0      0      0 S   0.0  0.0   9:21.24 rcu_sched
   11 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 lru-add-dr+
   12 root      rt   0       0      0      0 S   0.0  0.0   0:30.28 watchdog/0
   13 root      rt   0       0      0      0 S   0.0  0.0   0:07.69 watchdog/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.45 migration/1
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.84 ksoftirqd/1
   17 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/1:+
   19 root      rt   0       0      0      0 S   0.0  0.0   0:07.20 watchdog/2
```

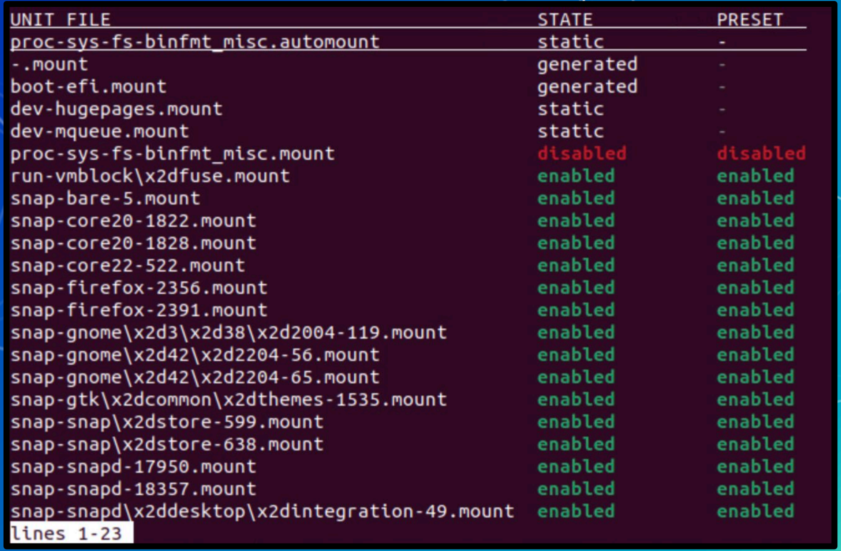
$top

How do we see our machine’s services?

- Service managers
- How else can we find services?



Name	PID	Description	Status	Group
ActiveBooks Agent		ActiveBooks Agent	Stopped	
ActiveBooks Server	1160	ActiveBooks Server	Running	
AdobeFlashPlayerUpdateSvc		Adobe Flash Player Update Service	Stopped	
AeLookupSvc		Application Experience	Stopped	netsvcs
ALG		Application Layer Gateway Service	Stopped	
AllUserInstallAgent		Windows All-User Install Agent	Stopped	LocalSystem...
AppHostSvc	1216	Application Host Helper Service	Running	apphost
AppIDSvc		Application Identity	Stopped	LocalService...
Appinfo		Application Information	Stopped	netsvcs
AppMgmt		Application Management	Stopped	netsvcs
AudioEndpointBuilder		Windows Audio Endpoint Builder	Stopped	LocalSystem...
Audiosrv		Windows Audio	Stopped	LocalService...
BAMBOO		Apache Tomcat 7.0 BAMBOO	Stopped	
BFE	724	Base Filtering Engine	Running	LocalService...
BITS		Background Intelligent Transfer Service	Stopped	netsvcs
BrokerInfrastructure	592	Background Tasks Infrastructure Service	Running	DcomLaunch
Browser		Computer Browser	Stopped	netsvcs



```
UNIT FILE                                   STATE          PRESET
proc-sys-fs-binfmt_misc.automount           static         -
-.mount                                     generated      -
boot-efi.mount                              generated      -
dev-hugepages.mount                         static         -
dev-mqueue.mount                            static         -
proc-sys-fs-binfmt_misc.mount               disabled       disabled
run-vmblock\x2dfuse.mount                   enabled        enabled
snap-bare-5.mount                           enabled        enabled
snap-core20-1822.mount                      enabled        enabled
snap-core20-1828.mount                      enabled        enabled
snap-core22-522.mount                       enabled        enabled
snap-firefox-2356.mount                     enabled        enabled
snap-firefox-2391.mount                     enabled        enabled
snap-gnome\x2d3\x2d38\x2d2004-119.mount     enabled        enabled
snap-gnome\x2d42\x2d2204-56.mount           enabled        enabled
snap-gnome\x2d42\x2d2204-65.mount           enabled        enabled
snap-gtk\x2dcommon\x2dthemes-1535.mount     enabled        enabled
snap-snap\x2dstore-599.mount                enabled        enabled
snap-snap\x2dstore-638.mount                enabled        enabled
snap-snapd-17950.mount                      enabled        enabled
snap-snapd-18357.mount                      enabled        enabled
snap-snapd\x2ddesktop\x2dintegration-49.mount enabled        enabled
lines 1-23
```

Sneaky Services

- Open ports may indicate which services are running (listening)
  - ss
  - Get-NetTCPConnection (Windows)
  - Netstat (Windows)
- Network scans can reveal ports that are open and closed.
- Tools for network reconnaissance (Cyber Kill Chain)
  - nmap/zenmap
  - OpenVAS
  - Nikto

Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

In Class Activity

NMAP Activity

NMAP Activity

- Use `UbuntuClient` to scan AdminNet
  - Install nmap
    - `sudo apt install nmap`
  - Read the man pages for nmap
    - `man nmap`
  - Use nmap to scan an entire subnet
    - `nmap 10.42.<X>.0/24`
  - What did you notice about the results?

NMAP Activity

- Use `OutsideDevice` to scan ServerNet
  - `nmap 10.43.<X>.0/24`
  - What did you notice about the results?

NMAP Activity

- Use `pfctl -d` to disable the firewall
- Use `OutsideDevice` to scan ServerNet
  - `nmap 10.43.<X>.0/24`
  - What did you notice about the results?

Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Logs

- Examples of some logs are:
  - File system journals
  - Security logs
  - System logs
  - Application logs
    - e.g., `tail -f /var/log/apache2/access.log`
- Why are logs important?

In Class Activity

Log files

Log file activity

- Use a web browser on any VM to go to the following IP address
  `192.168.13.87`

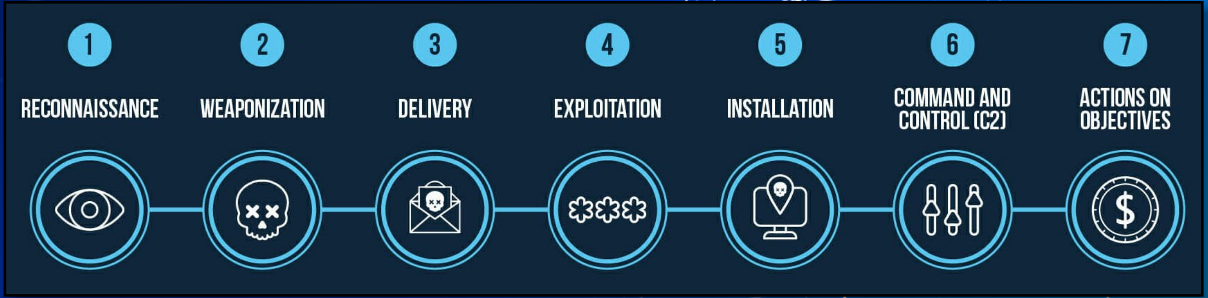
Agenda

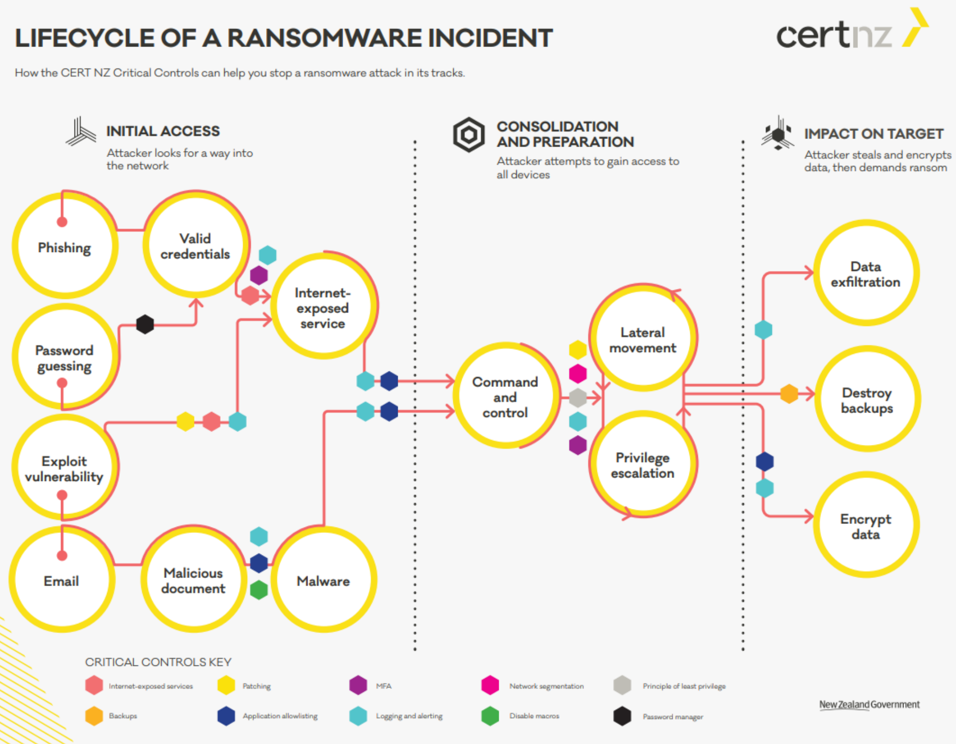
- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Threat Hunting: You Are Here

Kill Chains

- Cyber Kill Chain
  - Developed by Lockheed Martin
- Lifecycle of a Ransomware Incident Model
  - Developed by New Zealand Government





LIFECYCLE OF A RANSOMWARE INCIDENT

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

INITIAL ACCESS

Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

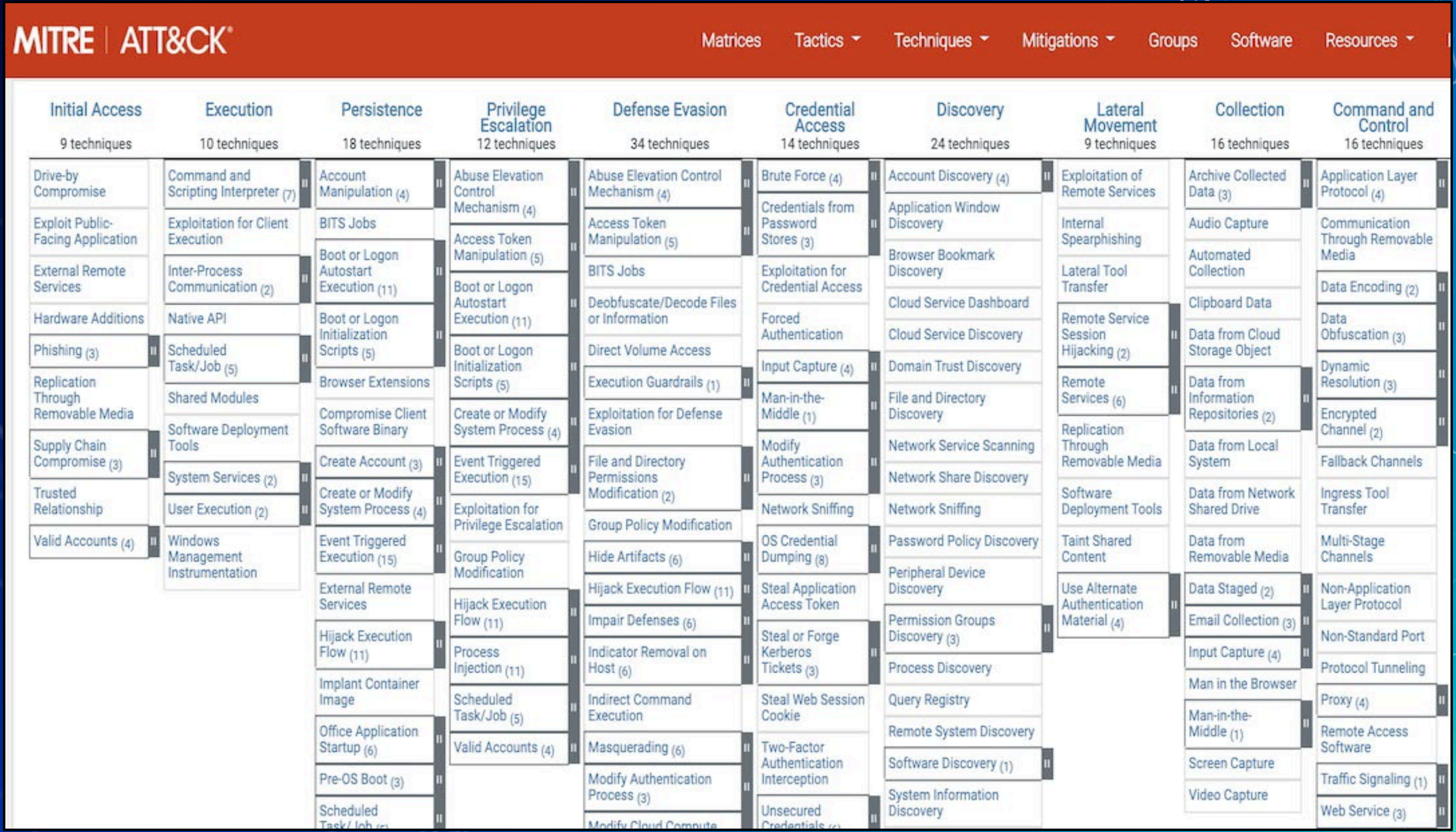
Attacker steals and encrypts data, then demands ransom

CRITICAL CONTROLS KEY

Internet-exposed services	Patching	MFA	Network segmentation	Principle of least privilege
Backups	Application allowlisting	Logging and alerting	Disable macros	Password manager

New Zealand Government

MITRE ATT&CK Framework



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
10 techniques

- Command and Scripting Interpreter (7)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (11)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Container Image
- Office Application Startup (6)
- Pre-OS Boot (3)
- Scheduled Task/Job (5)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (11)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
34 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Group Policy Modification
- Hide Artifacts (6)
- Hijack Execution Flow (11)
- Impair Defenses (6)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (3)
- Modify Cloud Compute

Credential Access
14 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (4)
- Man-in-the-Middle (1)
- Modify Authentication Process (3)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (3)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials

Discovery
24 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
16 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (1)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Linux Threat Hunting

- Find unwanted network connections.
- Discover rogue processes.
- Disable/stop rogue services.

In Class Activity

Linux Threat Hunting

Threat Hunting Activity

- Log into `InfectedLinux`
  - Username: `sysadmin`
  - Password: `Change.me!`
- Try using the following commands to check services, network connections and processes.
  - `ps -aux`
  - `systemctl list-units -all`
  - `ss -tlp`

Hardening a DB

- Database security topics
  - Why is DB security important?
  - User access control to databases
  - DB encryption
    - How useful is encrypting data-at-rest
    - Encrypt whole storage device?
    - Encrypt logical segment of storage device?
    - Encrypt data inside DBs?
  - Shared vs dedicated DBs
  - DB logging and monitoring
  - Network Segmentation

Agenda

- Client vs. Server
- Protocols Review
- LAMP Stack
- Websites & Webservers
- Databases
- Setup
- Processes & Services
- Nmap Activity
- Logs Review
- Linux Threat Hunting Overview & Activity
- HW & Information Report Overview

Homework

- Two PDF’s submitted separately.
  - An instructional report
  - An informational report
- Configuring MediaWiki and MariaDB on UbuntuWeb and RockyDB.

Informational Reports

- What is an informational report?
- How are they different from instructional?
- Is there a style guide?

QUESTIONS?

Summary and Wrap-up

Today’s achievements:

- Explored the applications of remote and local services
- Initially configured a MySQL database
- Initialized MediaWiki setup
- Utilized application layer network protocols
- Learned how to use network reconnaissance tools