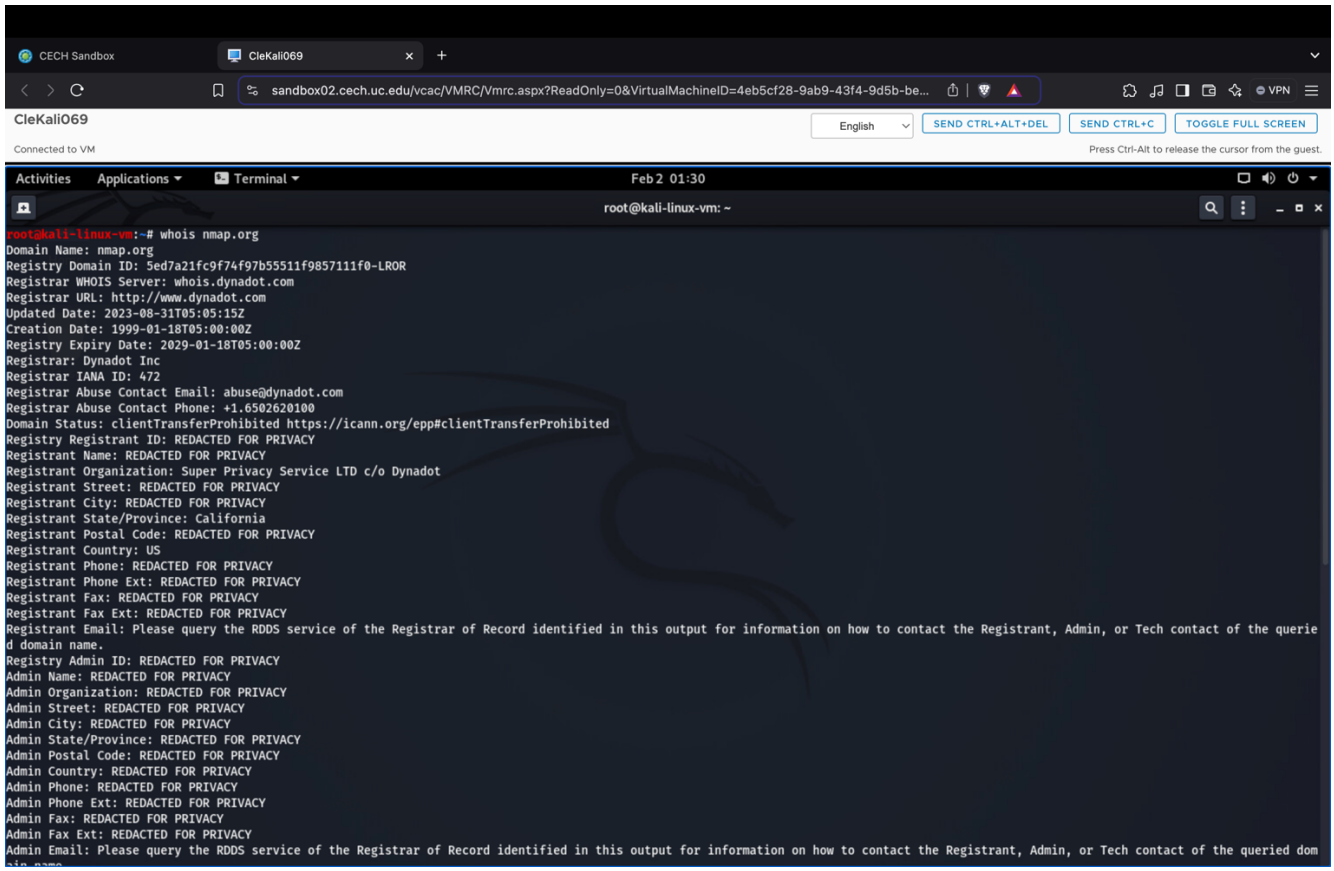
Name: Amit S Terdal
CSU ID: 2887869

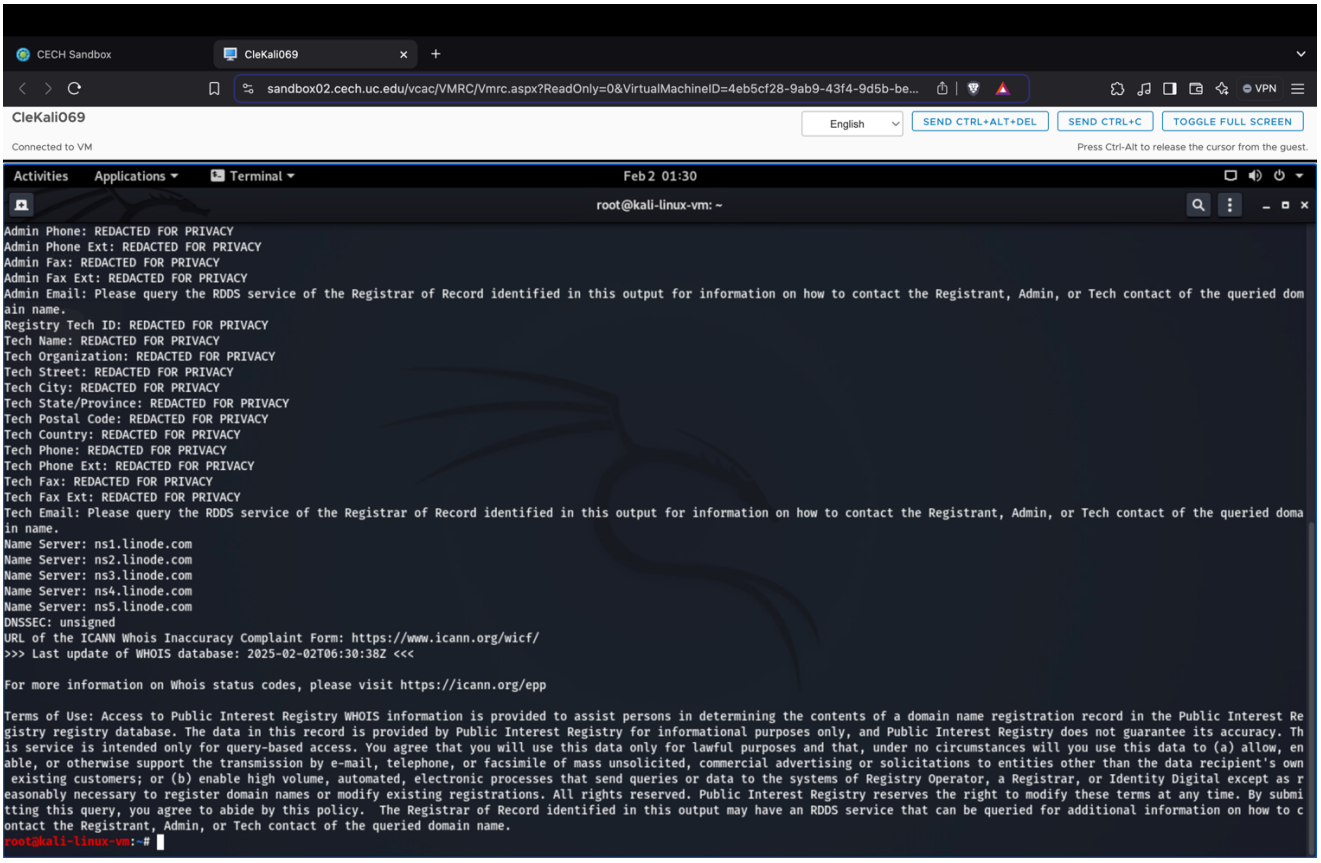
Module Activity Description:

Part One: **Passive Recon**

1. *Run a whois command on nmap.org.*

- **1. Paste a screen shot of all the information that you received.**





- **2. What specific information from this command could be useful to a penetration tester and should be documented?**

  Useful Information:
  - Registrar Details: Dynaddr Inc. (This could be useful for social engineering or identifying potential vulnerabilities in the registrar's systems.)
  - Domain Status: clientTransferProhibited (Indicates the domain cannot be transferred, which might affect certain attack vectors.)
  - Name Server: ns1.linode.com (This reveals the hosting provider, which could be targeted for further reconnaissance.)
  - Registration and Expiration Dates: These dates can help determine the domain's lifecycle, which might be useful for timing attacks or identifying abandoned domains.
  - Registrant Organization: Super Privacy Service LTD c/o Dynaddr (This suggests the use of a privacy service, which might make direct contact with the owner difficult but could still be useful for further investigation.)

- **3. What other tools/services could you use to find similar information?**

  - dig: (dig nmap.org) Query DNS records for IPs, name servers, and mail servers.
  - nslookup: (nslookup nmap.org) Look up DNS information for a domain.
  - host: (host nmap.org) Perform DNS lookups for IPs and name servers.
  - dnsenum: (dnsenum nmap.org) Enumerate DNS information, including subdomains and IP ranges.
  - Sublist3r: (sublist3r -d nmap.org) Enumerate subdomains using search engines and DNS queries.

- theHarvester: (theHarvester -d nmap.org -b all) Gather emails, subdomains, and IPs from public sources.
- Shodan: (shodan host nmap.org) Search for server information, open ports, and services.
- Metagoofil: (metagoofil -d nmap.org -t pdf,docx -l 10 -n 5 -o ~/output) Extract metadata from public documents.
- Amass: (amass enum -d nmap.org) Perform in-depth DNS enumeration and mapping.
- Maltego: (whois -h whois.dynadot.com nmap.org) Visualize and analyze domain relationships and entities.
- Recon-ng: (recon-ng
  marketplace install all
  modules load recon/domains-hosts/brute_hosts
  options set SOURCE nmap.org
  run) A reconnaissance framework for gathering domain information.

- **4. Linux Review Question: How can you find out more information about a command line tool, such as options, syntax, and examples?**

  - whois -help (options, syntax for kali linux as per the video walkthrough)
  - man: Full documentation and examples.
  - --help: Quick reference for options.
  - Info: Detailed GNU tool docs.
  - apropos: Discover tools related to a task.

- **5. List 3 additional ways, which penetration test can enumerate and find additional IP/network space given a single domain?**

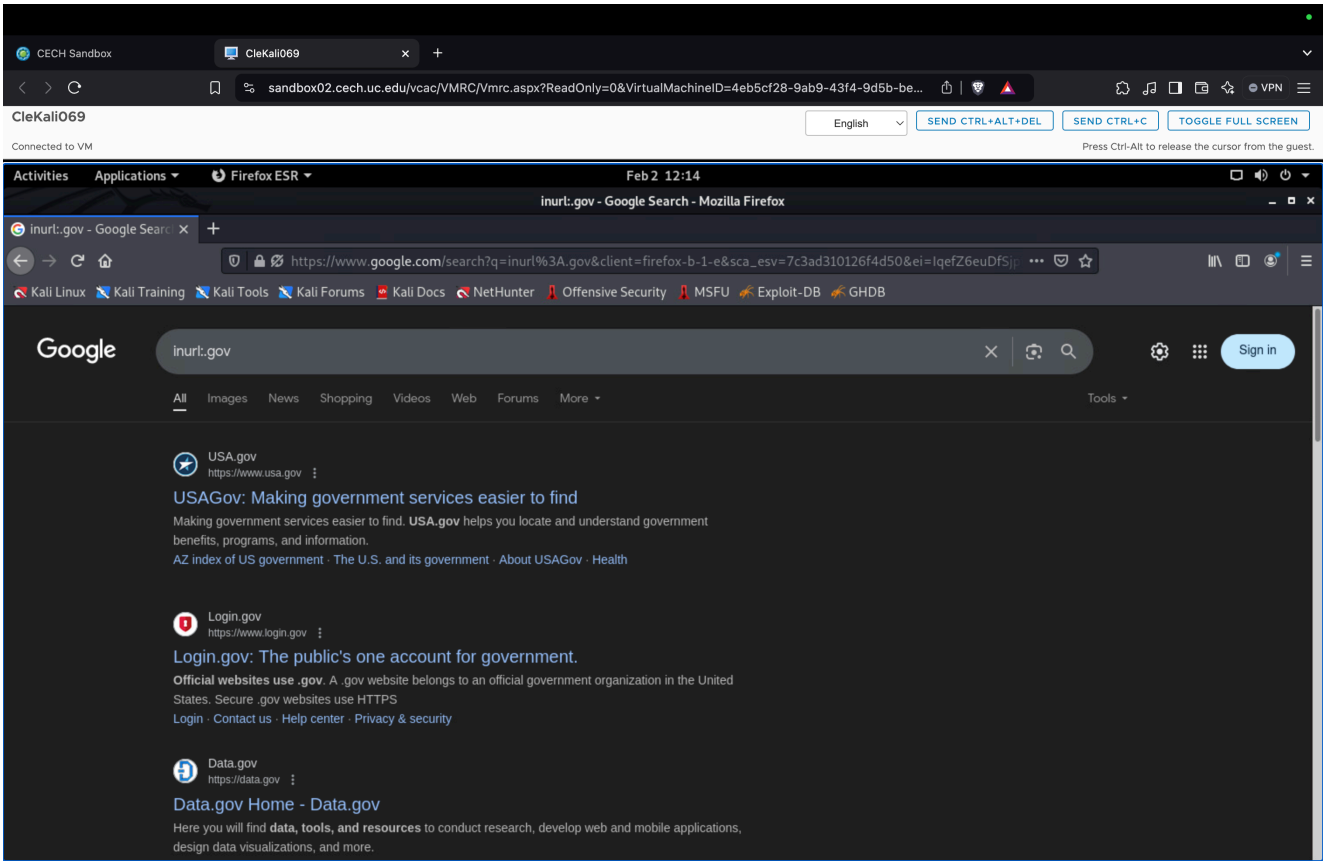
  - DNS Enumeration: Use tools like dnsenum or dnsrecon to find subdomains and associated IP addresses.
  - **Reverse DNS Lookup: Perform a reverse DNS lookup on the IP address associated with the domain to find other domains hosted on the same server.**
  - **ASN Lookup: Identify the Autonomous System Number (ASN) associated with the domain and use it to find other IP ranges owned by the same organization.**

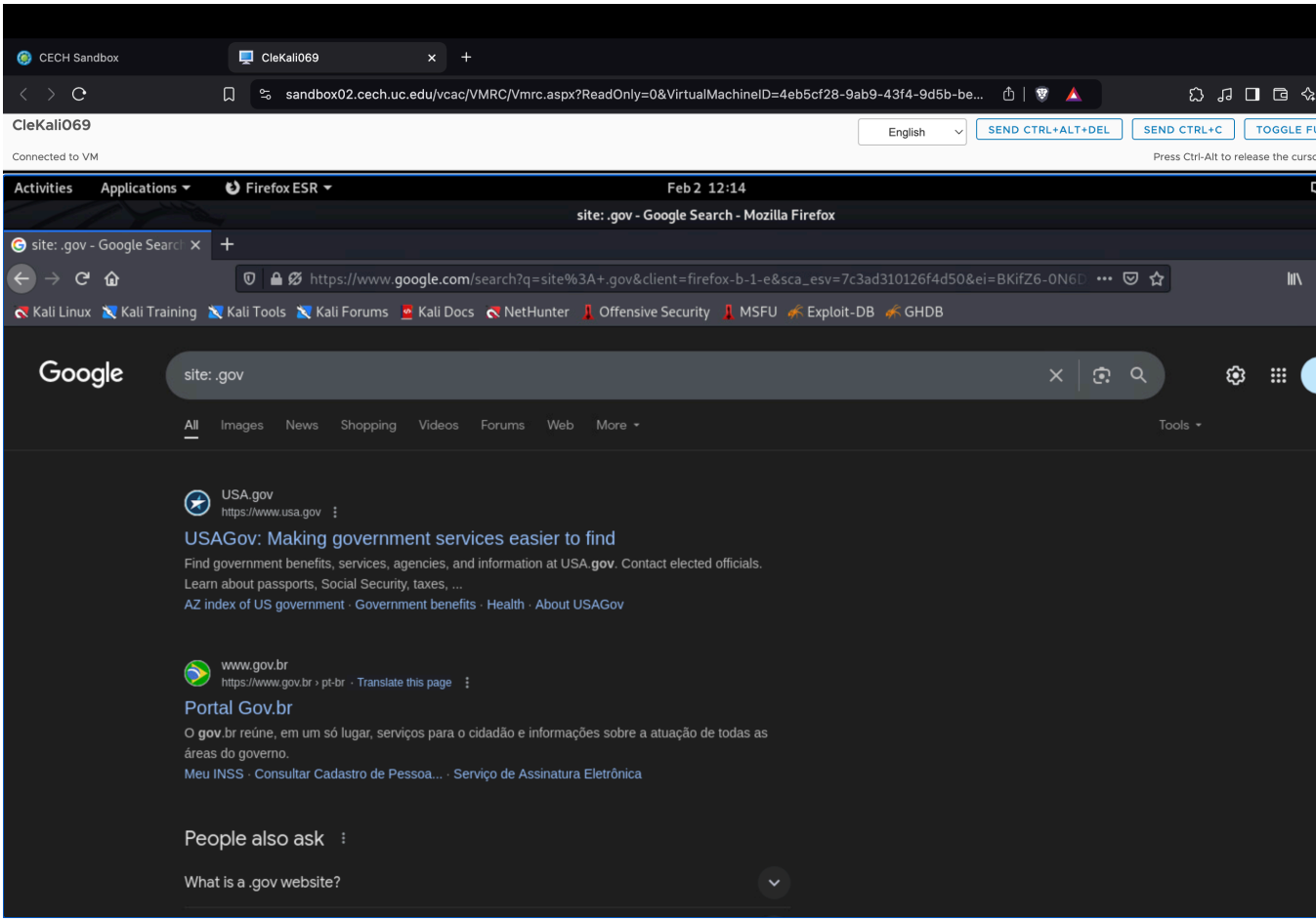
2. *Using Google Dorks, run a search and narrow the results to only include: all .gov TLDs, the term "password" inside the body of the page, the term "reset" in the URL, and only return .docx files.*

   - **6. What was the search query that you used?**

     - I used every search query that was shown in the video walkthrough such as: inurl:.gov, inbody: passwords, ext: pdf
     - I explored other similar search query on the google dorks
       site:.gov → Restrict results to .gov domains.
       intext:"password" → Search for pages containing "password" in the body.
       inurl:"reset" → Filter URLs containing the term "reset".
       filetype:docx → Only return .docx files.

   - **7. Paste a screen shot of the results of the Google Dorks search results.**


CECH Sandbox
CleKali069
sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5b-be...
CleKali069
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Connected to VM
Press Ctrl-Alt to release the cursor from the guest.
Activities
Applications
Firefox ESR
Feb 2 12:14
inurl:.gov - Google Search - Mozilla Firefox
https://www.google.com/search?q=inurl%3A.gov&client=firefox-b-1-e&sca_esv=7c3ad310126f4d50&ei=IqefZ6euDfSj
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Google
inurl:.gov
Sign in
All
Images
News
Shopping
Videos
Web
Forums
More
Tools
USA.gov
https://www.usa.gov
USAGov: Making government services easier to find
Making government services easier to find. USA.gov helps you locate and understand government benefits, programs, and information.
AZ index of US government · The U.S. and its government · About USAGov · Health
Login.gov
https://www.login.gov
Login.gov: The public's one account for government.
Official websites use .gov. A .gov website belongs to an official government organization in the United States. Secure .gov websites use HTTPS
Login · Contact us · Help center · Privacy & security
Data.gov
https://data.gov
Data.gov Home - Data.gov
Here you will find data, tools, and resources to conduct research, develop web and mobile applications, design data visualizations, and more.


CECH Sandbox
CleKali069
sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5b-be...
CleKali069
English
SEND CTRL+ALT+DEL
SEND CTRL+C
Connected to VM
Activities
Applications
Firefox ESR
Feb 2 12:14
site: .gov - Google Search - Mozilla Firefox
https://www.google.com/search?q=site%3A+.gov&client=firefox-b-1-e&sca_esv=7c3ad310126f4d50&ei=BKifZ6-0N6D
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Google
site: .gov
All
Images
News
Shopping
Videos
Forums
Web
More
Tools
USA.gov
https://www.usa.gov
USAGov: Making government services easier to find
Find government benefits, services, agencies, and information at USA.gov. Contact elected officials. Learn about passports, Social Security, taxes, ...
AZ index of US government · Government benefits · Health · About USAGov
www.gov.br
https://www.gov.br › pt-br · Translate this page
Portal Gov.br
O gov.br reúne, em um só lugar, serviços para o cidadão e informações sobre a atuação de todas as áreas do governo.
Meu INSS · Consultar Cadastro de Pessoa... · Serviço de Assinatura Eletrônica
People also ask
What is a .gov website?

- **8. Explain two ways a penetration testing could gather e-mail addresses of key employees**

  OSINT Tools (e.g., theHarvester):
  Use tools like theHarvester to scrape emails from:
  Search engines (Google, Bing).
  Social media (LinkedIn, Twitter).
  Public databases (PGP key servers, company websites).
  Command:
  theHarvester -d example.com -b google,linkedin

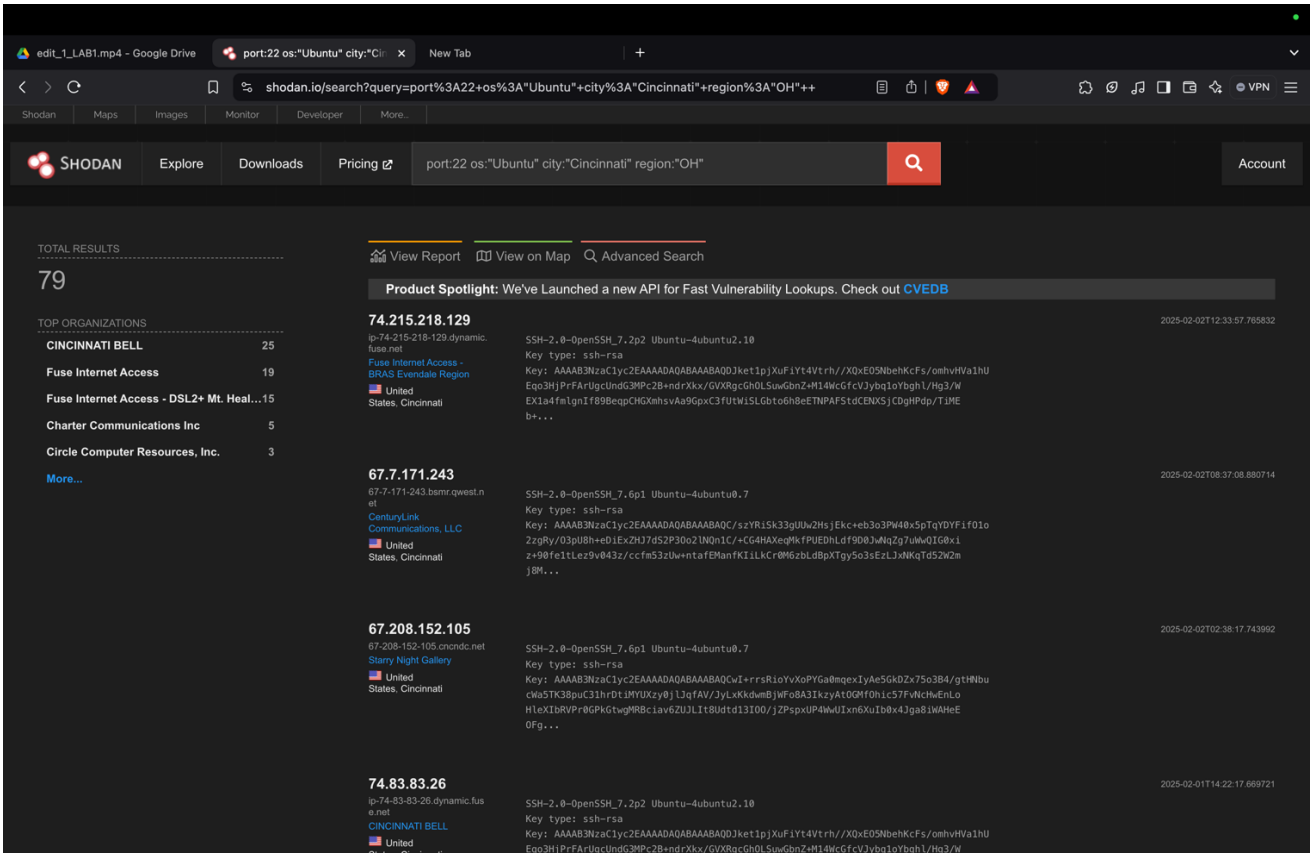
  Email Format Guessing + Verification:
  Guess email formats using common patterns (e.g., j.smith@example.com, john@example.com).
  Verify validity with tools like:
  Hunter.io (for domain email pattern detection).
  Email Hippo (email verification API).

- **9. Why would a list of e-mail addresses be useful to a penetration tester?**

  - Phishing Campaigns: Craft targeted attacks (e.g., fake login pages, malicious attachments).
  - Credential Stuffing: Test leaked passwords against corporate accounts.
  - Social Engineering: Impersonate employees to gain trust or sensitive information.
  - Password Reset Exploits: Abuse "forgot password" workflows using known emails.

3. *Run a search on Shodan to return results that have an Ubuntu server running with port 22 open and based in Cincinnati, OH.*

- **10. Paste a screen shot of your results.**



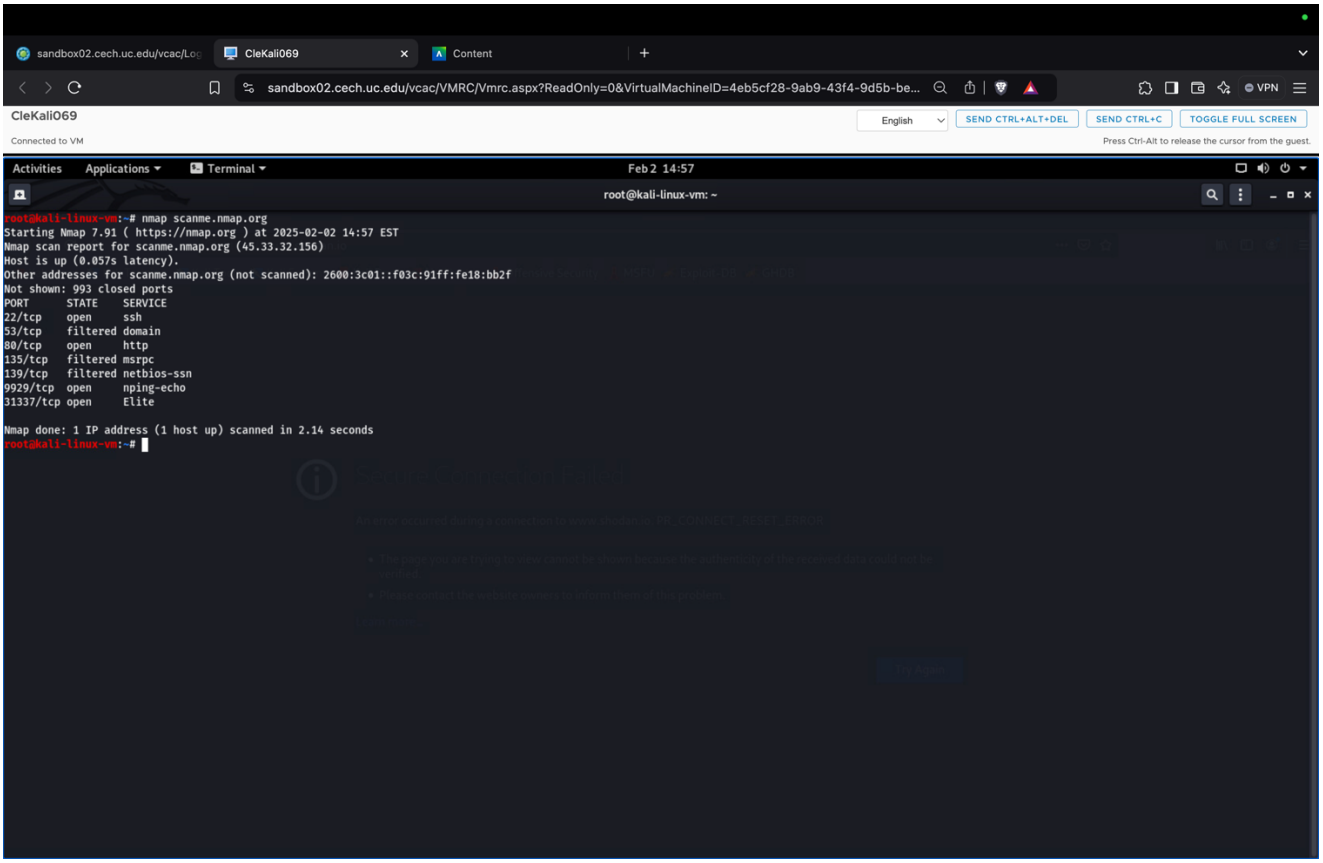
- **11. What version of SSH is running on the first returned result? Module Activity Description:**

- The SSH version running on the first returned result is OpenSSH 7.2p2.
Service: OpenSSH 7.2p2 Ubuntu 4ubuntu2.10
Banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
The 7.2p2 indicates the OpenSSH version, while Ubuntu 4ubuntu2.10 refers to the Ubuntu-specific package build.

Part Two: Active Recon

1. *Run an nmap scan against scanme.nmap.org*

- **1. Paste a screen shot of the results.**



2. Explain what information from this scan may be useful to a penetration tester.

- The Nmap scan of scanme.nmap.org reveals several pieces of information critical to a penetration tester. Here's a breakdown of the useful details and their implications:

Port	**Service**	**Usefulness to a Penetration Tester**
22/tcp	SSH	- Target for brute-force attacks (e.g., weak credentials). - Check for outdated SSH versions (e.g., CVE-2023-38408).
53/tcp	DNS	- Enumerate DNS records (e.g., dig, nslookup). - Attempt zone transfers or DNS cache poisoning.
80/tcp	HTTP	- Inspect the web server for vulnerabilities (e.g., outdated Apache, misconfigurations). - Crawl for sensitive files (e.g., robots.txt, login pages).
135/tcp	MSRPC (Windows)	- Unusual on a Linux server; possible misconfiguration or mixed environment. - Probe for Windows-specific vulnerabilities (e.g., EternalBlue).

139/tcp	NetBIOS (Windows)	- Enumerate SMB shares (e.g., smbclient). - Check for SMB vulnerabilities (e.g., CVE-2017-0144).
9929/tcp	Unknown Service	- Investigate further with nmap -sV to identify the service. - Check for custom/backdoor services.
31337/tcp	Elite (Backdoor)	- Commonly used for backdoors (e.g., Metasploit, custom malware). - Test for unauthorized access or exploits.

<u>Additional Useful Information</u>

Host Status:

- Host is up (0.057s latency) → Confirms the target is reachable and responsive.

Closed Ports (993):

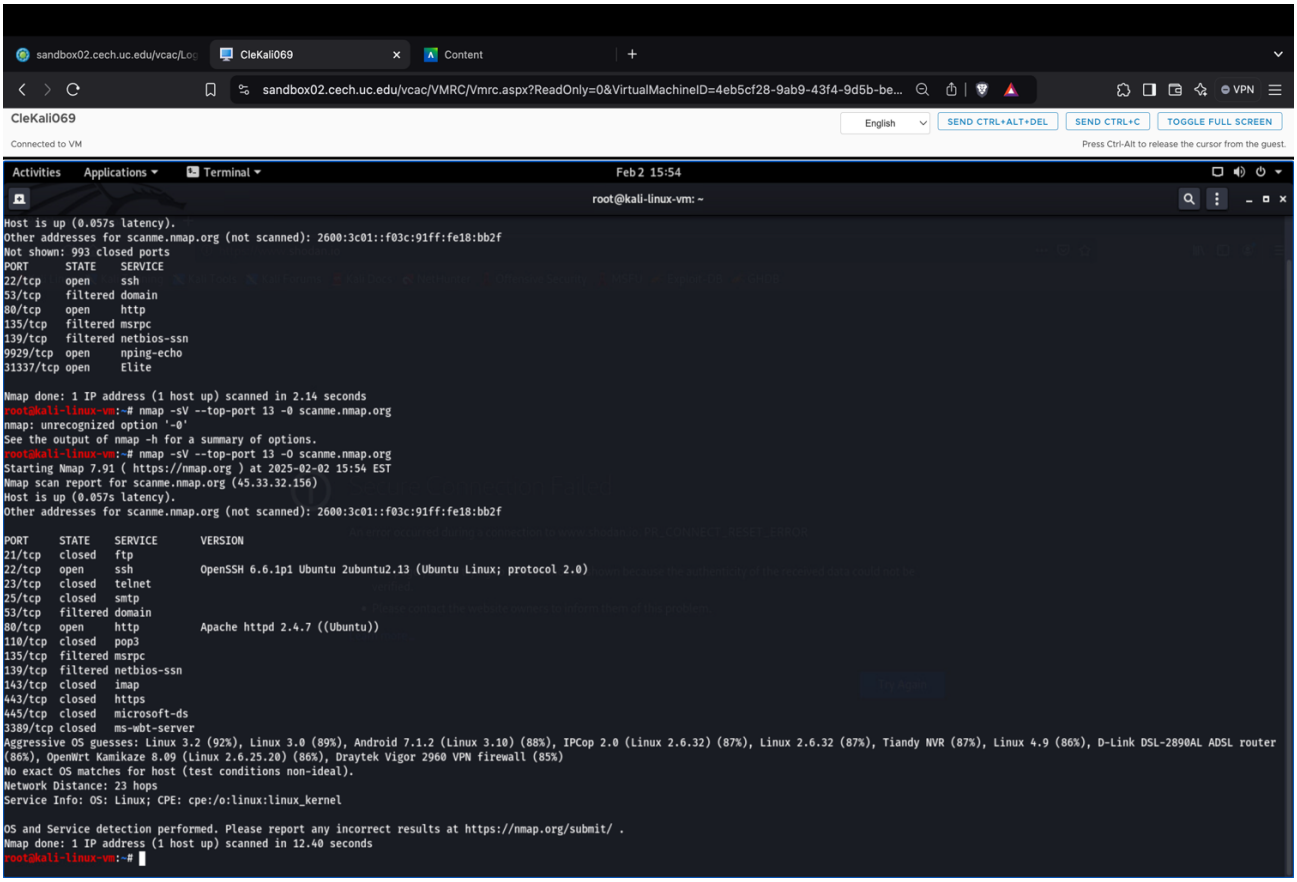
- Indicates a reduced attack surface; focus efforts on open ports.

IPv6 Address:

- 2600:3c01::f03c:91ff:fe18:bb2f → Test for IPv6-specific vulnerabilities or misconfigurations.

2. *Run another nmap scan against scanme.nmap.org. This time include the options to include version detection, the top 13 ports, and operating system detection*

- **3. Paste a screen shot of the results.**



- **4. What OS is this system running (Best guess)?**
  - The best guess is **Linux (Ubuntu)**, based on:
  - The SSH service banner: OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13.
  - The Apache version: Apache httpd 2.4.7 ((Ubuntu)).
  - Aggressive OS guesses include Linux 3.2 (92% confidence).

- **5. What version of Apache is this system running?**
  - **Apache 2.4.7** (As it is stated in the scan results under port 80/tcp).

- **6. What happens if nmap itself cannot determine if a host is alive or not?**
  - If Nmap cannot confirm a host is alive during its discovery phase (e.g., no response to ICMP/TCP probes), it will:
    Mark the host as **"down"**.
    Skip scanning its ports unless forced with the -Pn flag.

- **7. How could you bypass the above behavior?**
  - Use the **-Pn** flag to **skip host discovery** and scan all specified ports regardless of the host's status:
    "nmap -Pn scanme.nmap.org"

- **8. Explain the difference between a –sS and –sT scan? Which is faster and why?**

  - -sS (SYN Scan):
    - Mechanism: Sends a SYN packet and analyzes the response (SYN-ACK = open, RST = closed).
    - Speed: Faster because it does not complete the TCP handshake.
    - Stealth: Stealthier (avoids logging full connections).
  - -sT (TCP Connect Scan):
    - Mechanism: Completes the full TCP handshake (SYN → SYN-ACK → ACK).
    - Speed: Slower due to the full handshake process.
    - Use Case: Fallback when SYN scans are blocked (e.g., by firewalls).

  Faster Option: -sS (SYN Scan) is faster because it avoids establishing full TCP connections.