Using the online port scanner https://hackertarget.com/nmap-online-port-scanner// (Links to an external site.)

Scan the following hostname or IP:

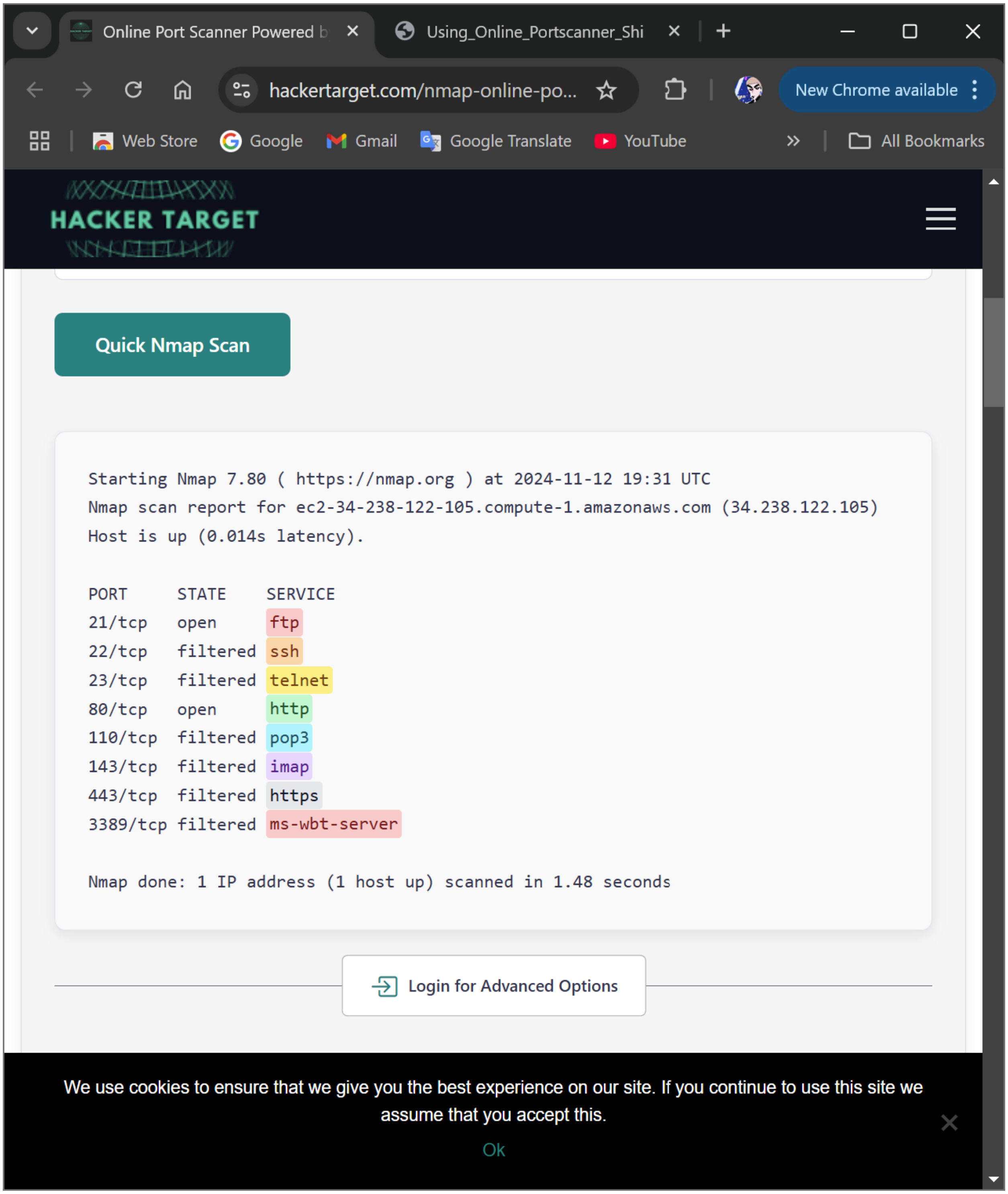
Hostname: ec2-34-238-122-105.compute-1.amazonaws.com

IP: 34.238.122.105

Note: if you get no results from hostname then try IP address.

Answer the following questions and provide screenshots showing the results of the scans.

1. **Which network services are running on the host?**
   The running network services on the host are FTP, SSH, Telnet, HTTP, POP3, IMAP, HTTPS, and RDP.

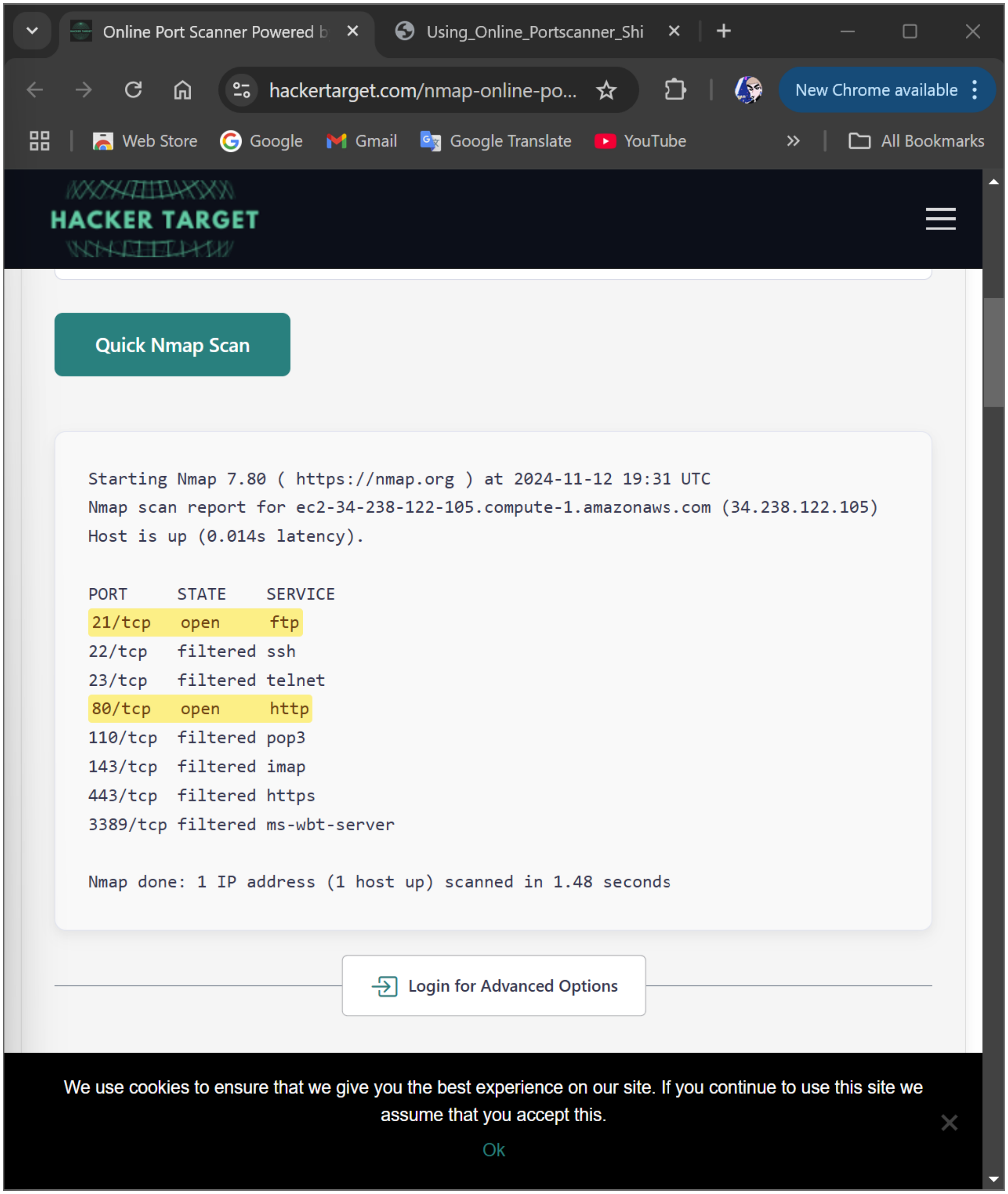


```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-12 19:31 UTC
Nmap scan report for ec2-34-238-122-105.compute-1.amazonaws.com (34.238.122.105)
Host is up (0.014s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  filtered https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

We use cookies to ensure that we give you the best experience on our site. If you continue to use this site we assume that you accept this.

2. **Which ports are open (specify ports DO NOT just show screenshot)?**

The open ports are 21/tcp and 80/tcp.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-12 19:31 UTC
Nmap scan report for ec2-34-238-122-105.compute-1.amazonaws.com (34.238.122.105)
Host is up (0.014s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  filtered https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

We use cookies to ensure that we give you the best experience on our site. If you continue to use this site we assume that you accept this.

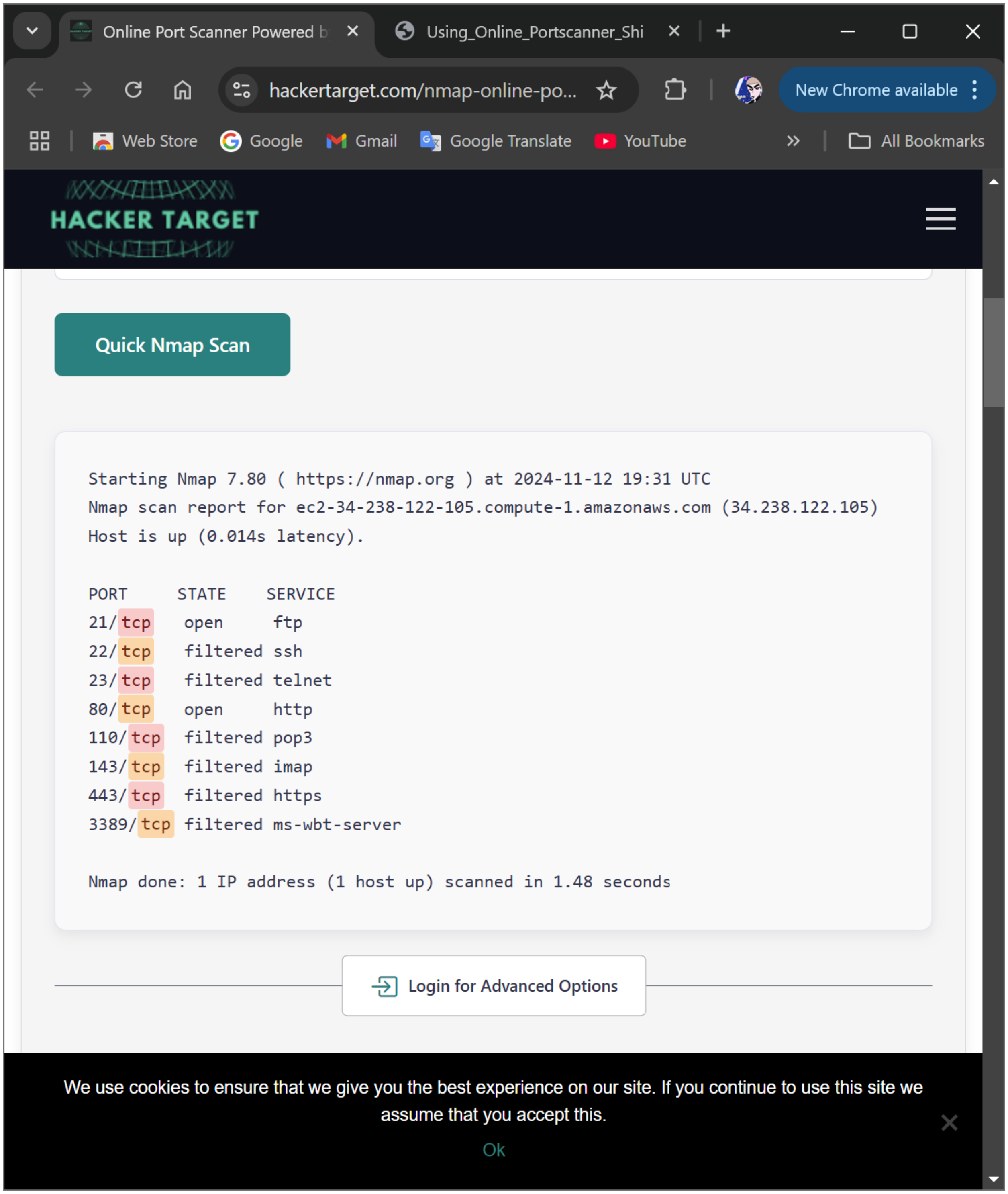
3. **Are these the standard ports for each network service (i.e., FTP using port 21 and not 2121)?**

   Yes, according to a couple of Google searches, the ports are standard for each network service listed:

   - SSH: Port 22

Telnet:	Port 23
SMTP:	Port 25
DNS:	Port 53
POP3:	Port 110
IMAP:	Port 143
HTTPS:	Port 443
RDP:	Port 3389

4. **Are the running network services using TCP or UDP?**
   The scan indicates the use of TCP for each open and filtered port in this list. There is no indication that any of the services are using UDP.

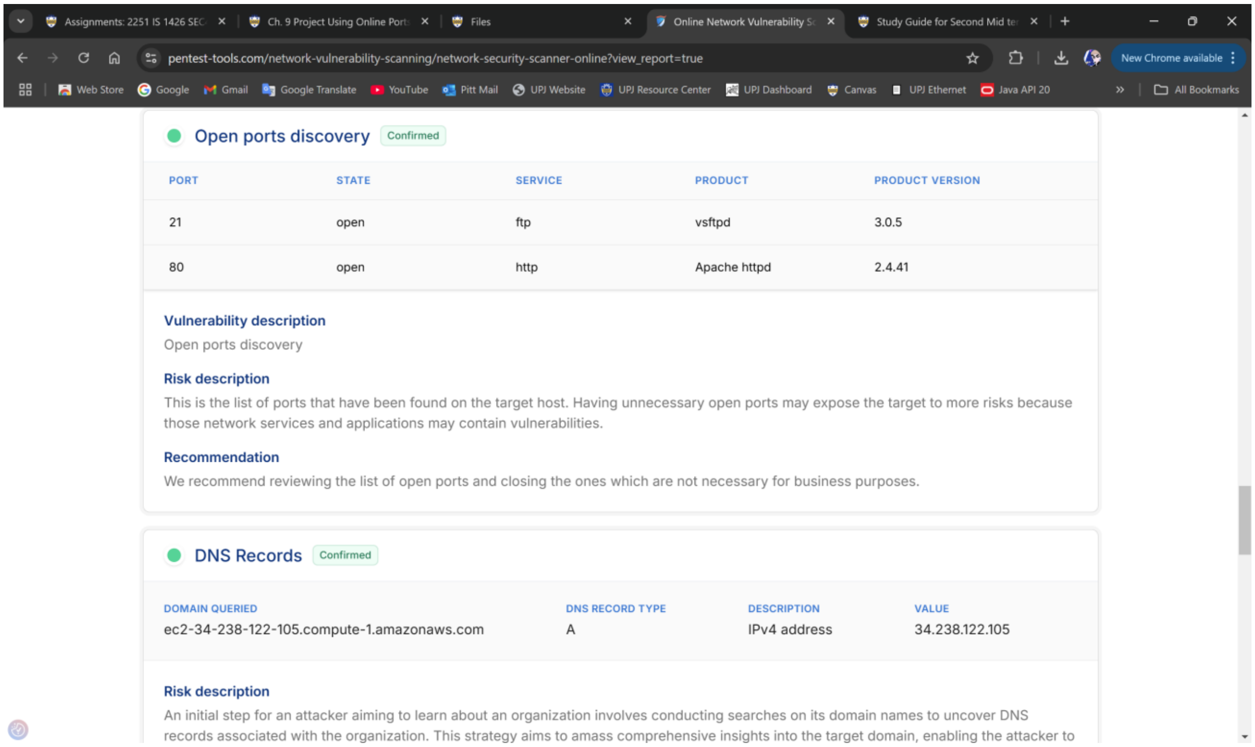


```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-12 19:31 UTC
Nmap scan report for ec2-34-238-122-105.compute-1.amazonaws.com (34.238.122.105)
Host is up (0.014s latency).

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  filtered https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

We use cookies to ensure that we give you the best experience on our site. If you continue to use this site we assume that you accept this.

5. **Do you have the same results using https://pentest-tools.com (Links to an external site.)? (Note: Select Network Vulnerability Scanner (Light))**

Yes, I have the same brief result, but many results are not shown here compared to online-port-scanner. However, pentest shows more about security information, while on the other hand, hackertarget only shows port, state, and service.


Assignments: 2251 IS 1426 SEC
Ch. 9 Project Using Online Ports
Files
Online Network Vulnerability Sc
Study Guide for Second Mid te
pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online?view_report=true
New Chrome available
Web Store
Google
Gmail
Google Translate
YouTube
Pitt Mail
UPJ Website
UPJ Resource Center
UPJ Dashboard
Canvas
UPJ Ethernet
Java API 20
All Bookmarks

● Open ports discovery Confirmed

PORT	STATE	SERVICE	PRODUCT	PRODUCT VERSION
21	open	ftp	vsftpd	3.0.5
80	open	http	Apache httpd	2.4.41

Vulnerability description

Open ports discovery

Risk description

This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation

We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

● DNS Records Confirmed

DOMAIN QUERIED	DNS RECORD TYPE	DESCRIPTION	VALUE
ec2-34-238-122-105.compute-1.amazonaws.com	A	IPv4 address	34.238.122.105

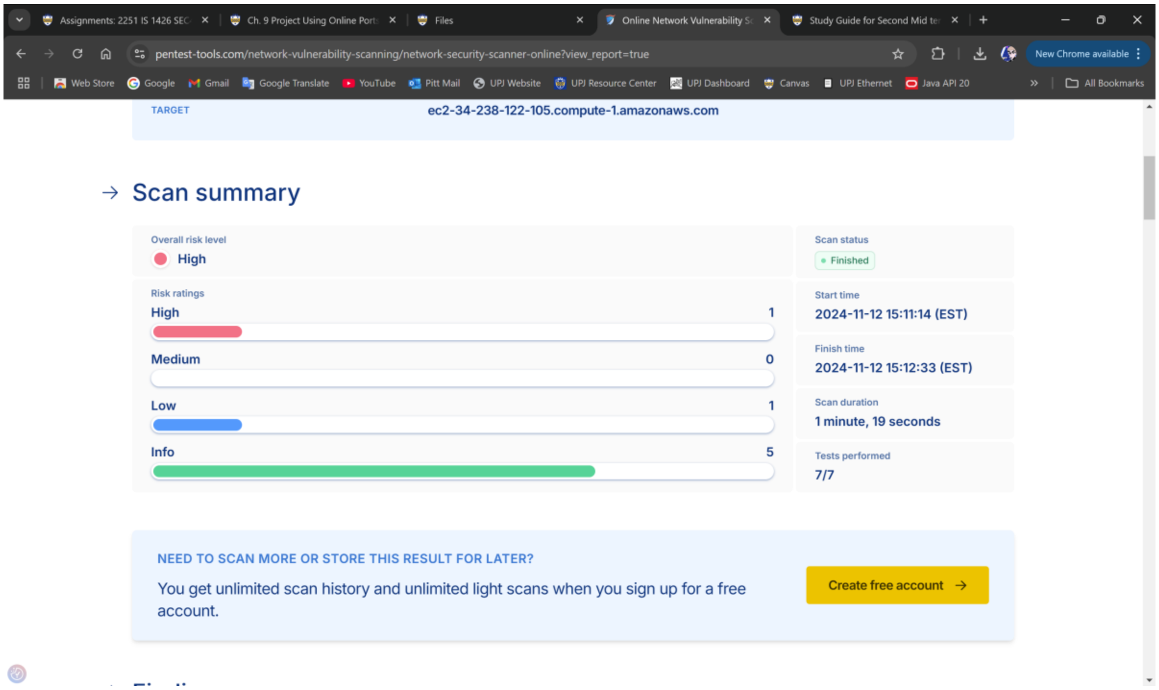
Risk description

An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to

6. **What additional information does https://pentest-tools.com (Links to an external site.) provide?**

The pentest light scan also includes:

- The risk level of the hostname
    - The vulnerabilities found for Apache HTTP Server 2.4.41 on Port 80.
    - The FTP service exposed to the Internet on Port 21.
    - Recommendation on vulnerability and/or risk


Assignments: 2251 IS 1426 SEC
Ch. 9 Project Using Online Port
Files
Online Network Vulnerability Sc
Study Guide for Second Mid te
pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online?view_report=true
New Chrome available
Web Store
Google
Gmail
Google Translate
YouTube
Pitt Mail
UPJ Website
UPJ Resource Center
UPJ Dashboard
Canvas
UPJ Ethernet
Java API 20
All Bookmarks

TARGET ec2-34-238-122-105.compute-1.amazonaws.com

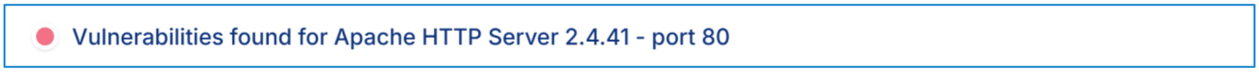
→ Scan summary

Overall risk level ● High	Scan status ● Finished
Risk ratings High 1	Start time 2024-11-12 15:11:14 (EST)
Medium 0	Finish time 2024-11-12 15:12:33 (EST)
Low 1	Scan duration 1 minute, 19 seconds
Info 5	Tests performed 7/7

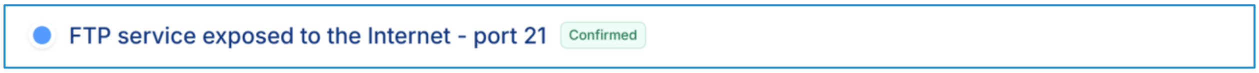
NEED TO SCAN MORE OR STORE THIS RESULT FOR LATER?

You get unlimited scan history and unlimited light scans when you sign up for a free account.

Create free account →

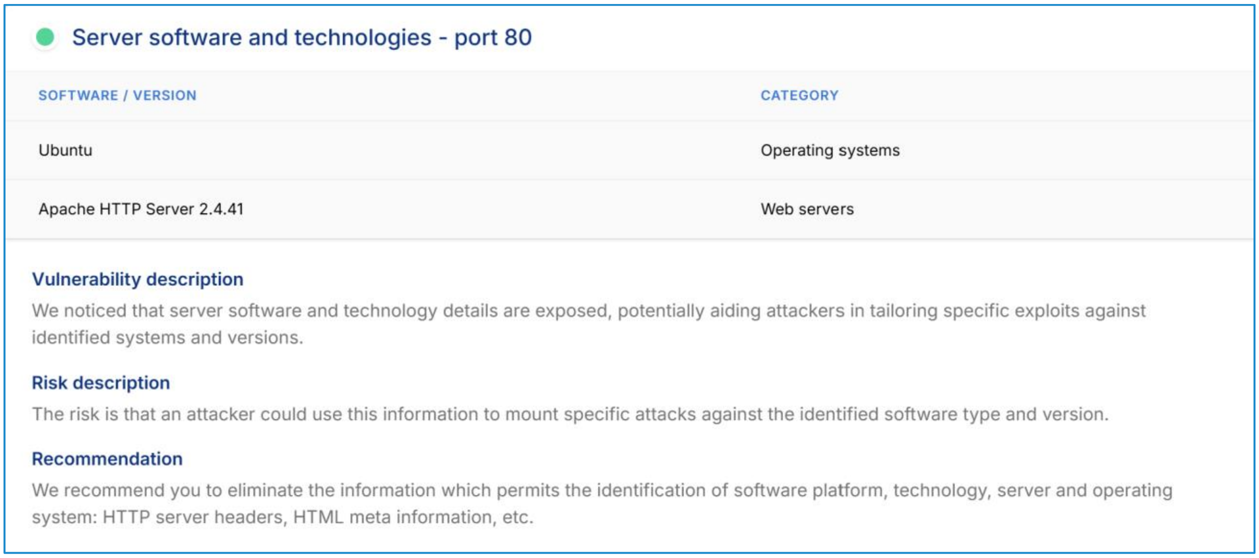


● Vulnerabilities found for Apache HTTP Server 2.4.41 - port 80



● FTP service exposed to the Internet - port 21 Confirmed

- Server software
  - **Operating Systems:** Ubuntu
  - **Web Server:** Apache HTTP Server 2.4.41



● Server software and technologies - port 80

SOFTWARE / VERSION	CATEGORY
Ubuntu	Operating systems
Apache HTTP Server 2.4.41	Web servers

Vulnerability description

We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

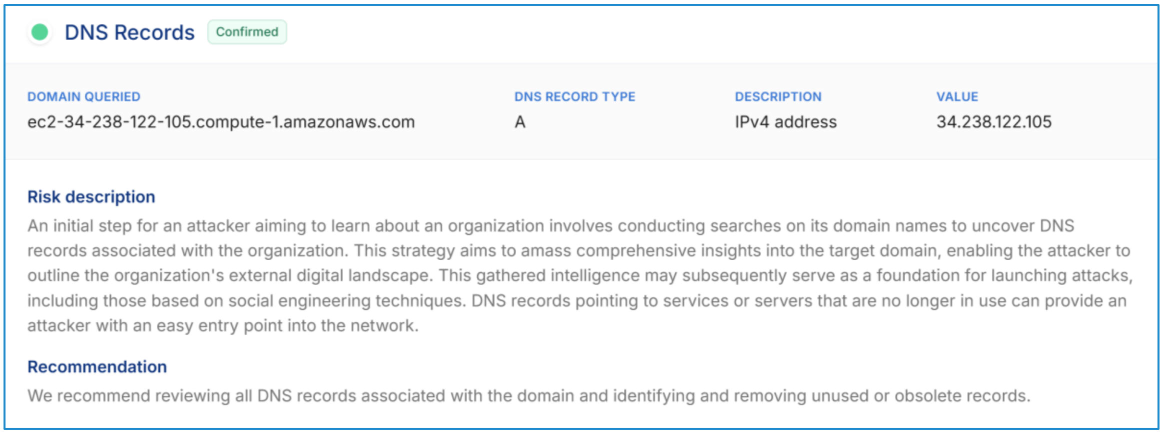
Risk description

The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

- DNS records
  - **DNS Record type:** A
  - **Description:** IPv4 Address
  - **Value (IP Address):** 34.238.122.105



● DNS Records Confirmed

DOMAIN QUERIED	DNS RECORD TYPE	DESCRIPTION	VALUE
ec2-34-238-122-105.compute-1.amazonaws.com	A	IPv4 address	34.238.122.105

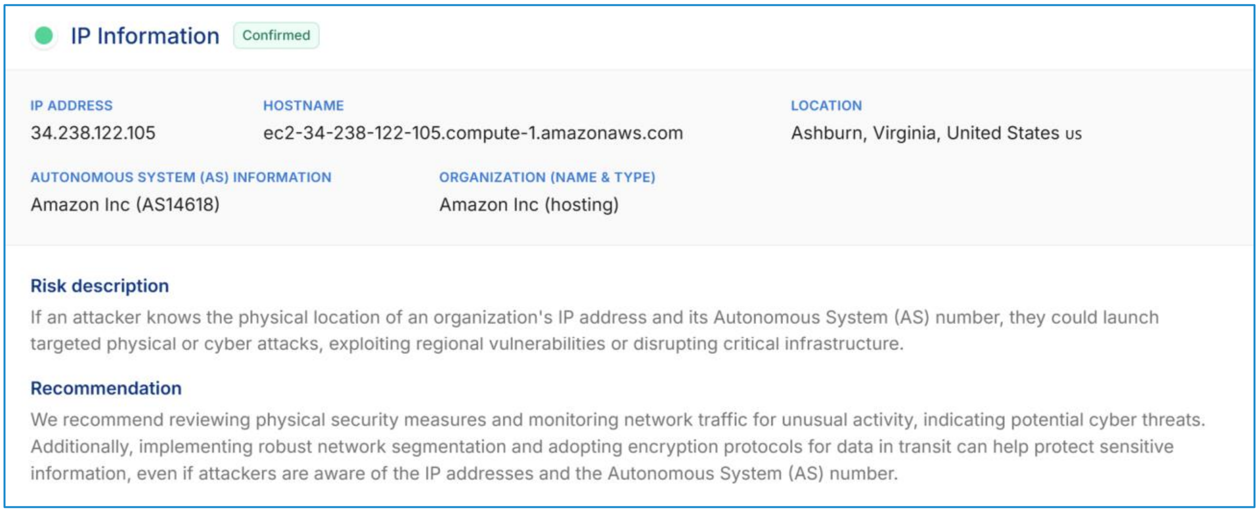
Risk description

An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation

We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

- IP address information
  - **Location:** Ashburn, Virginia, and United States
  - **Autonomous System Information:** Amazon Inc (AS14618)
  - **Organization:** Amazon Inc (hosting)



● IP Information Confirmed

IP ADDRESS	HOSTNAME	LOCATION
34.238.122.105	ec2-34-238-122-105.compute-1.amazonaws.com	Ashburn, Virginia, United States US

AUTONOMOUS SYSTEM (AS) INFORMATION	ORGANIZATION (NAME & TYPE)
Amazon Inc (AS14618)	Amazon Inc (hosting)

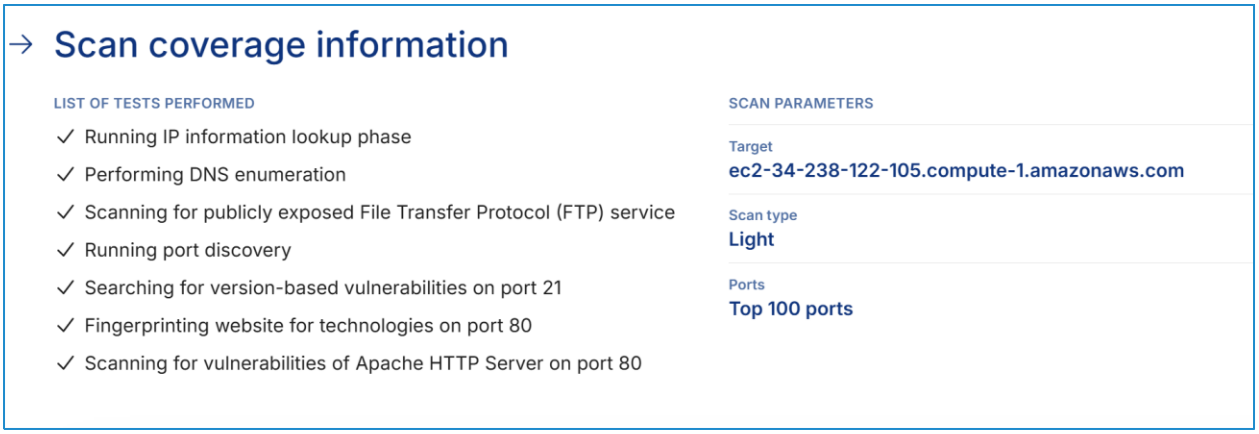
Risk description

If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation

We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

- Scan coverage information
  - Running IP information lookup phase
  - Performing DNS enumeration
  - Scanning for publicly exposed File Transfer Protocol (FTP) service
  - Running port discovery
  - Searching for version-based vulnerabilities on port 21
  - Fingerprinting website for technologies on port 80
  - Scanning for vulnerabilities of Apache HTTP Server on port 80



→ Scan coverage information

LIST OF TESTS PERFORMED

- ✓ Running IP information lookup phase
- ✓ Performing DNS enumeration
- ✓ Scanning for publicly exposed File Transfer Protocol (FTP) service
- ✓ Running port discovery
- ✓ Searching for version-based vulnerabilities on port 21
- ✓ Fingerprinting website for technologies on port 80
- ✓ Scanning for vulnerabilities of Apache HTTP Server on port 80

SCAN PARAMETERS

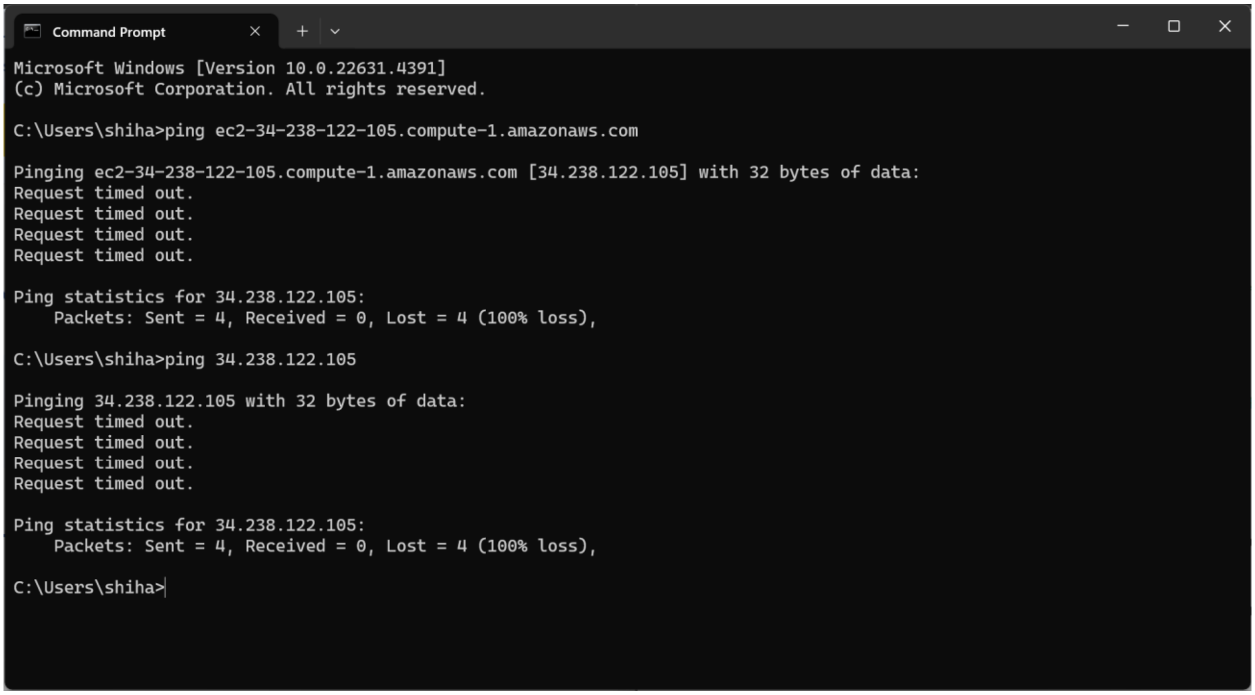
Target
ec2-34-238-122-105.compute-1.amazonaws.com

Scan type
Light

Ports
Top 100 ports

7. **Is the host pingable? Hint: online-port-scanner will not tell you this!**

No, hostname ec2-34-238-122-105.compute-1.amazonaws.com, is not pingable.



```
Microsoft Windows [Version 10.0.22631.4391]
(c) Microsoft Corporation. All rights reserved.

C:\Users\shiha>ping ec2-34-238-122-105.compute-1.amazonaws.com

Pinging ec2-34-238-122-105.compute-1.amazonaws.com [34.238.122.105] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.238.122.105:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\shiha>ping 34.238.122.105

Pinging 34.238.122.105 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.238.122.105:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\shiha>
```

8. **Which cloud provider is hosting the server you are scanning? How do you know?**

By looking at the hostname, ec2-34-238-122-105.compute-1.amazonaws.com, we can tell that the server is hosted on Amazon Web Services (AWS). The ec2 prefix and amazonaws.com domain indicate Amazon Elastic Compute Cloud (EC2), a service provided by AWS.