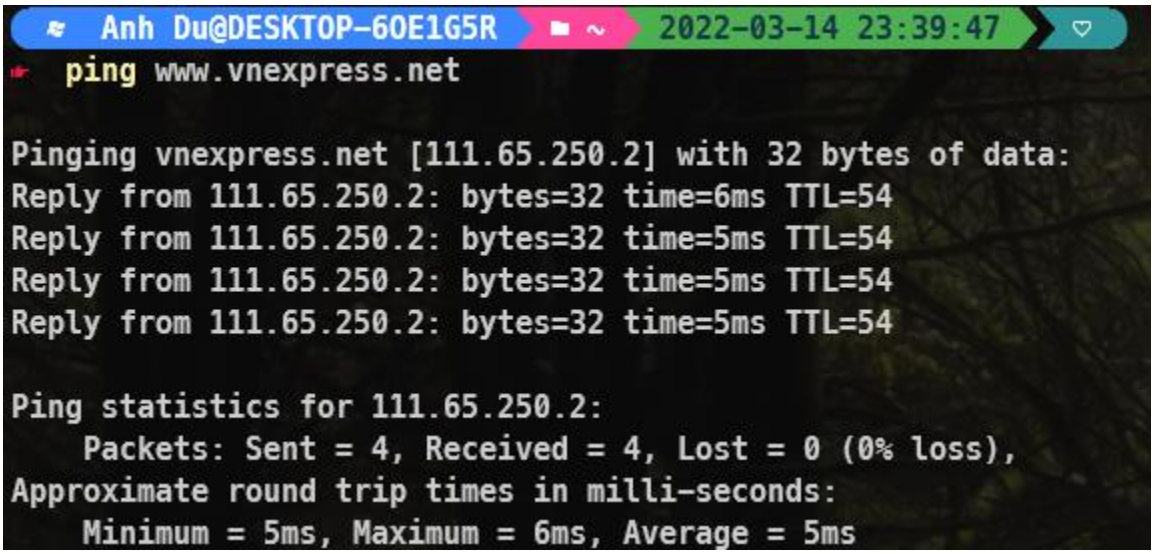
Họ tên: Huỳnh Anh Dự

MSSV: 450110401

LAB CÁ NHÂN

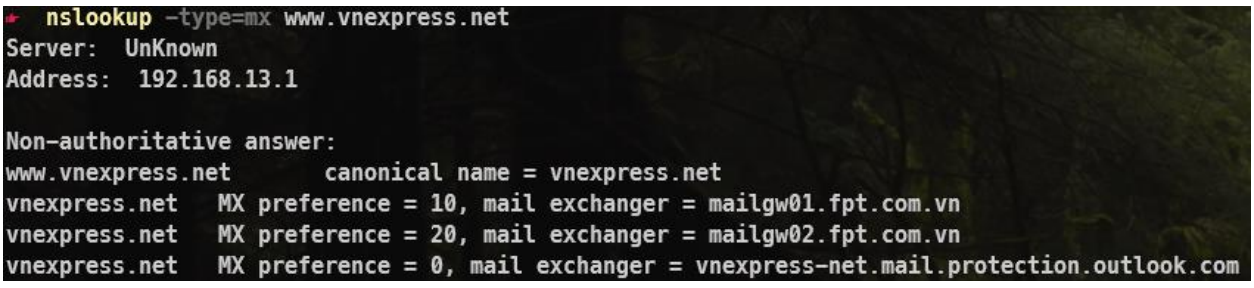
LAP01:

1/ Ping:



2/ NSLOOKUP:

+ Tìm MX record (Mail Exchange Record):



+ Tìm A record:

```
nslookup -type=a www.vnexpress.net
Server:  UnKnown
Address:  192.168.13.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    vnexpress.net
Address:  111.65.250.2
Aliases:  www.vnexpress.net
```

+ Tìm NS record:

```
nslookup -type=ns www.vnexpress.net
Server:  UnKnown
Address:  192.168.13.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
www.vnexpress.net       canonical name = vnexpress.net
vnexpress.net   nameserver = ns2.fptonline.vn
vnexpress.net   nameserver = ns1.fptonline.vn
```

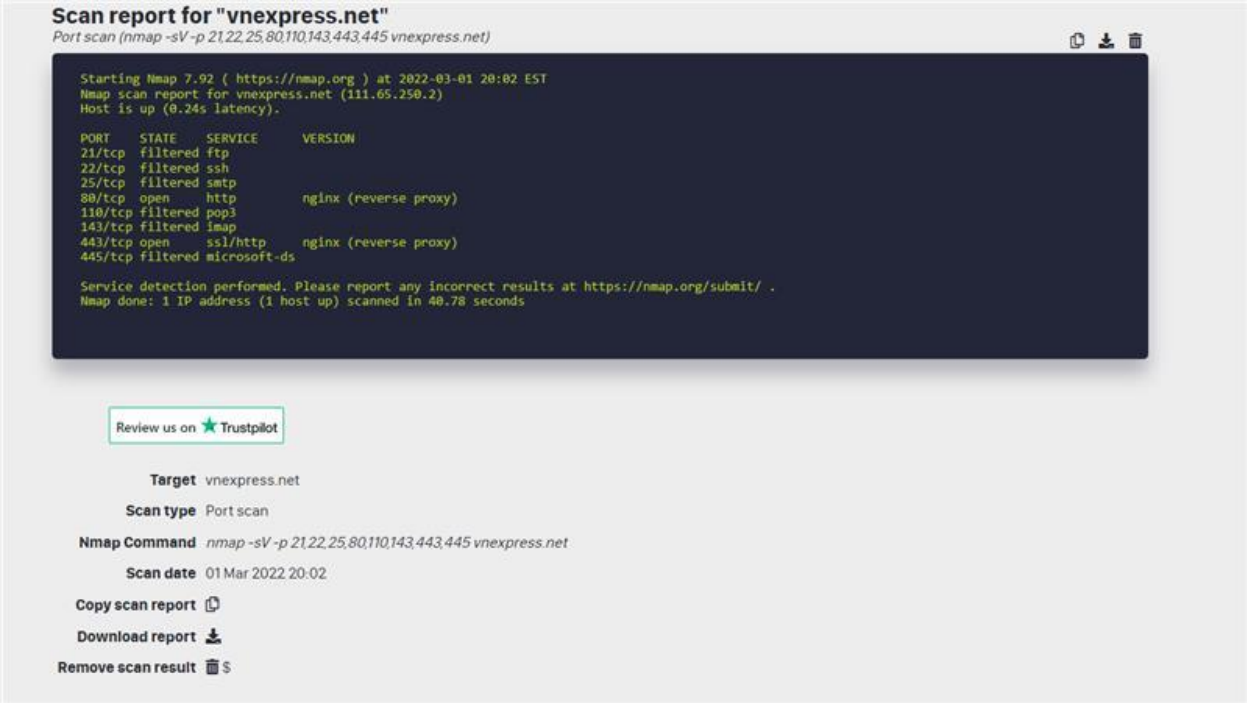
+ Tìm SOA Record:

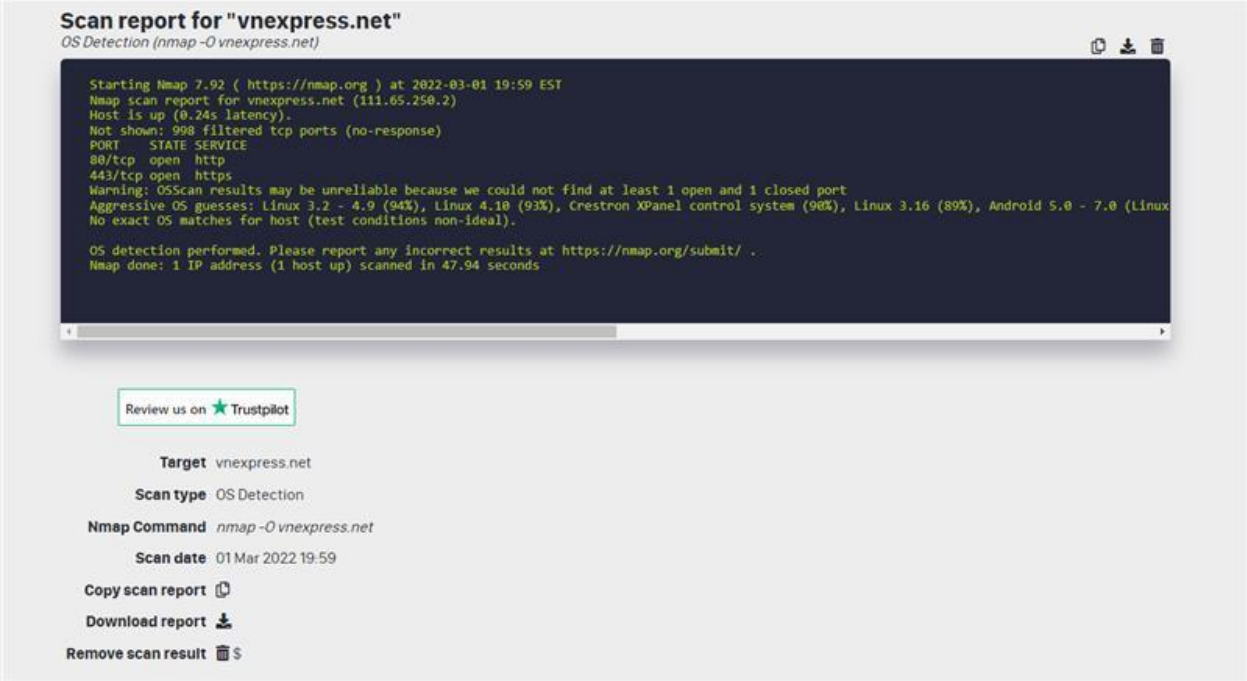
```
nslookup -type=soa www.vnexpress.net
Server:  UnKnown
Address:  192.168.13.1

Non-authoritative answer:
www.vnexpress.net       canonical name = vnexpress.net
vnexpress.net
        primary name server = ns1.fptonline.vn
        responsible mail addr = thuannv7.fpt.com.vn
        serial  = 2019051387
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 604800 (7 days)
        default TTL = 300 (5 mins)
```

3/ Traceroute:

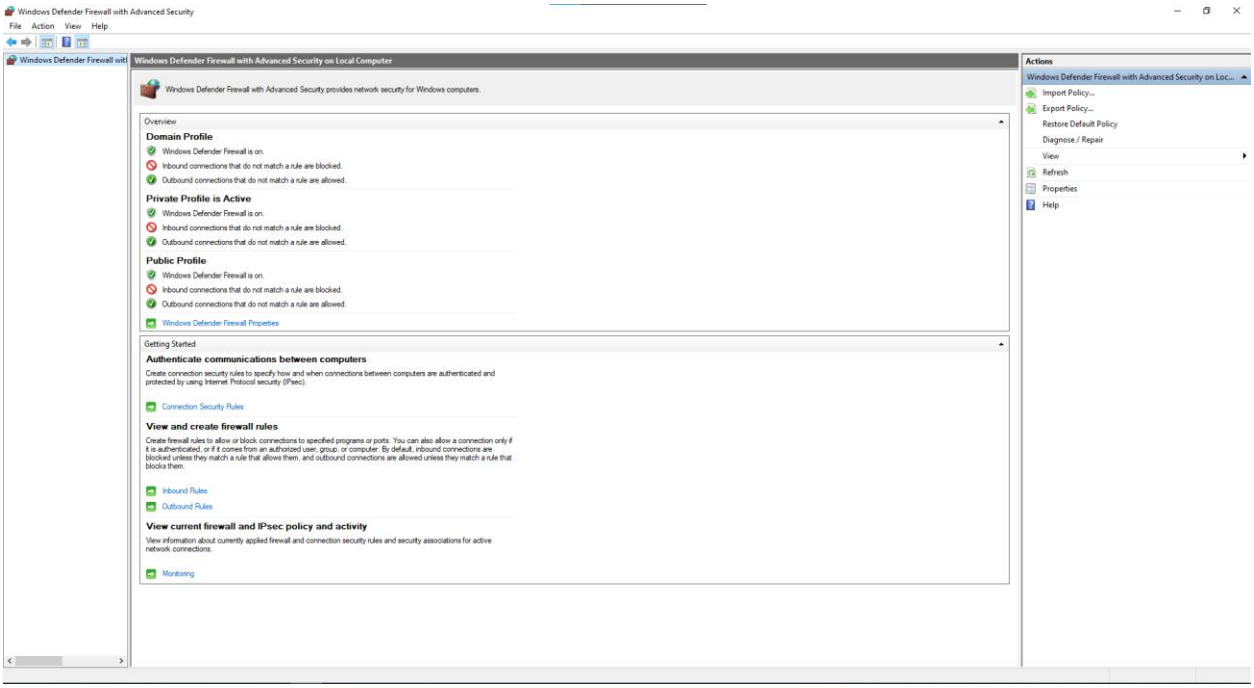
```
tracert www.vnexpress.net

Tracing route to www.vnexpress.net [111.65.250.2]
over a maximum of 30 hops:

  1     4 ms     4 ms     2 ms  192.168.13.1
  2     6 ms     2 ms     2 ms  192.168.0.1
  3     4 ms     4 ms     4 ms  100.123.1.62
  4     6 ms     4 ms     6 ms  118.69.253.221
  5     4 ms     4 ms     7 ms  100.123.0.254
  6     7 ms     5 ms     4 ms  183.80.132.38
  7     5 ms     4 ms     *     118.69.132.133
  8     5 ms     5 ms     3 ms  42.117.11.95
  9     4 ms     6 ms     4 ms  118.69.39.30
 10    10 ms     4 ms     4 ms  10.250.4.22
 11     5 ms    13 ms     5 ms  111.65.250.2

Trace complete.
```

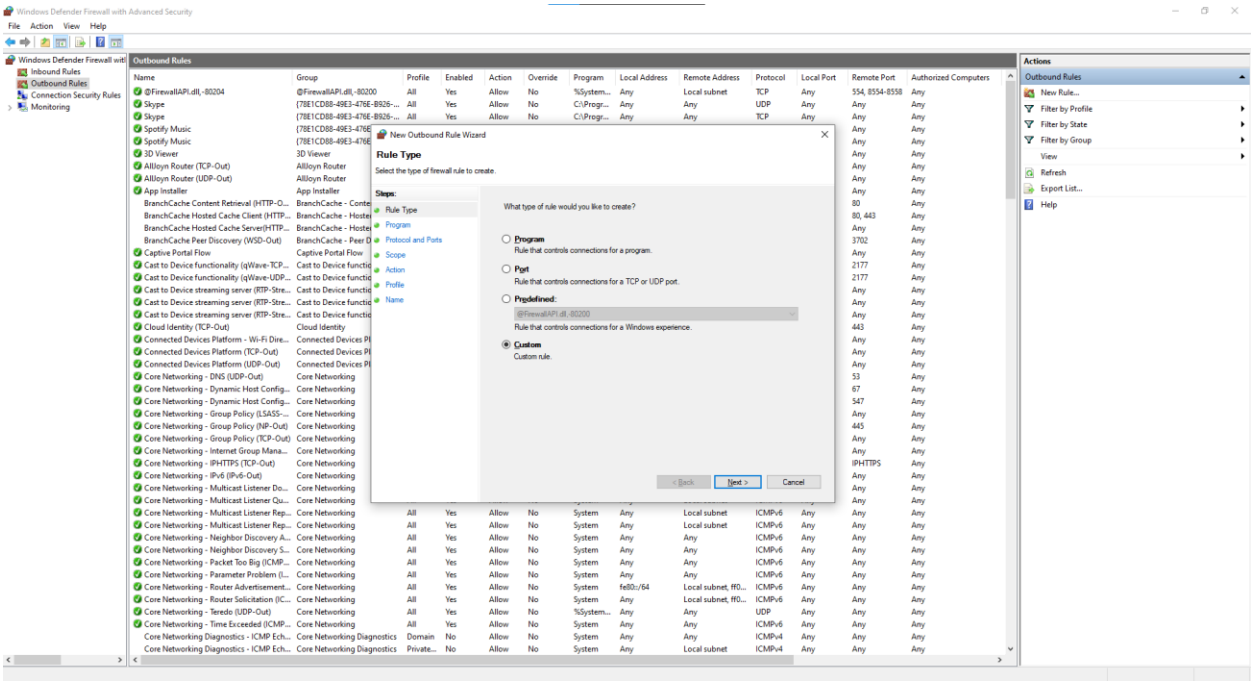
LAB02:

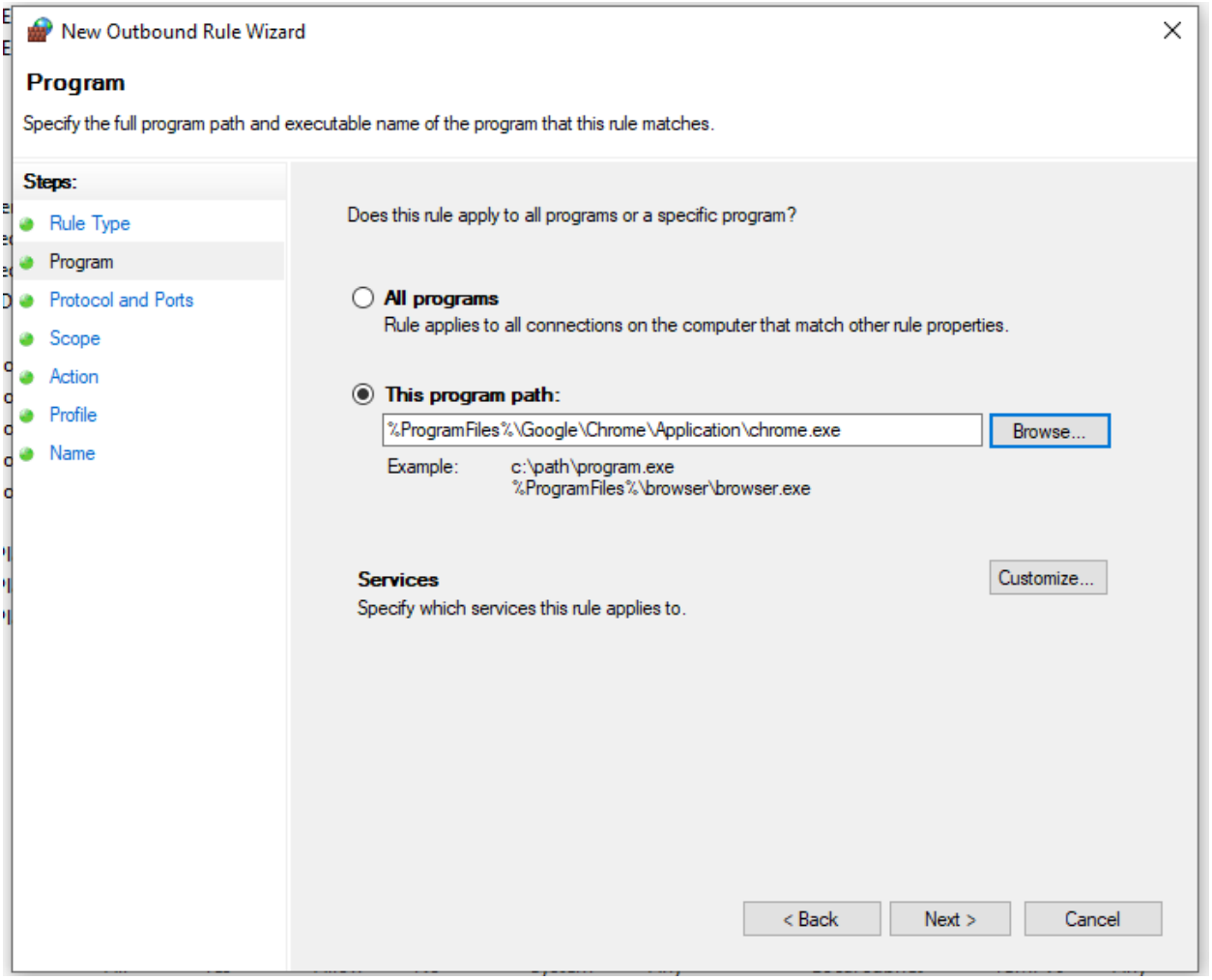

Scan report for "vnexpress.net"
Port scan (nmap -sV -p 21,22,25,80,110,143,443,445 vnexpress.net)
Starting Nmap 7.92 (https://nmap.org) at 2022-03-01 20:02 EST
Nmap scan report for vnexpress.net (111.65.250.2)
Host is up (0.24s latency).
PORT STATE SERVICE VERSION
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp filtered smtp
80/tcp open http nginx (reverse proxy)
110/tcp filtered pop3
143/tcp filtered imap
443/tcp open ssl/http nginx (reverse proxy)
445/tcp filtered microsoft-ds
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.78 seconds
Review us on Trustpilot
Target vnexpress.net
Scan type Port scan
Nmap Command nmap -sV -p 21,22,25,80,110,143,443,445 vnexpress.net
Scan date 01 Mar 2022 20:02
Copy scan report
Download report
Remove scan result $

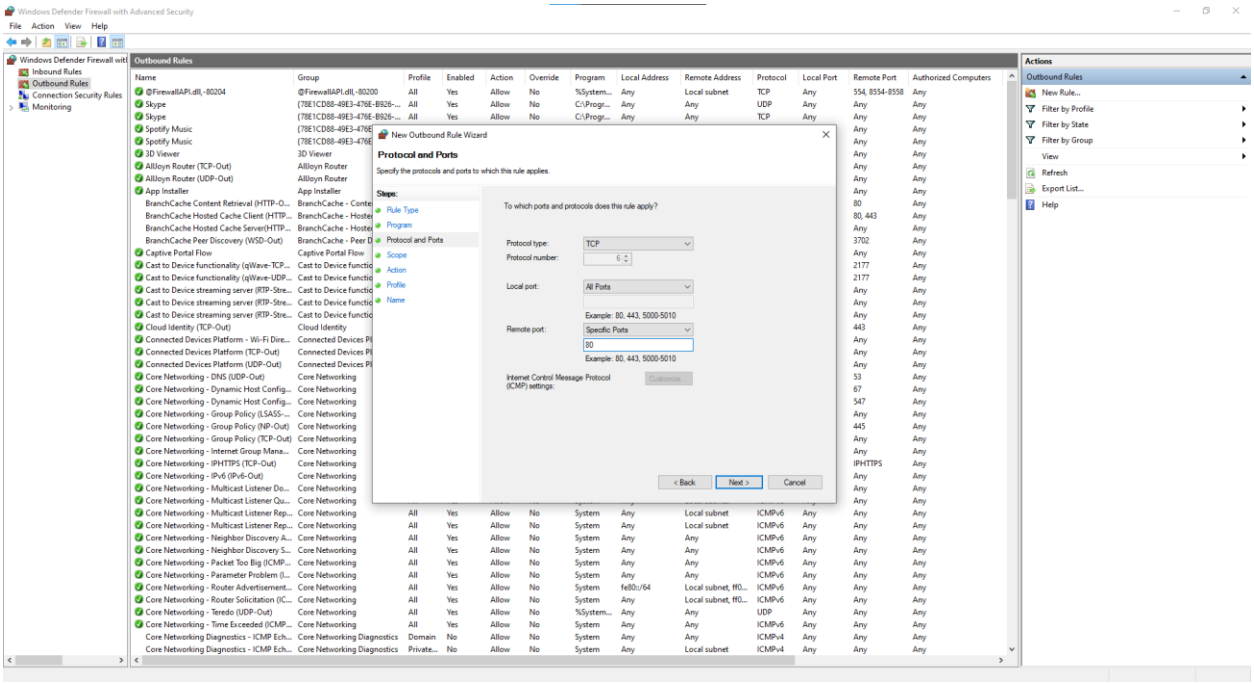

Scan report for "vnexpress.net"
OS Detection (nmap -O vnexpress.net)
Starting Nmap 7.92 (https://nmap.org) at 2022-03-01 19:59 EST
Nmap scan report for vnexpress.net (111.65.250.2)
Host is up (0.24s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (94%), Linux 4.10 (93%), Crestron XPanel control system (90%), Linux 3.16 (89%), Android 5.0 - 7.0 (Linux
No exact OS matches for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.94 seconds
Review us on Trustpilot
Target vnexpress.net
Scan type OS Detection
Nmap Command nmap -O vnexpress.net
Scan date 01 Mar 2022 19:59
Copy scan report
Download report
Remove scan result $

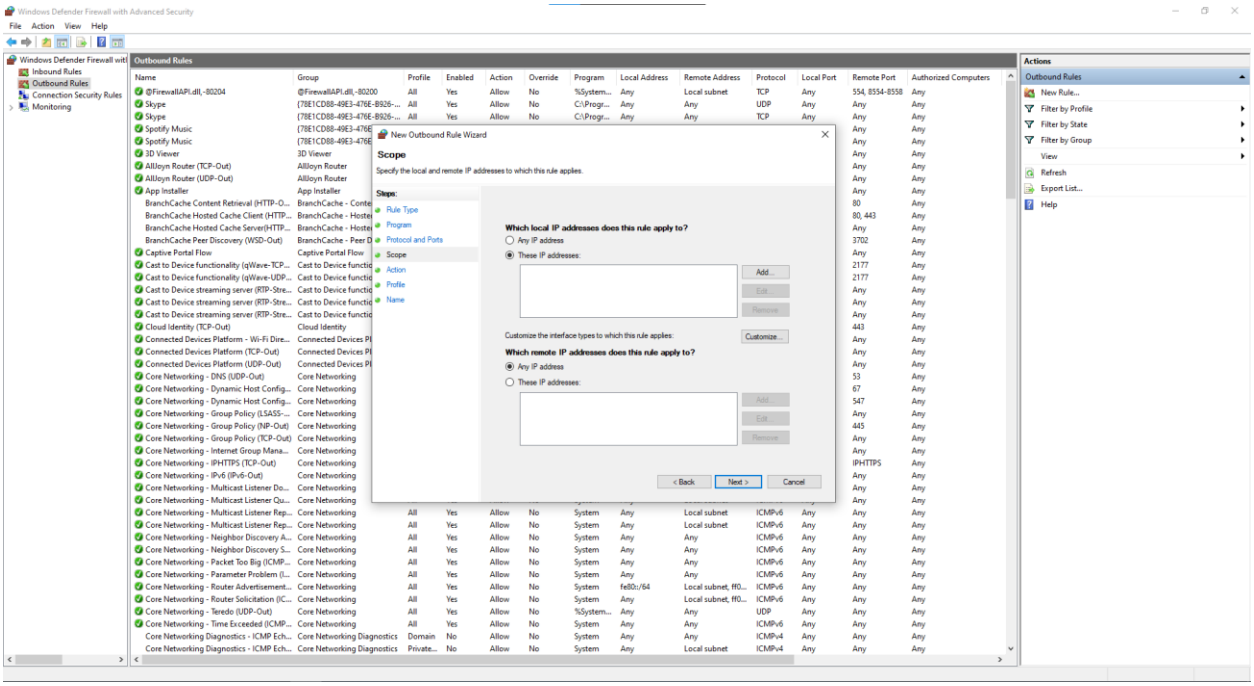
LAB05:

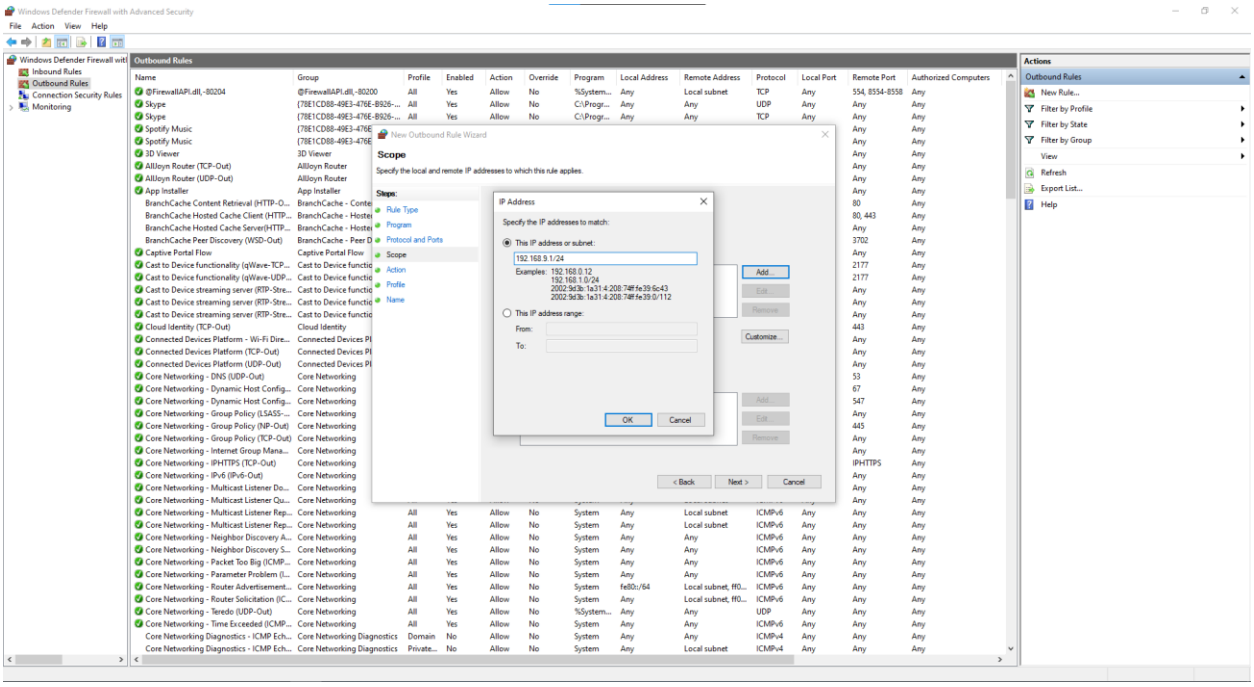

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
Inbound Rules
Outbound Rules
View current firewall and IPsec policy and activity
View information about currently applied firewall and connection security rules and security associations for active network connections.
Monitoring
Actions
Windows Defender Firewall with Advanced Security on Loc...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

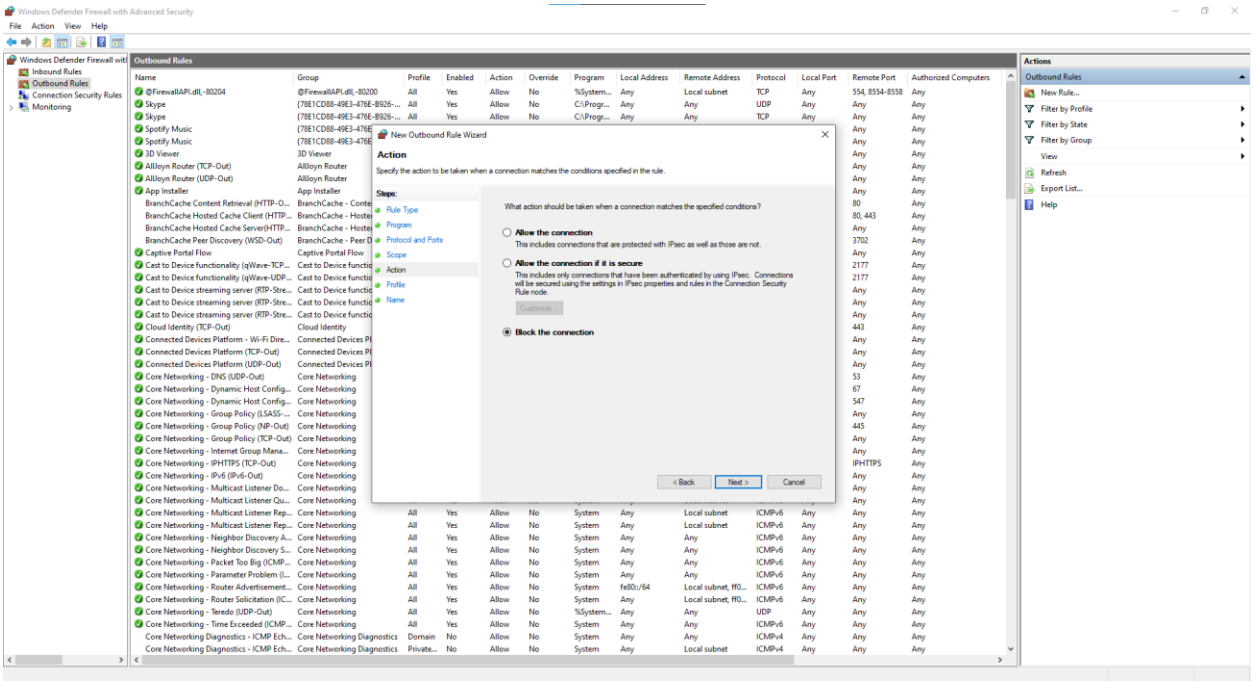

Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
New Outbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

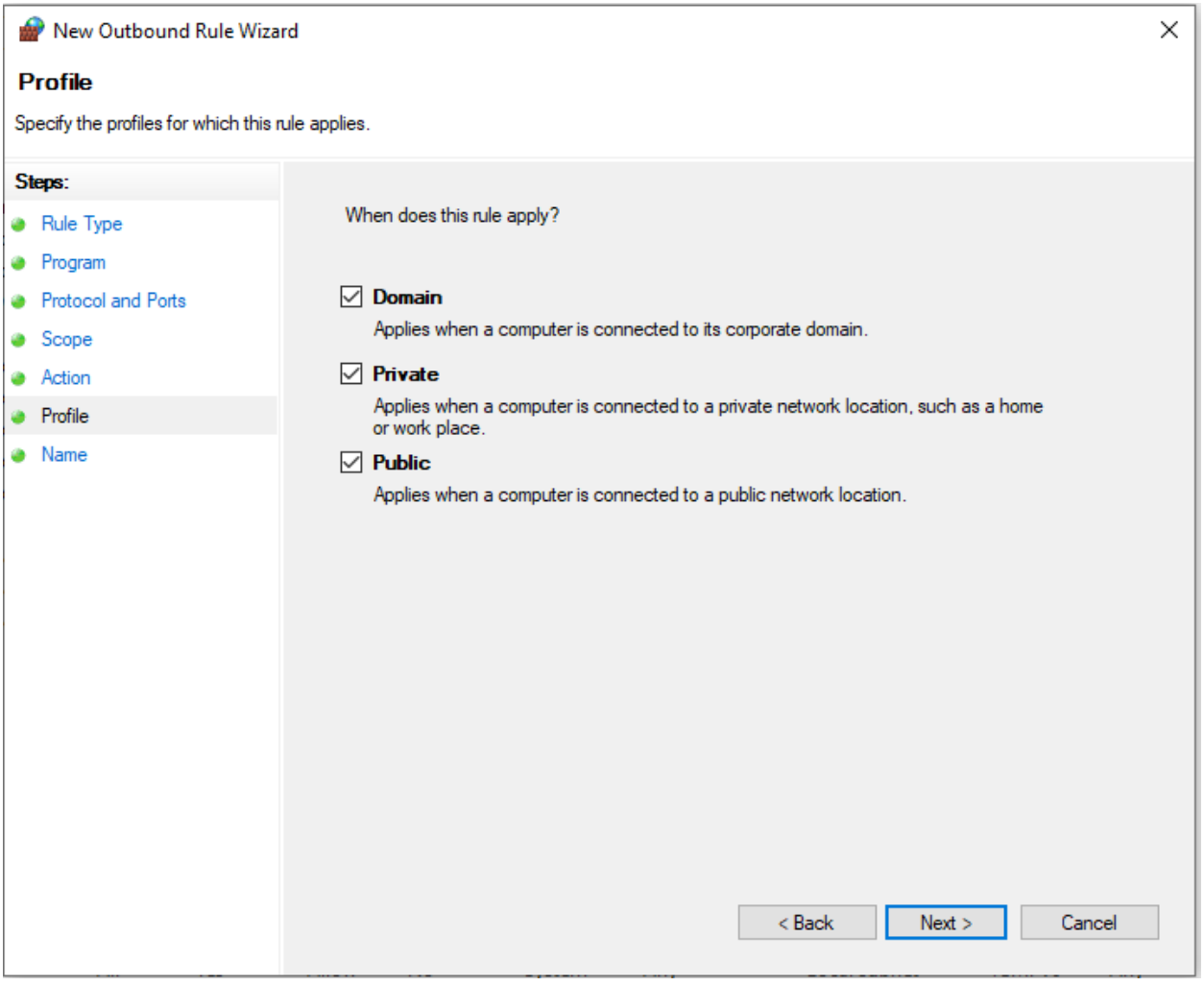

New Outbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles%\Google\Chrome\Application\chrome.exe
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel

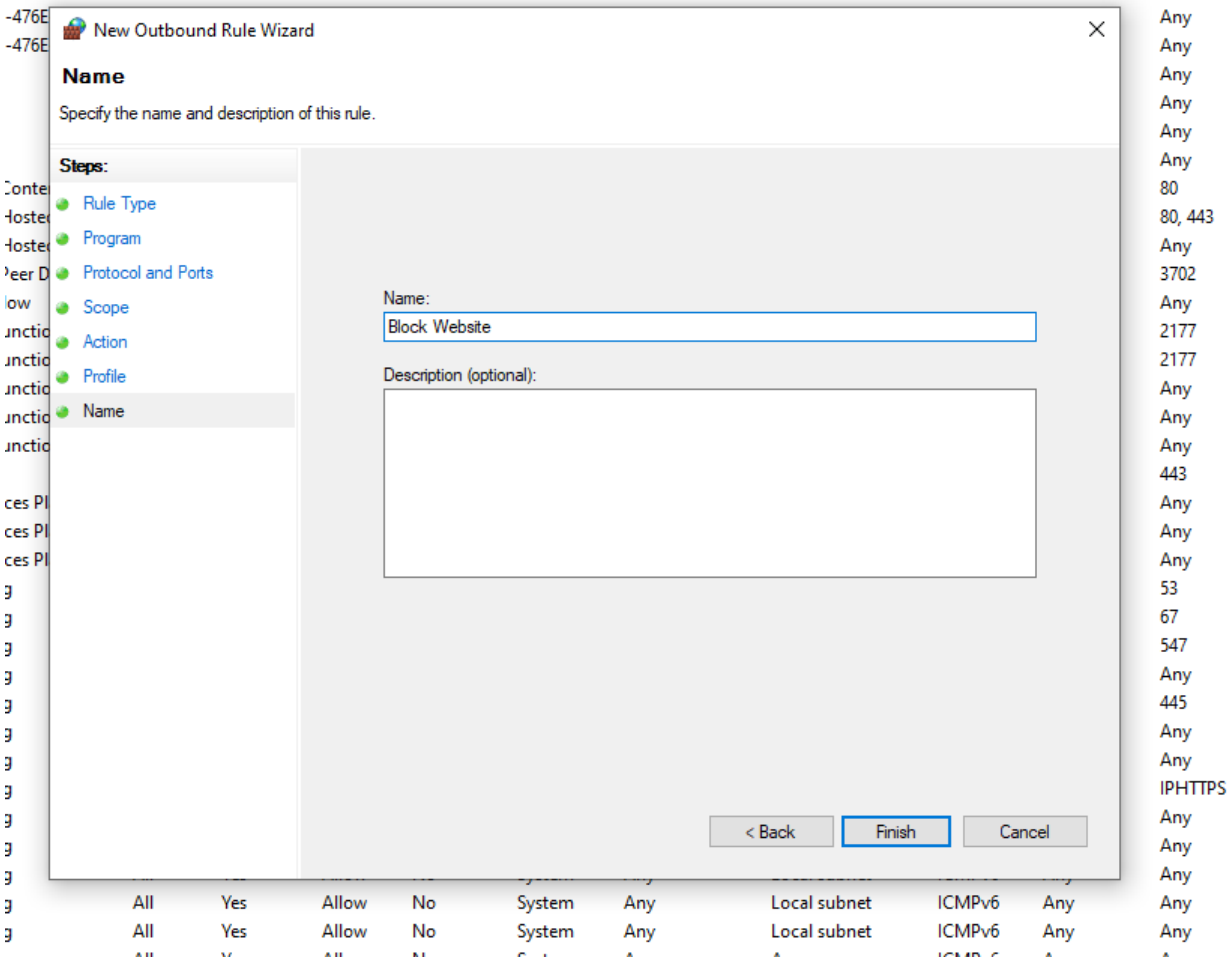


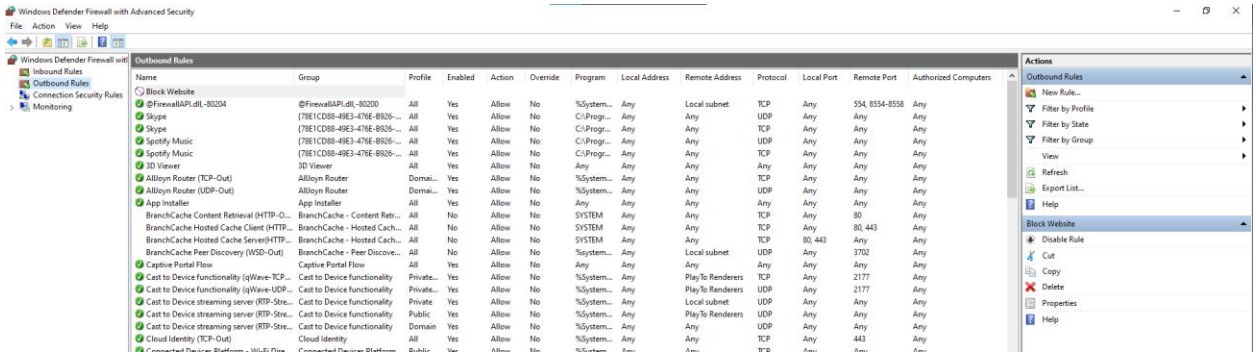

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
Remote Address
Protocol
Local Port
Remote Port
Authorized Computers
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Outbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove...
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
New Outbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
IP Address
Specify the IP addresses to match:
This IP address or subnet:
192.168.9.1/24
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
OK
Cancel
Add...
Edit...
Remove...
Customize...
< Back
Next >
Cancel




New Outbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel


New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
Block Website
Description (optional):
< Back
Finish
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Outbound Rules
Actions