اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

SUBJECT: BCN2023 DATA AND NETWORK SECURITY
SEMESTER I 2024/2025
LECT NAME: ENCIK ABDULLAH BIN MAT SAFRI
TITLE: PROGRESSION

NAME	MATRIC ID	SECTION
RASYID BIN ROSLI	CA22076	01B
NUR AMIRAH SHAHIRA BINTI ZULKIFLI	CA22044	01A
AMIRULARIFF ISKANDAR BIN ADNAN	CD22026	01B
NUR SYAHILA BINTI KHARULAZWA	CB22063	01A

ROLES AND RESPONSIBILITIES

NAME	ROLE	RESPONSIBILITIES
	BLUE TEAM	
NUR AMIRAH SHAHIRA BINTI ZULKIFLI	BLUE TEAM	Responsible for defense mechanism and mitigation plan
RASYID BIN ROSLI	RED TEAM	Responsible for attacking mechanism
AMIRULARIFF ISKANDAR BIN ADNAN	RED TEAM	Responsible for attacking mechanism

TABLE OF CONTENT

Red Team Configuration and Tools.......... **5**

Tools to Use:.......... 5

Activities and Steps:.......... 5

Network Configuration:.......... 5

Blue Team Configuration and Tools.......... **7**

Tools to Use:.......... 7

Key Features of Nmap..........**17**

Nmap in Security Defense.......... **18**

1. Vulnerability Identification.......... 18

2. Attack Surface Reduction.......... 18

3. Monitoring Network Changes.......... 18

4. Testing Security Configurations.......... 18

Strengths and Limitations.......... **18**

Strengths:.......... 18

Limitations:..........18

Key Features of Wireshark.......... **20**

Wireshark in Security Defense..........**20**

Detecting Threats.......... 20

Blue Team Strategy.......... 21

Strengths and Limitations.......... **21**

Strengths:.......... 21

Limitations:..........21

Activities and Steps:.......... 21

Network Configuration:.......... 22

Overview of Team Responsibilities..........**22**

1. FINAL PROJECT SUMMARY

The project involves setting up a simulated cyber-security environment with three virtual operating systems (Windows, Linux, and another designated as an attacker). It evaluates Red Team (attackers) and Blue Team (defenders) roles, including their tools, techniques, and response mechanisms. The project emphasizes attack execution, defense measures, and mitigation plans to enhance the participants' understanding of data and network security concepts.

1.1 CONTENT SUMMARY

SCOPE

SCHEDULE

- **Week 1: Research and environment setup.**
- **Week 2: Initial attacks and defense setup.**
- **Week 3: Advanced attacks and mitigations.**
- **Week 4: Documentation and final report preparation.**

COSTS

- **Virtualization Software: Free (VirtualBox).**
- **Operating System Licenses: Free (using open-source Linux distributions and trial versions of Windows).**
- **Tools: Open-source tools like Wireshark, Nmap, Metasploit, and Snort.**

RISKS

RISK DESCRIPTION	IMPACT LEVEL	PROBABILITY	MITIGATION
Virtual environment failure	High	High	Regular backups and use of snapshots.
Misconfiguration issues	Medium	High	Double-check configurations; assign a QA lead.
Time overruns	Medium	Medium	Define strict deadlines and regular checkpoints.
Tool incompatibility	Medium	Medium	Pre-test all tools and versions before use.

COMMUNICATION STRATEGY AND METHODS

Whatsapp platform for communication regarding the project

1.2 LESSONS LEARNED

1. **The importance of understanding OS-level security settings for hardening systems.**
2. **2. Practical implementation of attack and defense strategies for real-world scenarios.**
3. **Effective team collaboration and communication for managing cybersecurity incidents.**
4. **Critical thinking in assessing risks and developing mitigation strategies.**

1.3 LEARNING OUTCOMES

Briefly summarize how the learning outcomes were met. Then, describe the outcomes in detail in each section below. If applicable, provide the relevant Appendix number for the reader to reference.

OUTCOME NAME	
1. Ability to deploy and configure secure virtual environments. **2. Proficiency in using cybersecurity tools like Wireshark, Nmap, Metasploit, and Snort.** **3. Enhanced understanding of Red Team attack techniques and Blue Team defense mechanisms.** **4. Improved documentation and reporting skills in a professional security context.**	

DISCLAIMER

Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.

RED TEAM

Red Team Configuration and Tools

Tools to Use:

1. Metasploit Framework
   - A penetration testing tool for simulating attacks and exploiting vulnerabilities in systems.
2. Social-Engineering Toolkit (SET)
   - Used for phishing attacks, website cloning, and other social engineering exploits.
3. SQLMap
   - An automated tool for detecting and exploiting SQL injection vulnerabilities in web applications.
4. John the Ripper
   - A password-cracking tool that performs brute force or dictionary attacks on hashed passwords.

Activities and Steps:

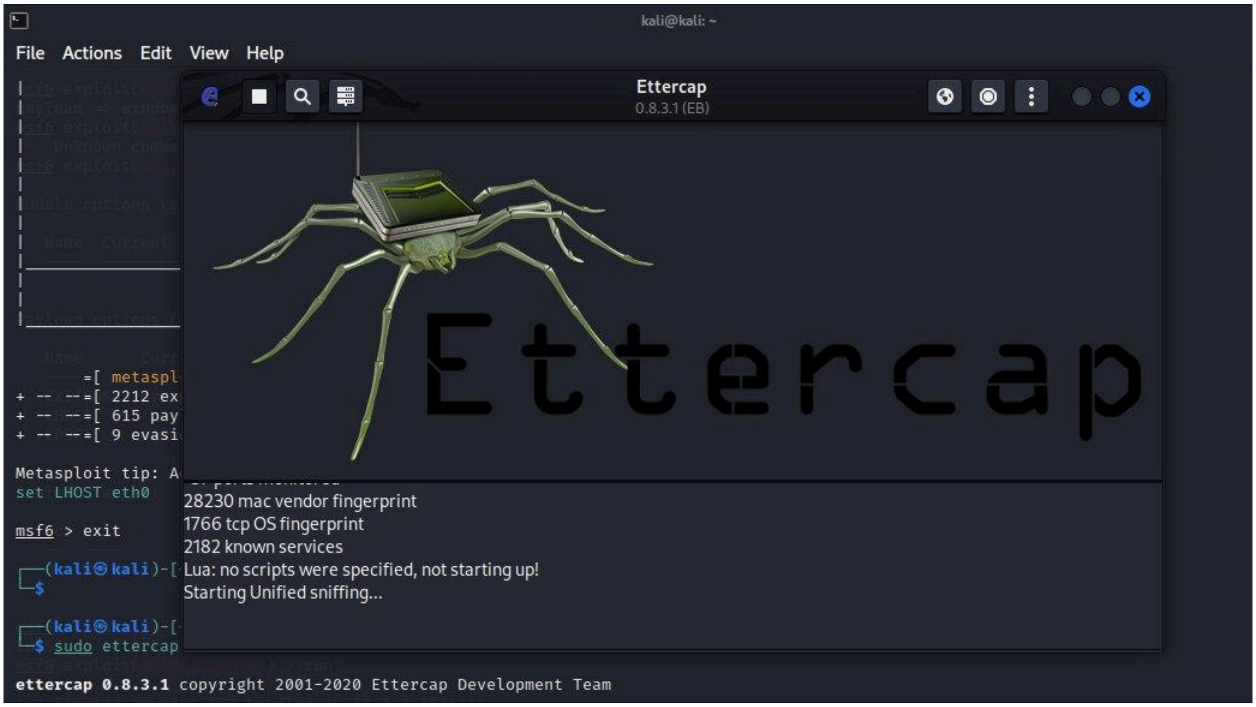
1. Phishing Attack:
   - Use Social-Engineering Toolkit (SET) to craft a fake website or phishing email.
   - Example: Clone a legitimate website (e.g., Google or Twitter) and send the link via email to the Blue Team's machine.
   - Monitor any credentials entered into the fake website.
2. Payload Delivery with Metasploit:
   - Create a backdoor using msfvenom.
   - Deliver the payload via phishing email or malicious website.
   - Gain remote access to the target system using Meterpreter.
   - Example: Exploit a vulnerable Windows machine using a reverse TCP connection.
3. SQL Injection:
   - Use SQLMap to test a web application for SQL injection vulnerabilities.
   - Example: Target a URL with potential vulnerabilities (e.g., `http://testphp.vulnweb.com/login.php`).
   - Extract sensitive data from the database if successful.
4. Password Cracking:
   - Use John the Ripper to crack hashed passwords retrieved during attacks.
   - Attempt brute force, dictionary attacks, or hybrid attacks to find weak passwords.

Network Configuration:

- Virtual Machine: Kali Linux with offensive tools.
- IP Address: `10.0.2.15` (Example).
- Network Mode: NAT or Host-Only for secure and isolated testing.

ATTACKING TOOLS:

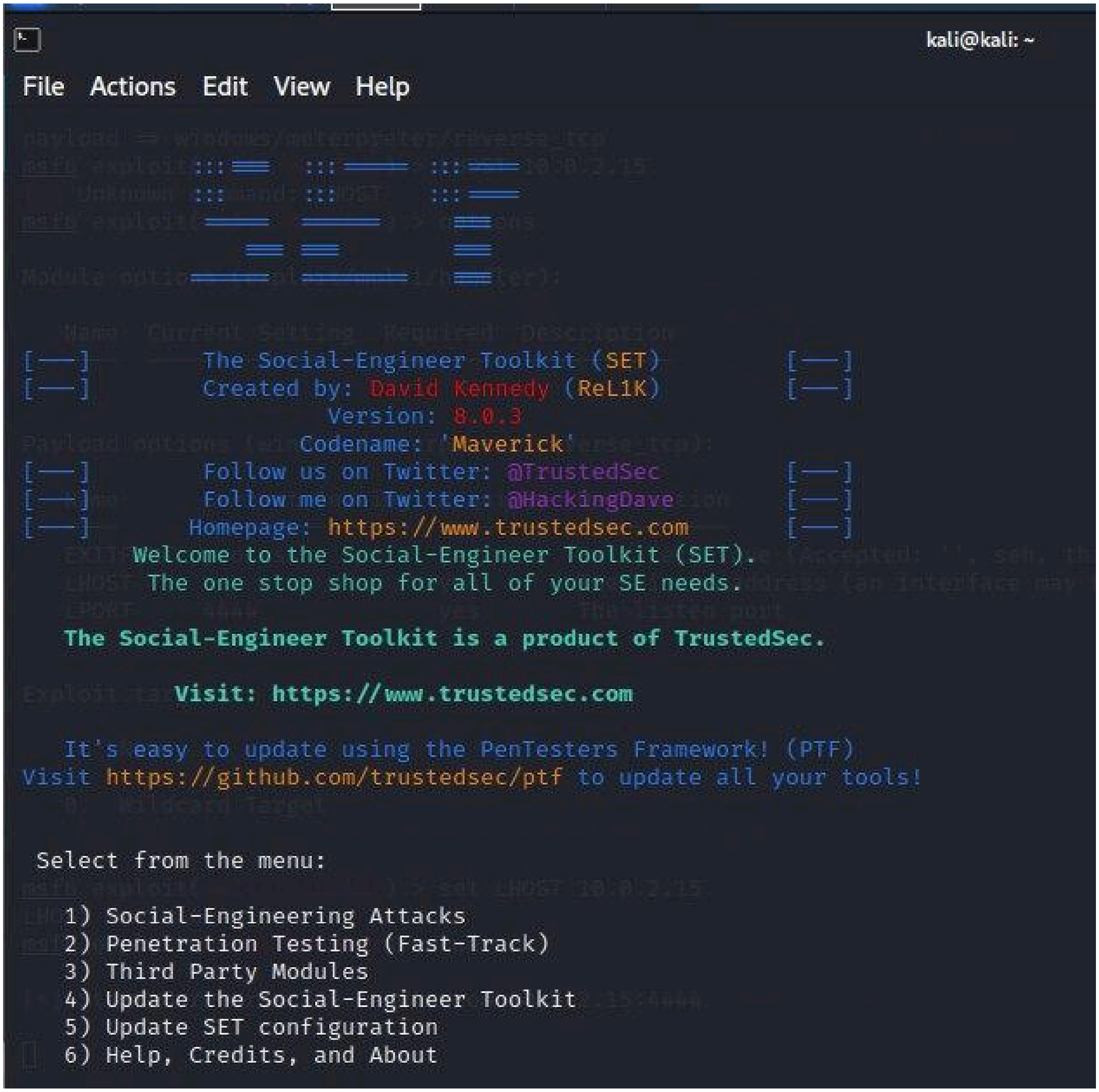
1) ETTERCAP



```
       =[ metaspl
+ -- --=[ 2212 ex
+ -- --=[ 615 pay
+ -- --=[ 9 evasi

Metasploit tip: A
set LHOST eth0

msf6 > exit

┌──(kali㉿kali)-[
└─$

┌──(kali㉿kali)-[
└─$ sudo ettercap
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

2) SOCIAL-ENGINEER TOOLKIT



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About
```

BLUE TEAM

Blue Team Configuration and Tools

Tools to Use:

1. **Windows Firewall**

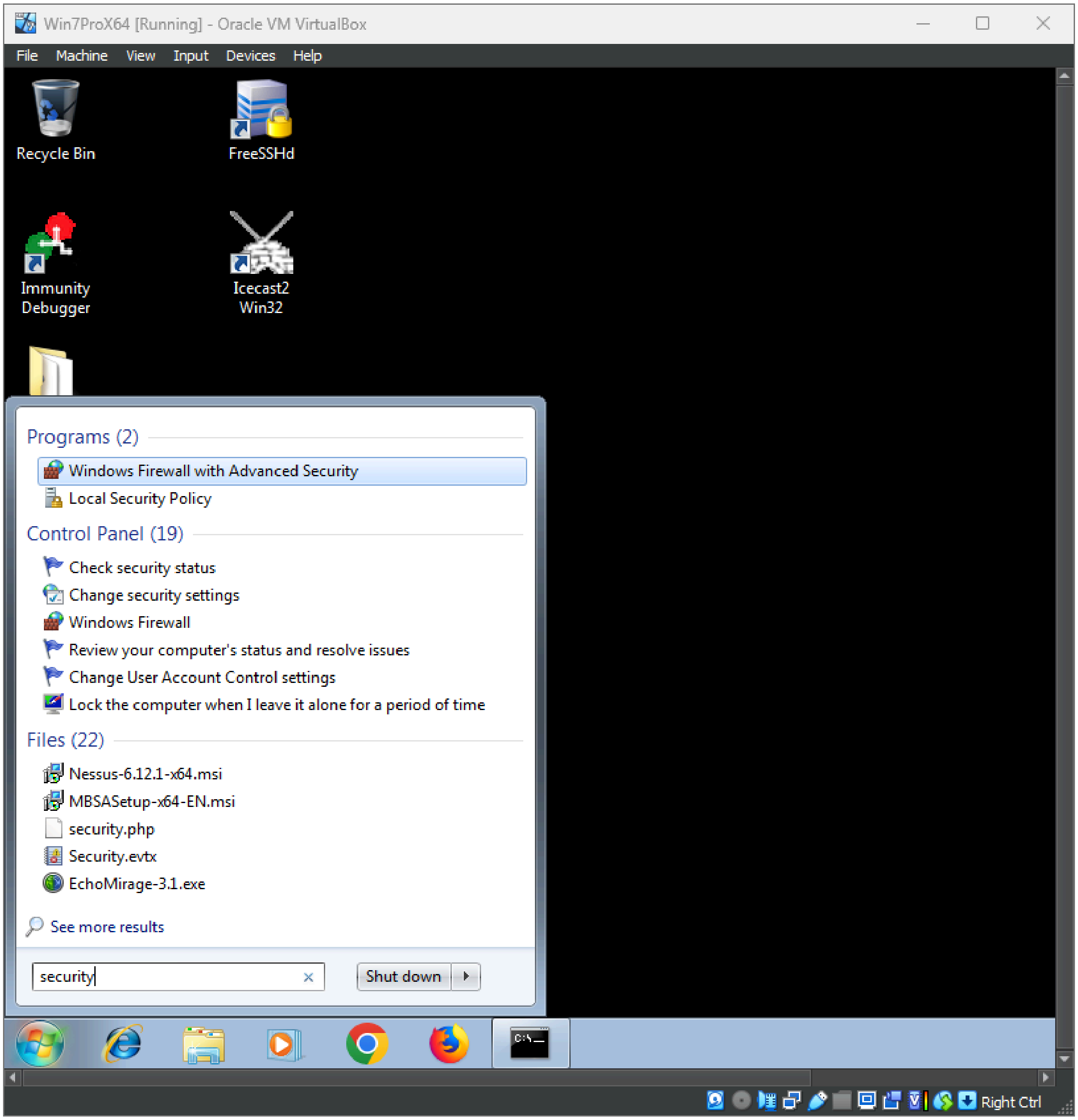
    - Ensure it is enabled to block unauthorized traffic.

    - Key feature:
        - Traffic Filtering: Inspects and blocks or allows incoming and outgoing traffic based on rules
        - Logging and Reporting: Records connection attempts, blocked activities, and suspicious traffic for analysis.
        - Stateful inspection: Monitors active connections and ensures only legitimate packets associated with an existing session are allowed.

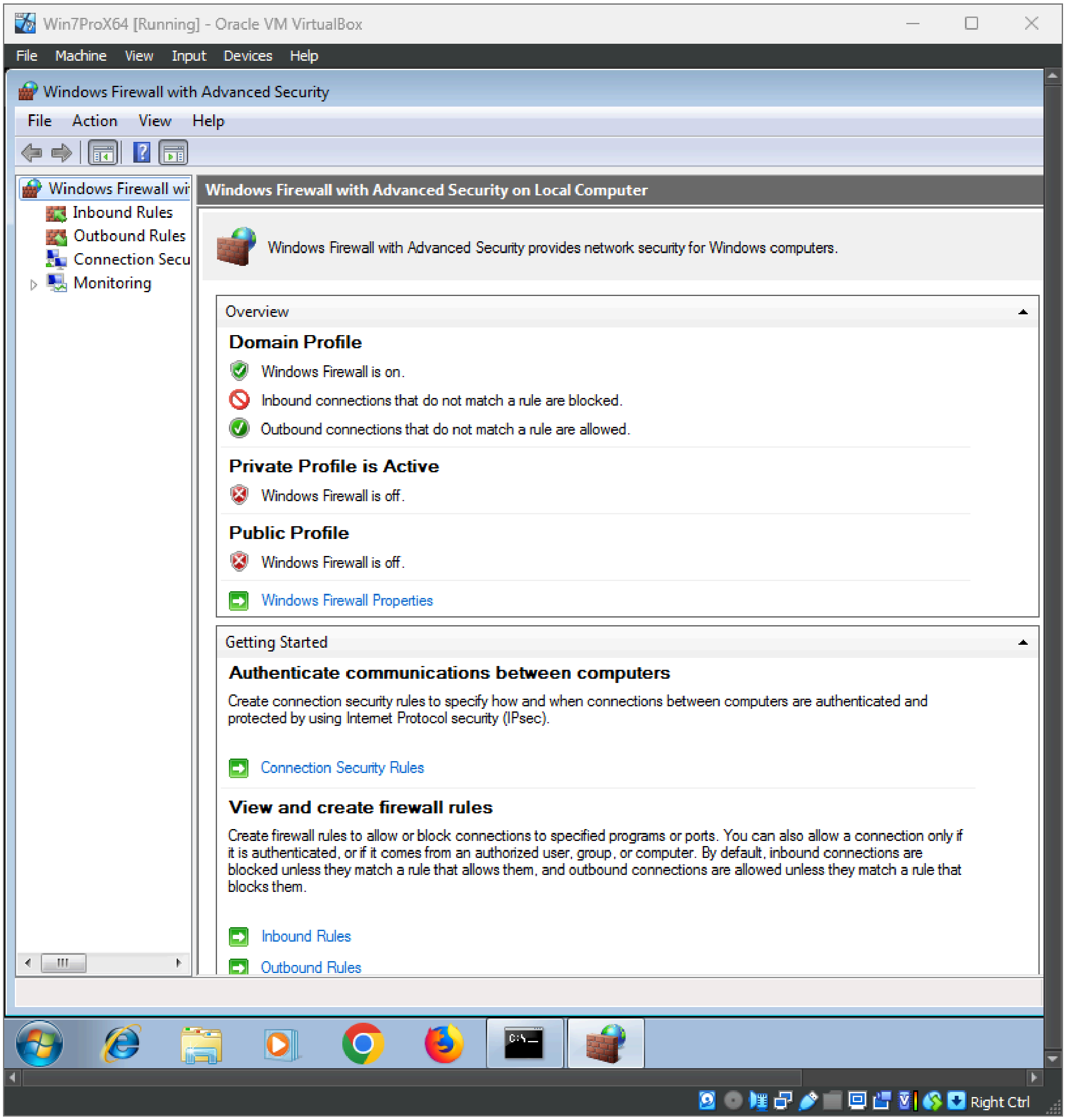
    - Strength:
        - Prevents unauthorized access by default.
        - Automatically blocks suspicious traffic.
        - Can protect individual devices (host-based firewalls) or entire networks (network firewalls).

    - Limitation:
        - Limited visibility into traffic content
        - Cannot detect internal threats
        - Rule misconfiguration

Step 1: In the Windows security window, click on **Windows Firewall and Advanced Security.**



Step 2: In the Firewall & Network Protection window, ensure all network profiles (**Domain, Private, Public**) show the firewall as "On."


Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall wi
Inbound Rules
Outbound Rules
Connection Secu
Monitoring
Right Ctrl

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows 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 Firewall is off.

Public Profile

✗ Windows Firewall is off.

Windows 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

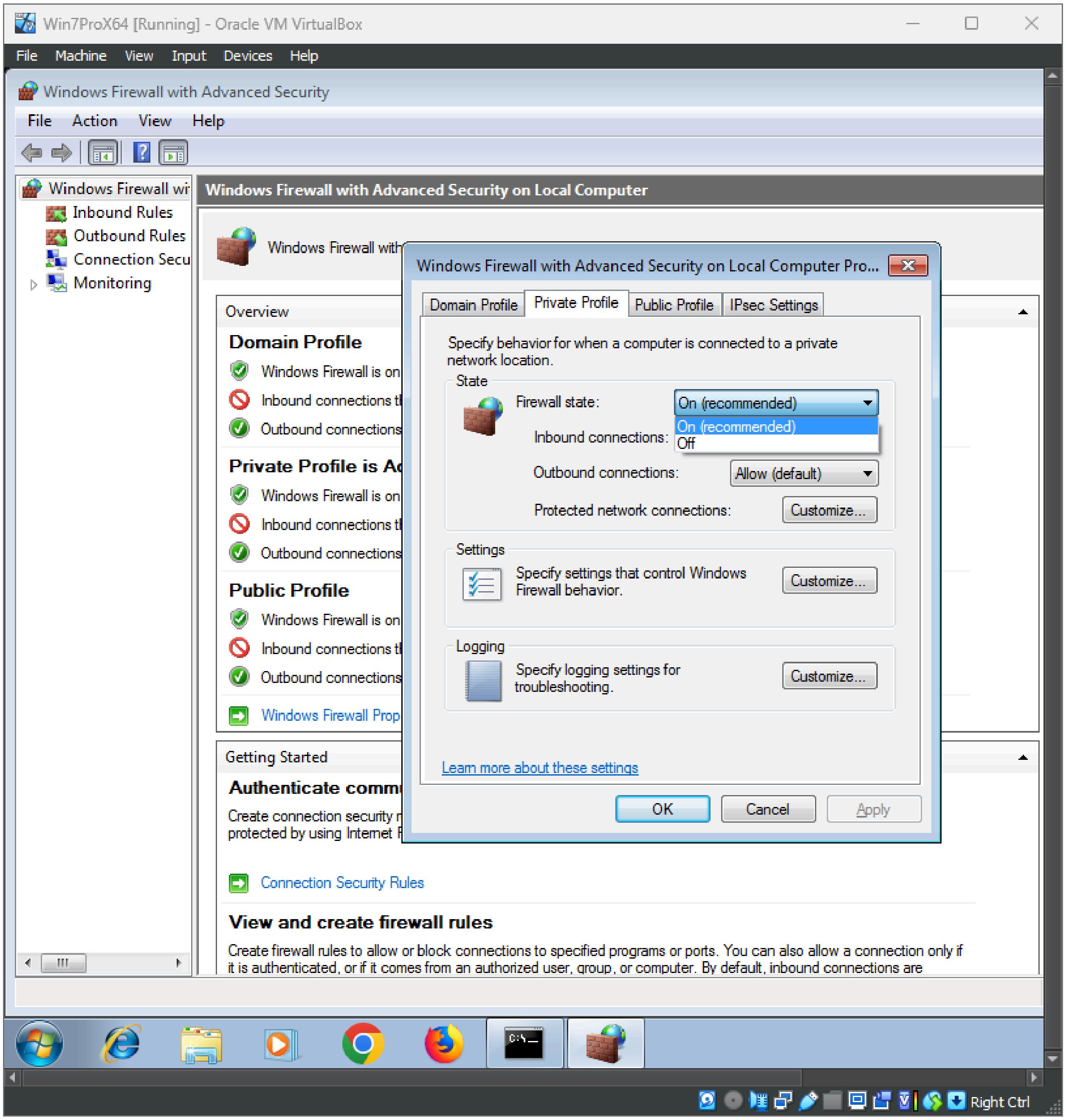
View and create firewall rules

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

Step 3: If the firewall is off, click on each profile (**Domain network**, **Private network**, **Public network**) and toggle the switch to **On**.



Windows Firewall with Advanced Security on Local Computer Pro...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a private network location.

State

Firewall state: On (recommended)

Inbound connections:

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

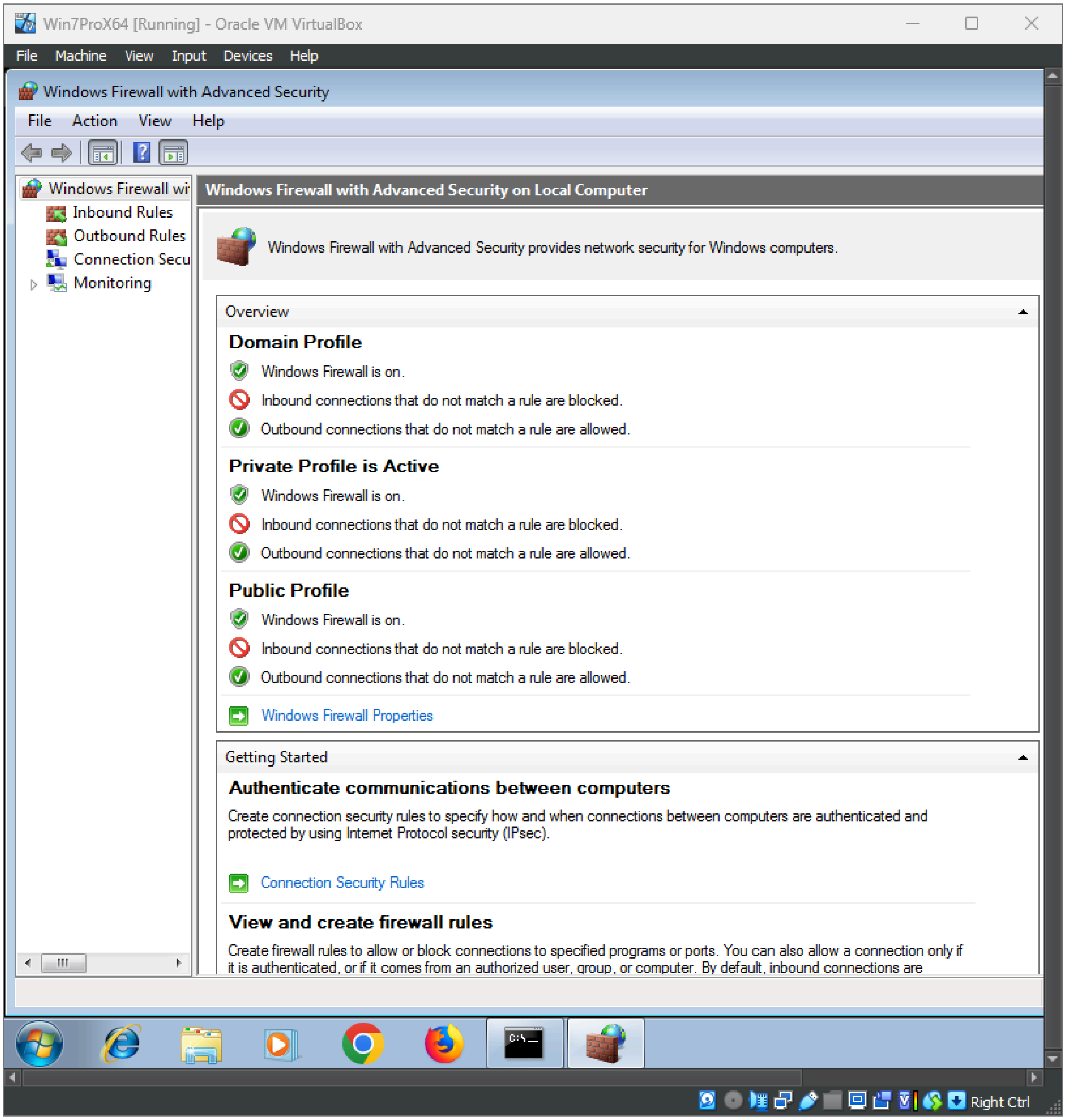
Specify logging settings for troubleshooting. Customize...

Learn more about these settings

OK Cancel Apply

Win7ProX64 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall wi
Inbound Rules
Outbound Rules
Connection Secu
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with
Overview
Domain Profile
Windows Firewall is on
Inbound connections tl
Outbound connections
Private Profile is Ac
Windows Firewall is on
Inbound connections tl
Outbound connections
Public Profile
Windows Firewall is on
Inbound connections tl
Outbound connections
Windows Firewall Prop
Getting Started
Authenticate comm
Create connection security r
protected by using Internet F
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
On (recommended)
Off
Right Ctrl

Step 4: Then, check back the firewall status to ensure each network profile shows the firewall as "On".


Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall wi
Inbound Rules
Outbound Rules
Connection Secu
Monitoring
Right Ctrl

Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows 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 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 Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows 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

2. Wireshark

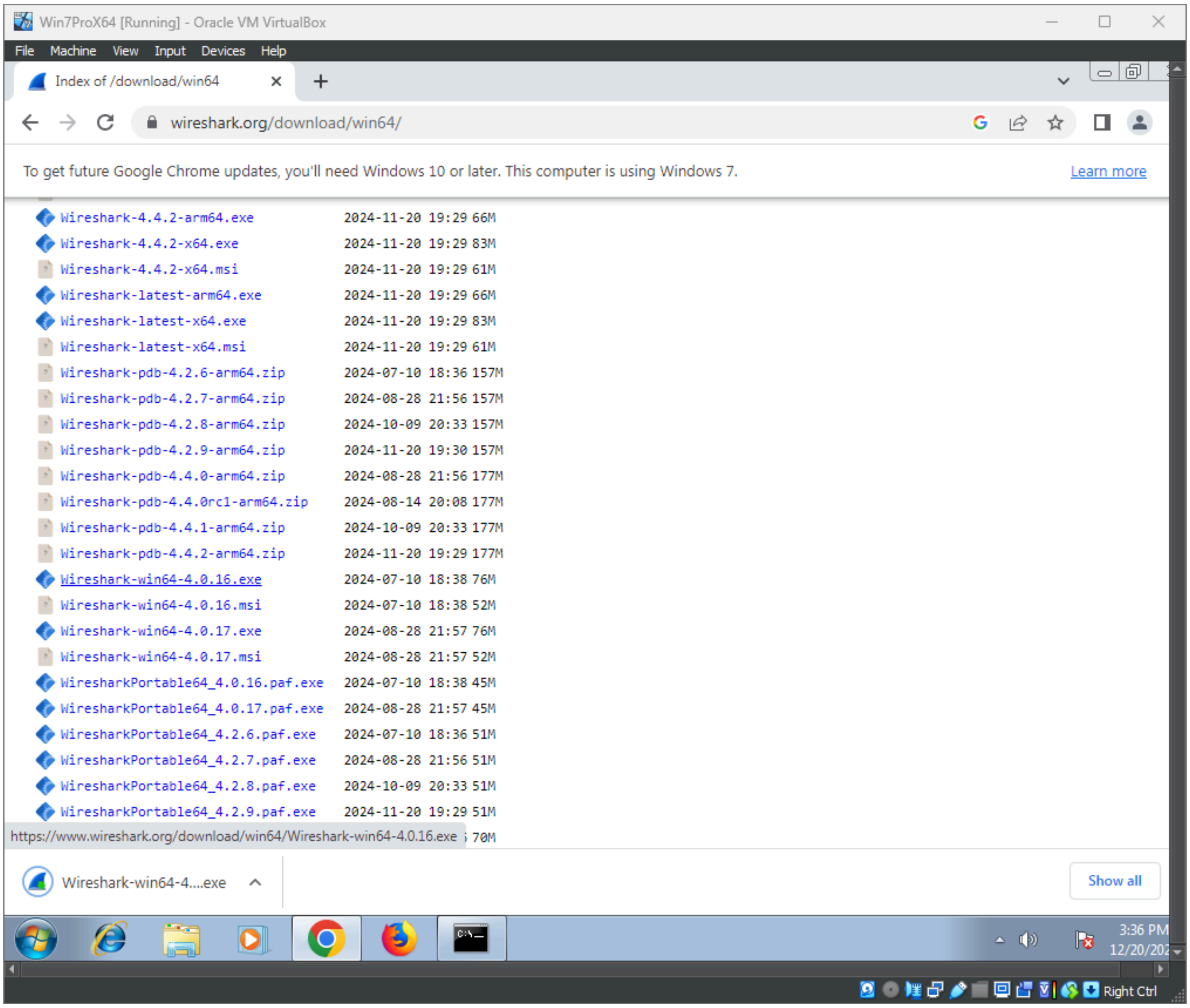
- ○ A network protocol analyzer for monitoring and identifying suspicious traffic.

- ○ Key Features:
  - Packet Capture: Captures network traffic in real-time or from saved files in various formats (e.g., .pcap).
  - Deep packet Inspection: Examines detailed contents of packets, including headers and payloads.
  - Protocol Support: Supports hundreds of protocols and can dissect their structure for analysis.

- ○ Strength:
  - Detailed visibility: Provides unmatched granularity into network activities, making it easier to identify anomalies.
  - Troubleshooting: Diagnoses network issues like slow connections, packet loss, and misconfigurations.
  - Free and open source: A powerful, cost-effective solution for network monitoring and analysis.

- ○ Limitation:
  - Passive monitoring: Wireshark is a passive tool; it does not actively block or prevent threats.
  - Limited to the monitoring point: Wireshark only captures traffic visible from its monitoring location.
  - Performance constraints: Capturing traffic on high-speed networks or large volumes of traffic can overwhelm Wireshark, causing packet loss.

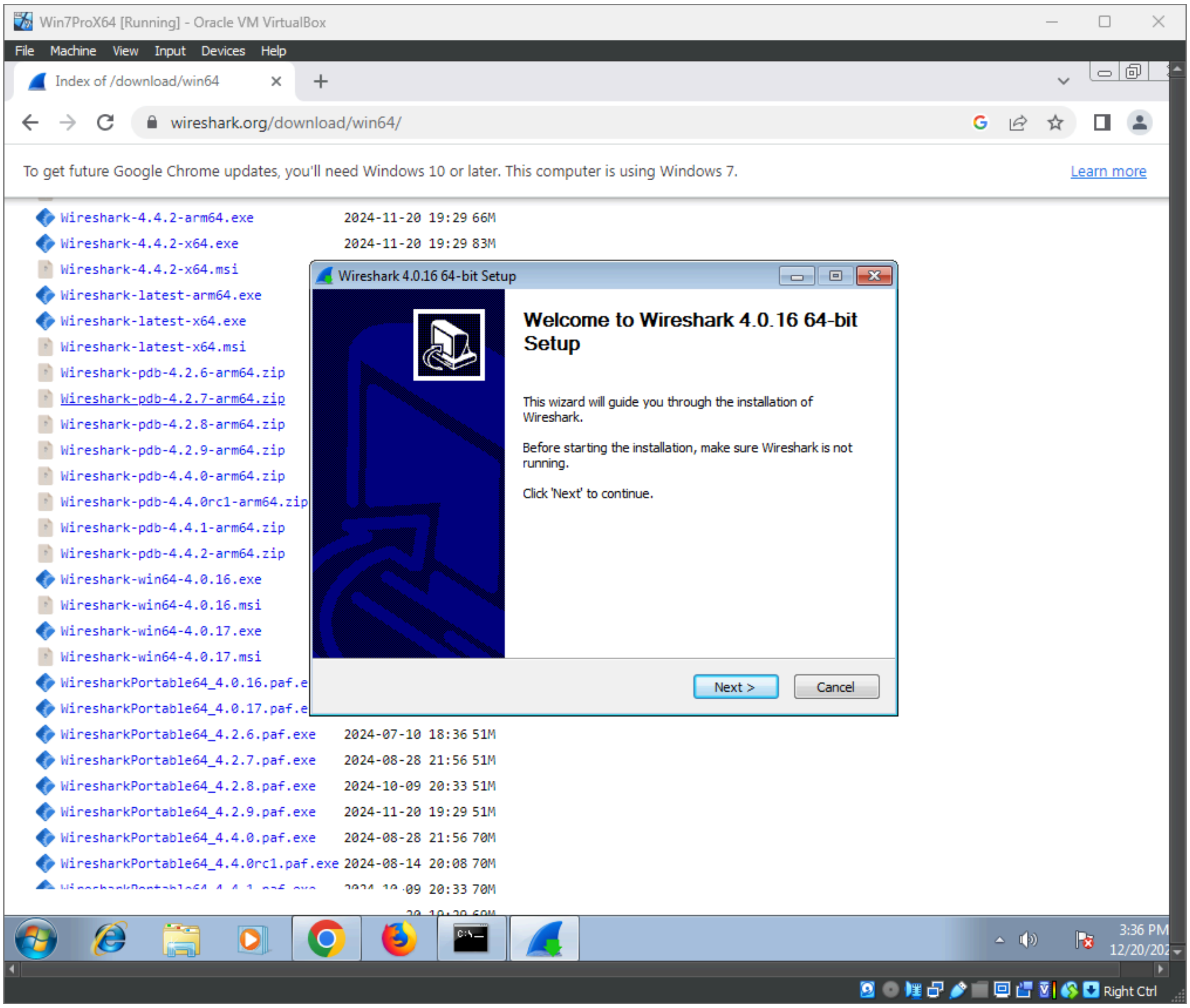
Step 1: Install Wireshark.



To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

```
Wireshark-4.4.2-arm64.exe          2024-11-20 19:29 66M
Wireshark-4.4.2-x64.exe            2024-11-20 19:29 83M
Wireshark-4.4.2-x64.msi            2024-11-20 19:29 61M
Wireshark-latest-arm64.exe         2024-11-20 19:29 66M
Wireshark-latest-x64.exe           2024-11-20 19:29 83M
Wireshark-latest-x64.msi           2024-11-20 19:29 61M
Wireshark-pdb-4.2.6-arm64.zip      2024-07-10 18:36 157M
Wireshark-pdb-4.2.7-arm64.zip      2024-08-28 21:56 157M
Wireshark-pdb-4.2.8-arm64.zip      2024-10-09 20:33 157M
Wireshark-pdb-4.2.9-arm64.zip      2024-11-20 19:30 157M
Wireshark-pdb-4.4.0-arm64.zip      2024-08-28 21:56 177M
Wireshark-pdb-4.4.0rc1-arm64.zip   2024-08-14 20:08 177M
Wireshark-pdb-4.4.1-arm64.zip      2024-10-09 20:33 177M
Wireshark-pdb-4.4.2-arm64.zip      2024-11-20 19:29 177M
Wireshark-win64-4.0.16.exe         2024-07-10 18:38 76M
Wireshark-win64-4.0.16.msi         2024-07-10 18:38 52M
Wireshark-win64-4.0.17.exe         2024-08-28 21:57 76M
Wireshark-win64-4.0.17.msi         2024-08-28 21:57 52M
WiresharkPortable64_4.0.16.paf.exe 2024-07-10 18:38 45M
WiresharkPortable64_4.0.17.paf.exe 2024-08-28 21:57 45M
WiresharkPortable64_4.2.6.paf.exe  2024-07-10 18:36 51M
WiresharkPortable64_4.2.7.paf.exe  2024-08-28 21:56 51M
WiresharkPortable64_4.2.8.paf.exe  2024-10-09 20:33 51M
WiresharkPortable64_4.2.9.paf.exe  2024-11-20 19:29 51M
https://www.wireshark.org/download/win64/Wireshark-win64-4.0.16.exe ; 70M
```

Step 2: Run the installer and follow the setup wizard.



Win7ProX64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /download/win64
wireshark.org/download/win64/
Learn more
3:36 PM
12/20/202
Right Ctrl

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

```
Wireshark-4.4.2-arm64.exe           2024-11-20 19:29 66M
Wireshark-4.4.2-x64.exe             2024-11-20 19:29 83M
Wireshark-4.4.2-x64.msi
Wireshark-latest-arm64.exe
Wireshark-latest-x64.exe
Wireshark-latest-x64.msi
Wireshark-pdb-4.2.6-arm64.zip
Wireshark-pdb-4.2.7-arm64.zip
Wireshark-pdb-4.2.8-arm64.zip
Wireshark-pdb-4.2.9-arm64.zip
Wireshark-pdb-4.4.0-arm64.zip
Wireshark-pdb-4.4.0rc1-arm64.zip
Wireshark-pdb-4.4.1-arm64.zip
Wireshark-pdb-4.4.2-arm64.zip
Wireshark-win64-4.0.16.exe
Wireshark-win64-4.0.16.msi
Wireshark-win64-4.0.17.exe
Wireshark-win64-4.0.17.msi
WiresharkPortable64_4.0.16.paf.e
WiresharkPortable64_4.0.17.paf.e
WiresharkPortable64_4.2.6.paf.exe   2024-07-10 18:36 51M
WiresharkPortable64_4.2.7.paf.exe   2024-08-28 21:56 51M
WiresharkPortable64_4.2.8.paf.exe   2024-10-09 20:33 51M
WiresharkPortable64_4.2.9.paf.exe   2024-11-20 19:29 51M
WiresharkPortable64_4.4.0.paf.exe   2024-08-28 21:56 70M
WiresharkPortable64_4.4.0rc1.paf.exe 2024-08-14 20:08 70M
WiresharkPortable64_4.4.1.paf.exe   2024-10-09 20:33 70M
```

Wireshark 4.0.16 64-bit Setup

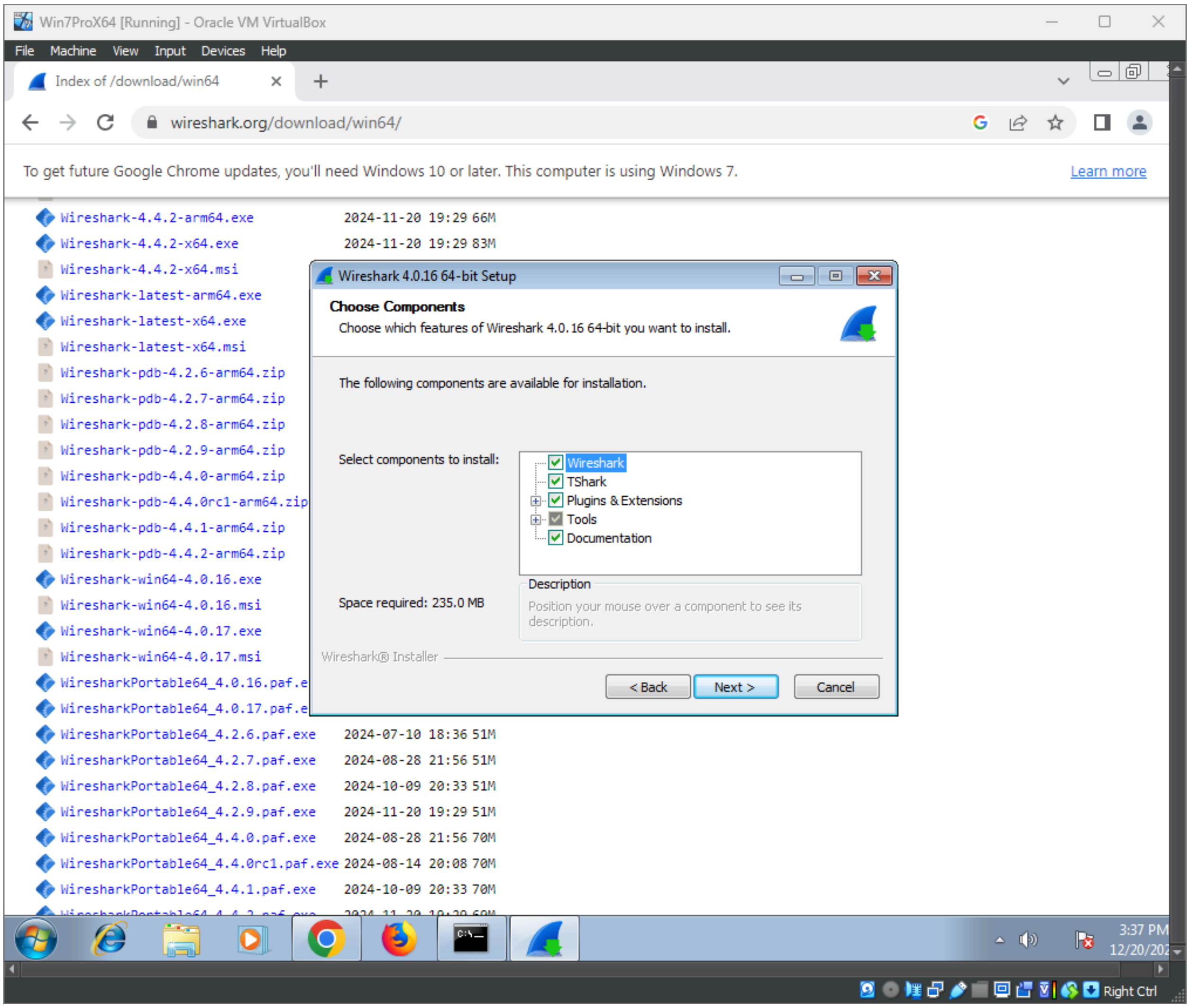
Welcome to Wireshark 4.0.16 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Step 3: Select component as needed.



Win7ProX64 [Running] - Oracle VM VirtualBox

Index of /download/win64

wireshark.org/download/win64/

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. Learn more

```
Wireshark-4.4.2-arm64.exe          2024-11-20 19:29 66M
Wireshark-4.4.2-x64.exe            2024-11-20 19:29 83M
Wireshark-4.4.2-x64.msi
Wireshark-latest-arm64.exe
Wireshark-latest-x64.exe
Wireshark-latest-x64.msi
Wireshark-pdb-4.2.6-arm64.zip
Wireshark-pdb-4.2.7-arm64.zip
Wireshark-pdb-4.2.8-arm64.zip
Wireshark-pdb-4.2.9-arm64.zip
Wireshark-pdb-4.4.0-arm64.zip
Wireshark-pdb-4.4.0rc1-arm64.zip
Wireshark-pdb-4.4.1-arm64.zip
Wireshark-pdb-4.4.2-arm64.zip
Wireshark-win64-4.0.16.exe
Wireshark-win64-4.0.16.msi
Wireshark-win64-4.0.17.exe
Wireshark-win64-4.0.17.msi
WiresharkPortable64_4.0.16.paf.e
WiresharkPortable64_4.0.17.paf.e
WiresharkPortable64_4.2.6.paf.exe    2024-07-10 18:36 51M
WiresharkPortable64_4.2.7.paf.exe    2024-08-28 21:56 51M
WiresharkPortable64_4.2.8.paf.exe    2024-10-09 20:33 51M
WiresharkPortable64_4.2.9.paf.exe    2024-11-20 19:29 51M
WiresharkPortable64_4.4.0.paf.exe    2024-08-28 21:56 70M
WiresharkPortable64_4.4.0rc1.paf.exe 2024-08-14 20:08 70M
WiresharkPortable64_4.4.1.paf.exe    2024-10-09 20:33 70M
```

Wireshark 4.0.16 64-bit Setup

Choose Components

Choose which features of Wireshark 4.0.16 64-bit you want to install.

The following components are available for installation.

Select components to install:

- ☑ Wireshark
- ☑ TShark
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ Documentation

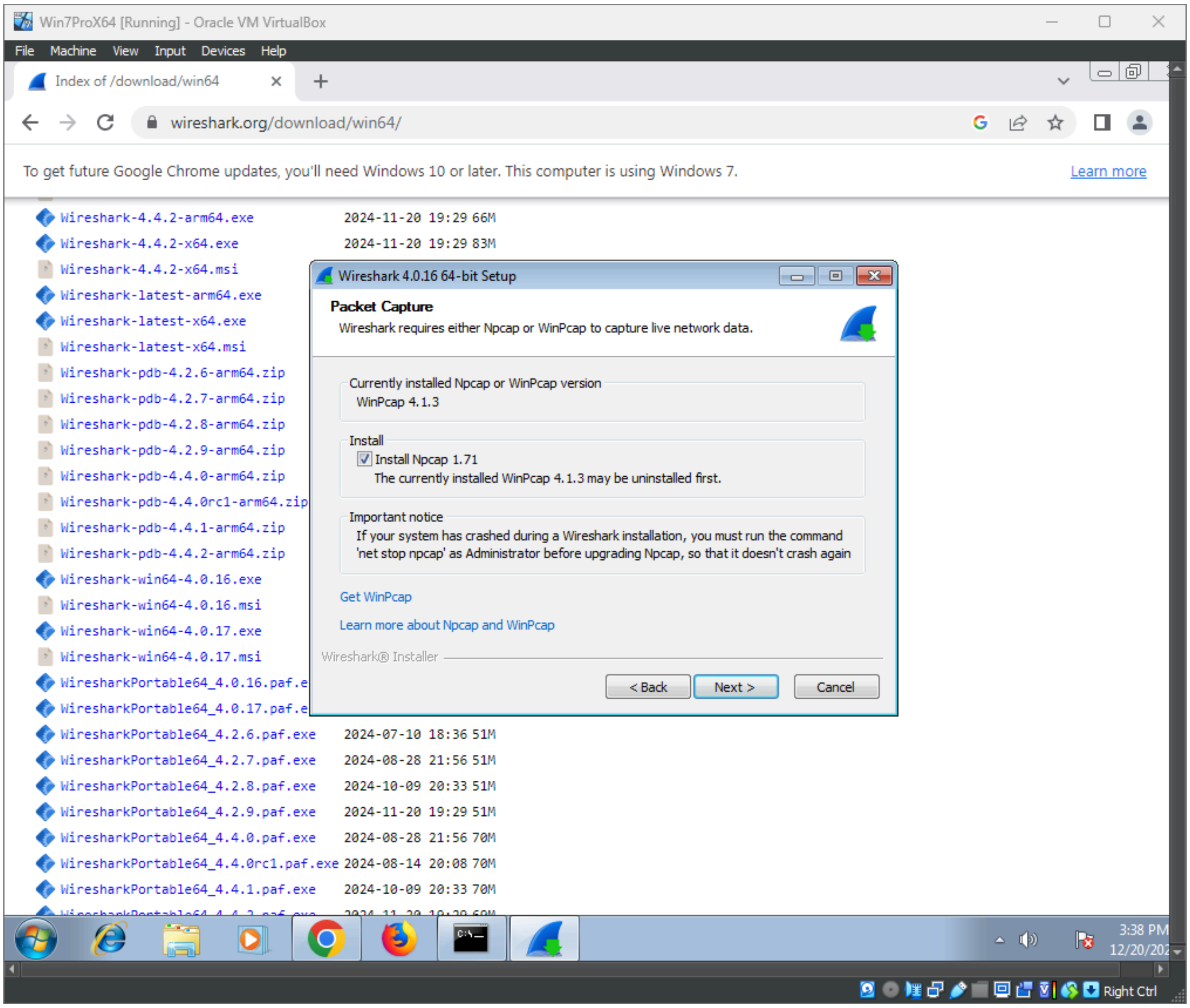
Space required: 235.0 MB

Description

Position your mouse over a component to see its description.

Wireshark® Installer

Step 4: Install **WinPcap** or **Npcap** if prompted (this is essential for capturing packets).



Win7ProX64 [Running] - Oracle VM VirtualBox

Index of /download/win64

wireshark.org/download/win64/

To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7. Learn more

```
Wireshark-4.4.2-arm64.exe          2024-11-20 19:29 66M
Wireshark-4.4.2-x64.exe            2024-11-20 19:29 83M
Wireshark-4.4.2-x64.msi
Wireshark-latest-arm64.exe
Wireshark-latest-x64.exe
Wireshark-latest-x64.msi
Wireshark-pdb-4.2.6-arm64.zip
Wireshark-pdb-4.2.7-arm64.zip
Wireshark-pdb-4.2.8-arm64.zip
Wireshark-pdb-4.2.9-arm64.zip
Wireshark-pdb-4.4.0-arm64.zip
Wireshark-pdb-4.4.0rc1-arm64.zip
Wireshark-pdb-4.4.1-arm64.zip
Wireshark-pdb-4.4.2-arm64.zip
Wireshark-win64-4.0.16.exe
Wireshark-win64-4.0.16.msi
Wireshark-win64-4.0.17.exe
Wireshark-win64-4.0.17.msi
WiresharkPortable64_4.0.16.paf.e
WiresharkPortable64_4.0.17.paf.e
WiresharkPortable64_4.2.6.paf.exe    2024-07-10 18:36 51M
WiresharkPortable64_4.2.7.paf.exe    2024-08-28 21:56 51M
WiresharkPortable64_4.2.8.paf.exe    2024-10-09 20:33 51M
WiresharkPortable64_4.2.9.paf.exe    2024-11-20 19:29 51M
WiresharkPortable64_4.4.0.paf.exe    2024-08-28 21:56 70M
WiresharkPortable64_4.4.0rc1.paf.exe 2024-08-14 20:08 70M
WiresharkPortable64_4.4.1.paf.exe    2024-10-09 20:33 70M
WiresharkPortable64_4.4.2.paf.exe    2024-11-20 19:29 69M
```

Wireshark 4.0.16 64-bit Setup

Packet Capture

Wireshark requires either Npcap or WinPcap to capture live network data.

Currently installed Npcap or WinPcap version

WinPcap 4.1.3

Install

☑ Install Npcap 1.71

The currently installed WinPcap 4.1.3 may be uninstalled first.

Important notice

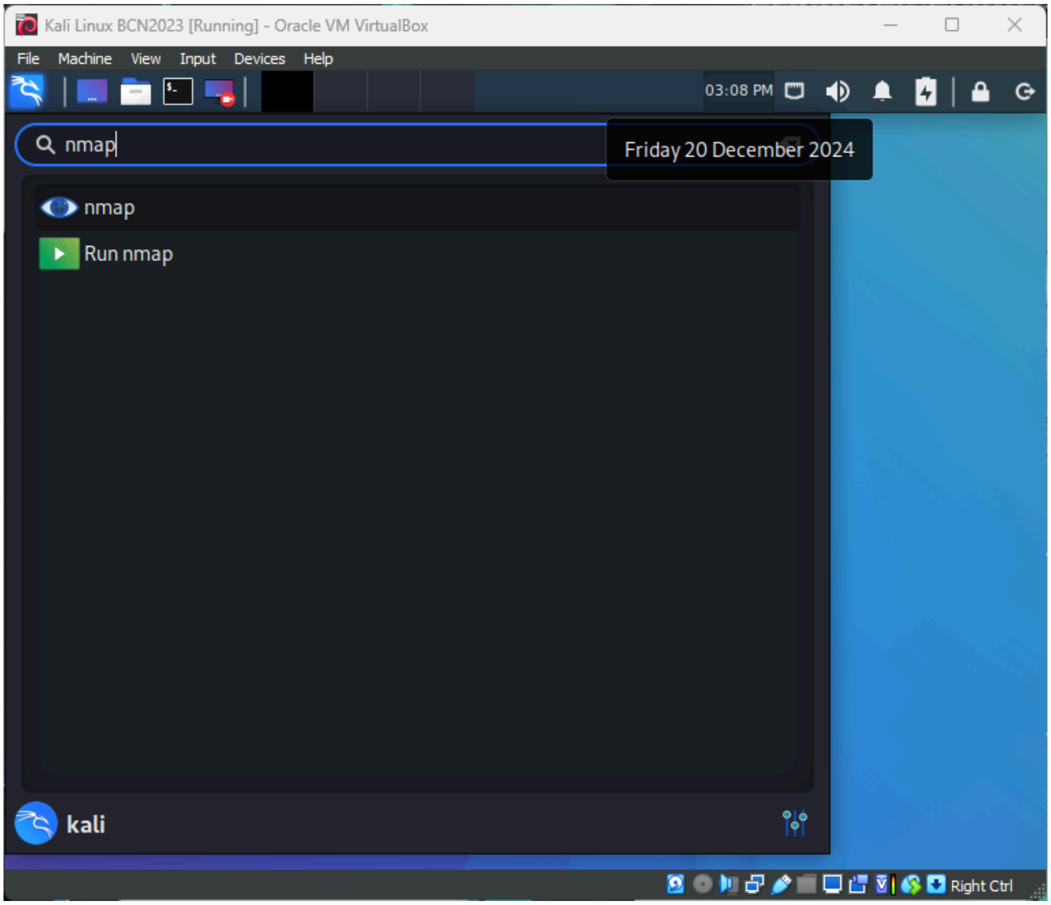
If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again

Get WinPcap

Learn more about Npcap and WinPcap

Wireshark® Installer

3. **Nmap**
   - An effective, open-source program for network exploration, vulnerability analysis, and security audits is called Nmap (Network Mapper). It offers thorough information about services, network structure, and any weaknesses. For Blue Teams to find system flaws that an attacker may take advantage of, Nmap is an essential tool.
   -



Key Features of Nmap

1. **Host Discovery**:
   - Detect active devices on a network and identify their IP addresses.
2. **Port Scanning**:
   - Identify open ports and the services running on those ports.
3. **Service and Version Detection**:
   - Determine the applications and versions running on open ports (e.g., Apache 2.4.41).
4. **Operating System Detection**:

    - Infer the operating system of a target device based on network behavior.
5. **Vulnerability Scanning**:
    - With scripts, Nmap can detect vulnerabilities in services or misconfigurations.
6. **Flexible Output**:
    - Export results in formats like plain text, XML, or interactive reports.

Nmap in Security Defense

1. Vulnerability Identification

Nmap helps identify open ports and services, which are potential entry points for attackers. For example:

- **Open Port 22 (SSH)**:
    - Ensure SSH is properly secured (e.g., key-based authentication).
- **Open Port 80/443 (Web Server)**:
    - Verify that web services are updated and not vulnerable to common attacks.

2. Attack Surface Reduction

- Close unnecessary ports or services discovered by Nmap scans.
- Configure firewalls to restrict access to critical services.

3. Monitoring Network Changes

- Regular Nmap scans can detect unauthorized devices or unexpected open ports, indicating a possible breach.

4. Testing Security Configurations

- Verify that firewall rules are working by scanning for blocked ports or services.
- Ensure intrusion detection/prevention systems (IDS/IPS) are flagging or blocking scans.

Strengths and Limitations

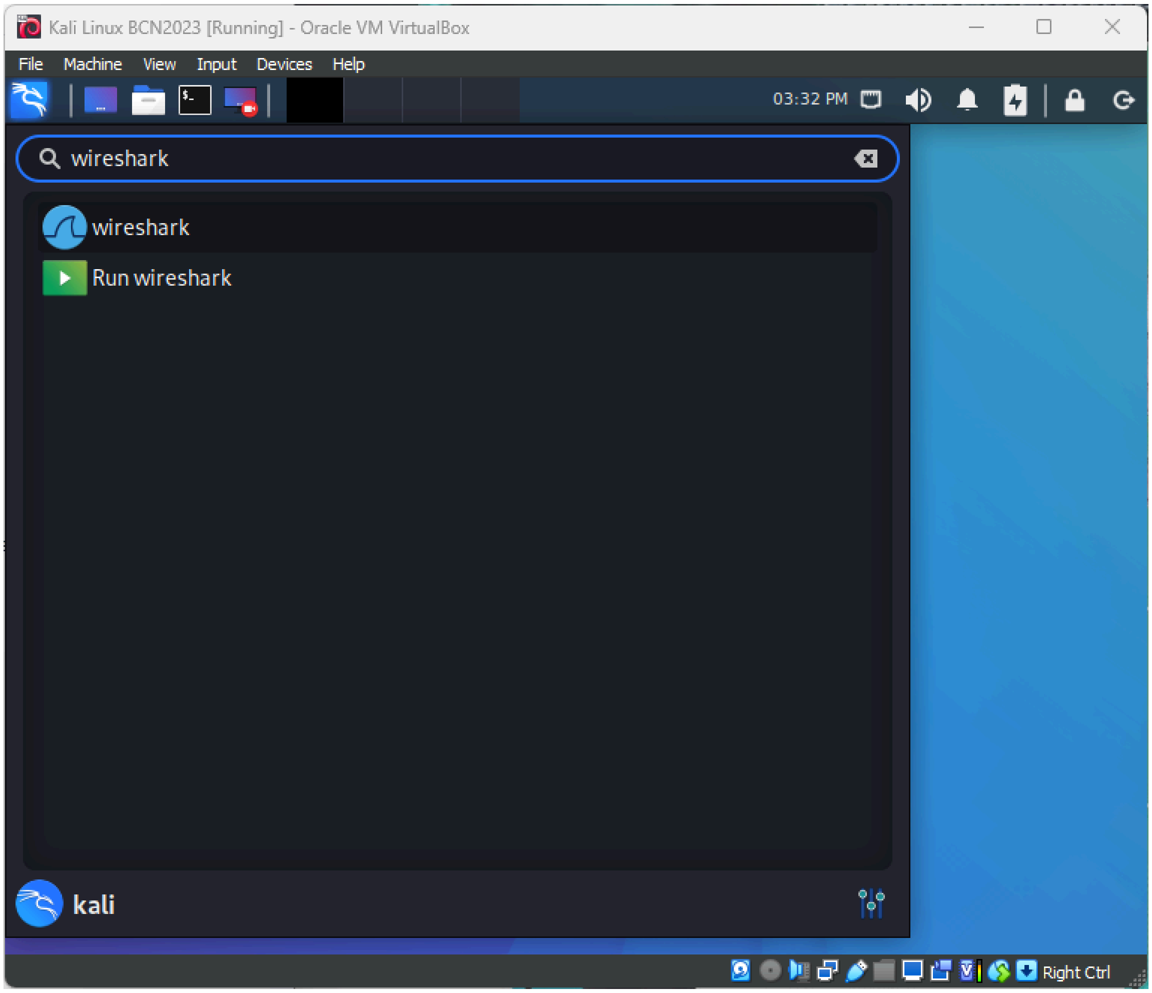
Strengths:

- Highly customizable and flexible.
- Supports large-scale scans with efficient algorithms.
- Active development ensures compatibility with new protocols.

Limitations:

- Requires administrative privileges for some scans.
- Stealth scans might still be logged by advanced IDS/IPS systems.
- Can generate network noise that might alert attackers.

4. **Wireshark**

- A network protocol analyzer called Wireshark is used to record and examine packets as they move across a network. Because it offers comprehensive insights into network activity, the Blue Team may use it to spot and look into any threats, irregularities, and suspicious activities.
- 

Key Features of Wireshark

1. **Packet Capturing**:
   - Wireshark captures data packets in real-time from a network interface (e.g., Ethernet, Wi-Fi).
   - These packets include details like source/destination IPs, protocols, ports, and payloads.
2. **Protocol Analysis**:
   - It supports hundreds of network protocols, including HTTP, TCP, UDP, DNS, FTP, and more.
   - Wireshark can decode these protocols to make the raw data readable and meaningful.
3. **Filtering and Search**:
   - Apply display filters to narrow down the captured data (e.g., `tcp.port == 80` to view HTTP traffic).
   - Enables quick identification of traffic patterns or specific data.
4. **Live and Offline Analysis**:
   - Analyze traffic in real-time or save it as a `.pcap` file for offline analysis.
5. **Visualization Tools**:
   - Graphical tools show traffic flow, conversations between hosts, or protocol hierarchy for easy interpretation.

Wireshark in Security Defense

Detecting Threats

- **Malware Communication**:
  - Look for unusual traffic to known malicious domains or IPs.
- **Port Scans**:
  - Repeated connection attempts to multiple ports from a single source could indicate scanning activity.
- **Data Exfiltration**:
  - Large outbound data flows to unknown servers might indicate sensitive data theft.

Blue Team Strategy

- **Integrate with IDS**:
  - Use Wireshark alongside Intrusion Detection Systems (like Snort) to verify alerts.
- **Incident Response**:
  - After an attack, Wireshark can help trace back to the source of the breach.
- **Compliance Checks**:
  - Validate that sensitive data is encrypted (e.g., ensuring HTTPS instead of HTTP).

Strengths and Limitations

Strengths:

- Intuitive graphical interface for both novice and expert users.
- Supports extensive protocol analysis.
- Free and open-source.

Limitations:

- High learning curve for advanced analysis.
- Can generate large volumes of data on busy networks, making analysis time-consuming.
- Requires administrative privileges to capture traffic on some systems

Activities and Steps:

1. Enable Firewall:
   - Turn on the firewall in Windows/Linux systems to block unauthorized access and suspicious connections.
   - Customize rules to deny traffic from Red Team's IP addresses.
2. Monitor Network Traffic:
   - Use Wireshark to capture and analyze network traffic.
   - Detect abnormal patterns like phishing attempts, suspicious packet transfers, or ARP spoofing.
3. Vulnerability Scanning with Nmap:
   - Regularly scan the network for open ports and exposed services using Nmap.
   - Example: Identify and close unused ports to reduce attack surface.
4. Password Policies:
   - Enforce strong password requirements, such as:
     - Minimum of 12 characters.
     - Combination of uppercase, lowercase, numbers, and symbols.
     - Regular password updates.

Network Configuration:

- Virtual Machines: Windows and Linux with defense tools.
- IP Address: `10.0.2.10` (Example).
- Network Mode: NAT or Host-Only for isolated network communication.

Overview of Team Responsibilities

- Red Team:
    - Focus on offensive techniques like phishing, exploiting vulnerabilities, and password cracking.
    - Simulate real-world attack scenarios to test Blue Team’s defenses.
- Blue Team:
    - Implement defensive strategies such as monitoring, patch management, and enforcing security policies.
    - Detect, block, and respond to simulated Red Team attacks effectively.

BLUE TEAM SETUP COMPUTER AND NETWORK SERVICES

We use Kali Linux and Windows 10 As our attacker and Victims.Connect The computer into the same network services.