

**INT 301**

**OPEN-SOURCE TECHNOLOGIES**

# CA-3

**SECTION: KM016**

Student Details:

|  |  |  |
| --- | --- | --- |
| **Roll no.** | **Name** | **Registration no.** |
| **RKE048B67** | **Shailesh Singh Yadav** | **11918833** |

# Submitted To: Rajeshwar Sharma

Lovely Professional University

(Jalandhar, Punjab, India)



## TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.NO** | **TITLE** | **PAGE NO.** |
| 1 | Introduction and Network Device Security | 3-7 |
| 2 | Physical Security | 8-11 |
| 4 | GitHub Link | 12 |

3. As a network administrator, briefly what techniques, tools, and methodologies would follow to perform testing on the following (use any open-source software): --

a) Network devices security

b) Physical security

a) As a Network administrator, when we perform testing for Network Devices Security, We use **Wireshark** Application Which is a Gui based Application.

Wireshark is a packet analyser for networks. A network packet analyser displays captured packet data as precisely as possible.

Consider a network packet analyser to be a measuring device for examining what's going on inside a network cable, similar to how an electrician uses a voltmeter to examine what's going on inside an electric cable (but at a higher level, of course).

Previously, such tools were either prohibitively expensive, proprietary, or both. That has changed with the introduction of Wireshark. Wireshark is a free, open-source packet analyser that is one of the best available today.

**Here are some of the reasons why people use Wireshark:**

It is used by network administrators to troubleshoot network issues.

It is used by network security engineers to investigate security issues.

It is used by QA engineers to test network applications.

It is used by developers to debug protocol implementations.

It is used to learn the internals of network protocols.

Wireshark can also be useful in a variety of other situations.

**Specifications**

Some of the many features offered by Wireshark include:

UNIX and Windows platforms are supported.

Live packet data from a network interface can be captured.

Open files containing packet data captured by tcpdump/WinDump, Wireshark, and a variety of other packet capture programmes.

Text files containing hex dumps of packet data can be used to import packets.

Show detailed protocol information in packets.

Save any captured packet data.

Some or all packets can be exported in a variety of capture file formats.

Filter packets according to a variety of criteria.

Search for packets based on a variety of criteria.

Filters are used to colourize the packet display.

Make several statistics.

... and so much more!

**Live capture from a variety of network media**

Wireshark can capture network traffic from a variety of network media, including Ethernet, Wireless LAN, Bluetooth, USB, and others. Several factors, including your hardware and operating system, may limit the specific media types supported.

**Import files from a variety of capture programmes.**

Wireshark is capable of opening packet captures from a wide range of capture programmes

**Export files to a variety of other capture programmes**

Wireshark can save captured packets in a variety of formats, including those supported by other capture software.

**There are numerous protocol dissectors**.

Many protocols have protocol dissectors (or decoders, as they are known in other products): see Appendix C, Protocols and Protocol Fields.

**Free and Open-Source Software**

Wireshark is a free and open-source software project licenced under the GNU General Public License (GPL). You can use Wireshark on as many computers as you want without worrying about licence keys or fees. Furthermore, all source code is available under the GPL. As a result, it is very simple for people to add new protocols to Wireshark, either as plugins or built into the source code, and they frequently do!

**Main Page of Wireshark**

Graphical user interface, text, application, email

Description automatically generated

When we click on Wi-Fi Option

Graphical user interface, text, application, email

Description automatically generated

**Colour Code for Wireshark**

**Graphical user interface, text, application, email

Description automatically generated**

### **How to Filter and Inspect Packets in Wireshark**

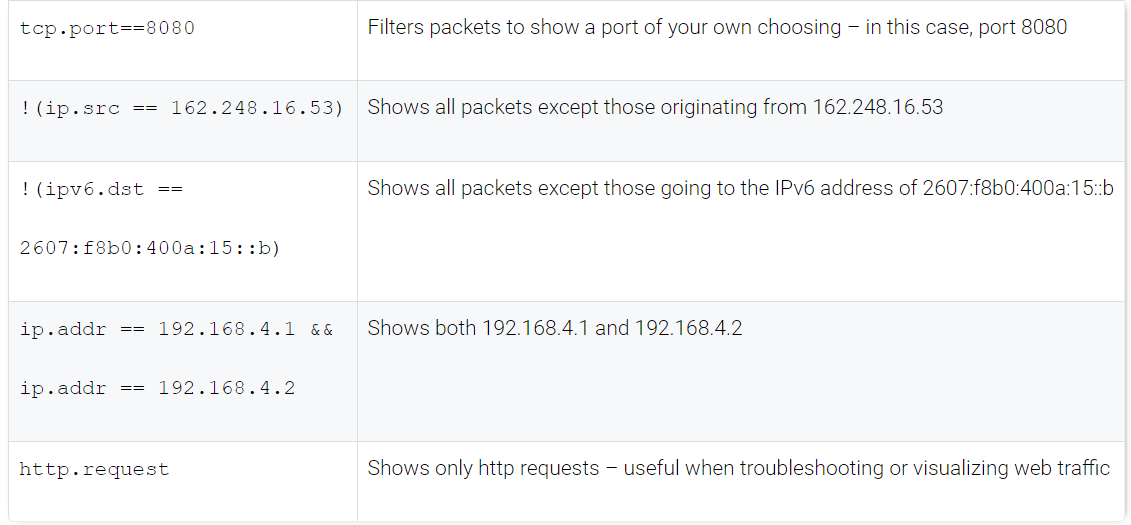
You can apply Wireshark filters in two ways:

* 1. In the Display Filter window, at the top of the screen
  2. By highlighting a packet (or a portion of a packet) and right-clicking on the packet

Wireshark filters use key phrases, such as the following:

A picture containing graphical user interface

Description automatically generated



**b) Physical Security**

Why is Physical Security needed?

* Authentication
  + Create access lists and identification mechanisms to allow approved persons through barriers.
* Authorization
  + Create barriers around a resource so that access can be controlled through defined entry and exit points.
* Accounting
  + Keep a record of when entry/exit points are used and detect security breaches.

**Tools, Technique and Methodology by which we achieved Physical Security**

* Site layout
  + Zone-based design to accommodate traffic flows and surveillance.
  + Signage
  + Industrial camouflage
* Barricades and entry/exit points
  + Bollards
* Fencing
* Lighting
  + Make staff feel secure.
  + Assist surveillance.

Gateways and Locks

* Lock types
  + Physical (conventional/deadbolt)
  + Electronic
    - Cipher/combination
    - Magnetic swipe card
    - Smart card/proximity reader
  + Biometric
* Access control vestibules/mantraps and turnstiles
* Cable locks

Physical Attacks against Smart Cards and USB

* Smart card attacks
  + Cloning
  + Skimming
  + Card types and vulnerability level
* Malicious USB/juice-jacking
  + USB data blocker

Alarm and Sensor System

* Circuit
  + Open or closed.
  + Detect intrusion through a barrier.
* Motion detection
  + Radar or infrared
  + Detect intrusion in a space.
* Noise detection
* Proximity readers
* Duress
  + Fixed or mobile

Security Guard and Camera

* Security guards
  + Police entry points
  + Operate surveillance mechanisms.
  + Respond to alarms.
* Remote surveillance and monitoring
  + Video/CCTV
  + Motion recognition
  + Object detection
  + Robot sentries
  + Drones/UAV

Reception Personnel and ID Badges

* Challenge policy
* Reception personnel and visitor logs
  + Sign-in/sign-out
  + Visitor information
* Two-person integrity/control
* ID badges

Secure Areas

* Server rooms and data centers
* Lockable cabinets
* Colocation cages
* Air gaps and demilitarized zones
* Safes
* Vaults

Protected Distributed and Faraday Cages

* Protected cable distribution/protected distribution system (PDS)
  + Prevent eavesdropping.
  + Prevent/delay cable cutting DoS.
* Faraday cage
  + Transient Electromagnetic Pulse Emanation Standard (TEMPEST)

Heating, Ventilation and Air Conditioning

* Cooling/warming, humidity, dust control
* Optimum temperature and humidity levels
  + Moisture detection sensors
  + Temperature detection sensors
* HVAC sizing
  + Equipment wattage
  + British Thermal Units (BTU)/hour
* Air flow
* Positive air pressure to remove contaminants.

Hot and Cold Aisles

* Optimize air flow.
* Place servers back-to-back
* Hot aisle/cold aisle
* Do not allow contamination of cooled air by warmed air.

Fire Detection and Suppression

* Fire safety
  + Fire exits and evacuation procedures.
  + Fire-resistant building design
  + Smoke/flame detectors/alarms
* Personal fire extinguishers
  + Class C for use around electrical hazard
* Sprinklers
  + Dry pipe
  + Pre-action
  + Halon
  + Clean Agent

Secure Data Destruction

* Media sanitization/remnant removal
* Physical destruction
  + Burning/incineration
  + Shredding/pulping
  + Pulverizing
  + Degaussing
* Use of third parties and certificates of destruction

Data Sanitization Tools

* Secure disposal of electronic data remnants
* Overwriting/disk wiping
  + Zero filling
  + Multiple passes
* Secure Erase (SE)
  + Hard disk drives (HDD)
  + Solid state drives (SSD)/flash media
* Instant Secure Erase (ISE)/crypto erase
  + Self-encrypting drives (SED)
  + Delete media encryption key.