Cryptography & Network Security

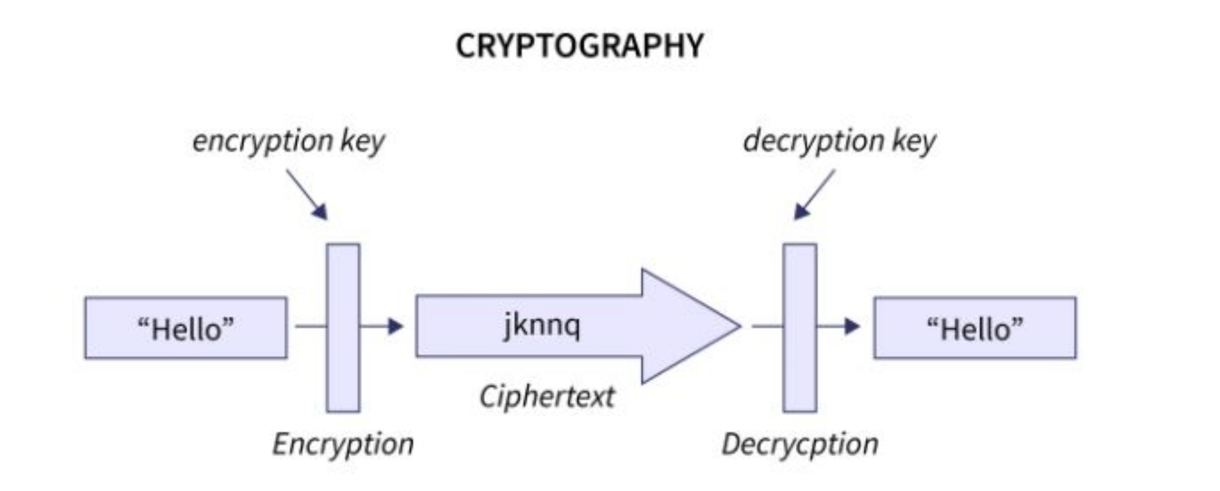
Jaspreet Singh

Project Engineer
E-Security Team
CDAC, Hyderabad

Introduction

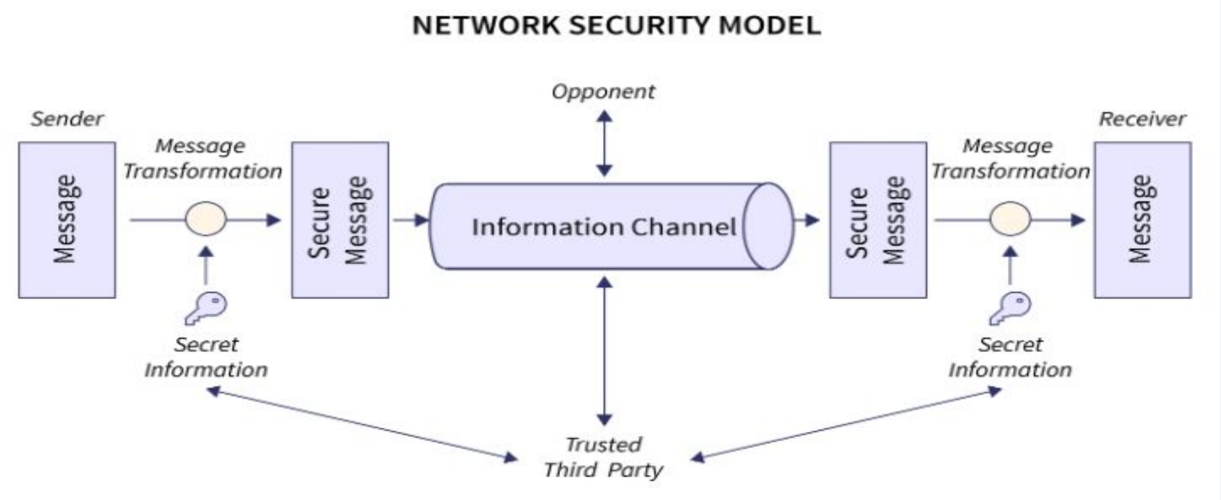
Cryptography

Cryptography generally deals with the study and practice of techniques for ensuring secure communication between two parties in the presence of a third party called adversaries.



Network Security

Network Security generally refers to action taken by an enterprise or organization to protect and secure its computer network and data. The main aim is to ensure the confidentiality and accessibility of the network and data.



Overview

- ➔ Networking devices -Router, Switch, Bridge
- ➔ Protocol Header Analysis using Wireshark [Lab]
- ➔ Introduction to Security Engineering & Network Security:
  - ❖ Security Services:
    - Authentication
    - Access Control,
    - Data Confidentiality.
    - Data Integrity
    - Non-Repudiation
    - Availability.

- ➔ Security Attacks - Active & Passive.
- ➔ Denial of Service (DoS) Attacks & Distributed Denial of Service Attacks (DDoS).
- ➔ Introduction to Vulnerability, Threat, Attack, Bug, Exploit.

Networking Devices

Key Features:

- ❑ Routing: *Forward data packets based on IP destination addresses*

- ❑ Forwarding: *Actively move data between networks, ensuring seamless communication*.

- ❑ Traffic Management: *Prioritize and manage data traffic, preventing congestion and optimizing network performance*.

- ❑ IP Addressing: Assign and manage IP addresses, facilitating communication between devices.

ROUTER

Networking Devices

Key Features:

- ❑ MAC Address Forwarding: *Forward data packets based on MAC destination addresses*
- ❑ Broadcast Domain Isolation: *Create individual broadcast domains for each port.*
- ❑ VLAN Segmentation: *Enable logical segmentation within a switch*.
- ❑ Full-Duplex Communication: Allowing simultaneous data transmission and reception.

SWITCH

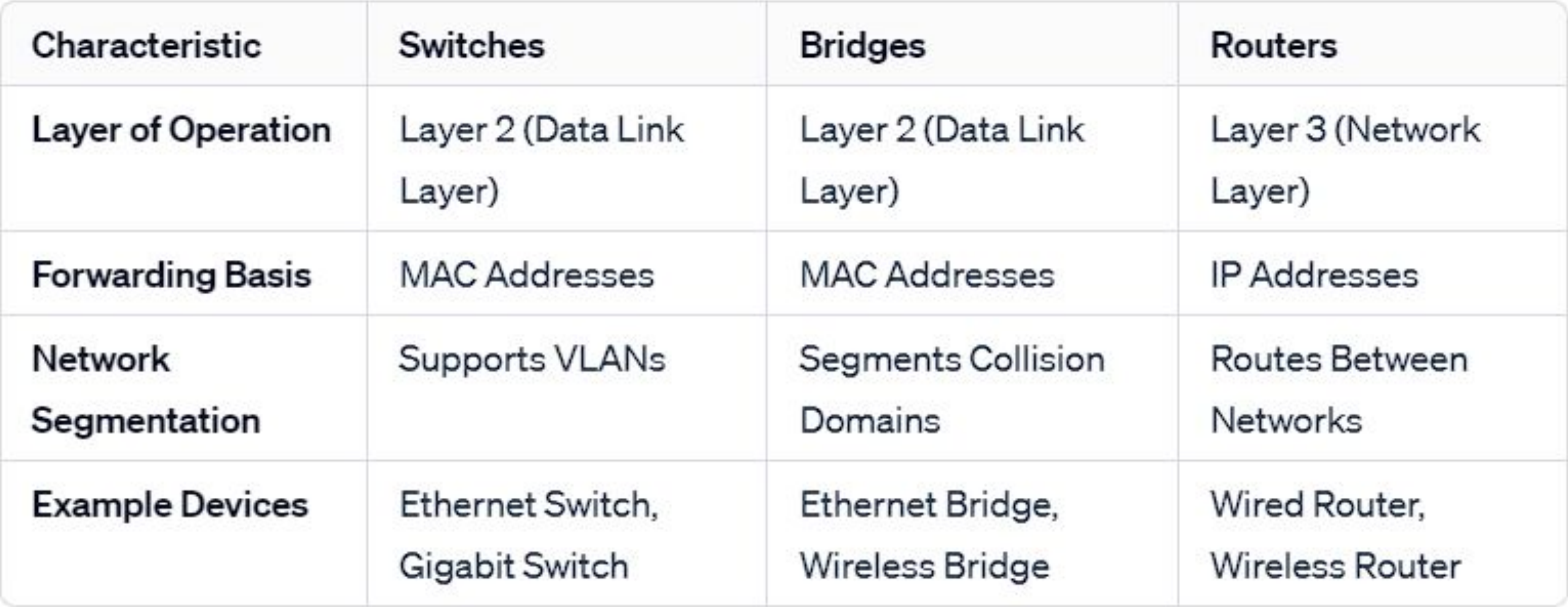
Networking Devices

Key Features:

- ❑ Transparent Filtering: *Bridges filter and forward data frames based on MAC addresses.*
- ❑ Segmenting Collision Domains: *Bridges segment network segments into collision domains.*
- ❑ Learning and Building MAC Address Tables: *Bridges dynamically learn the MAC addresses of connected devices and build MAC address tables.*
- ❑ Filtering Broadcast Traffic: Bridges filter and control the propagation of broadcast traffic.

BRIDGE

Networking Devices



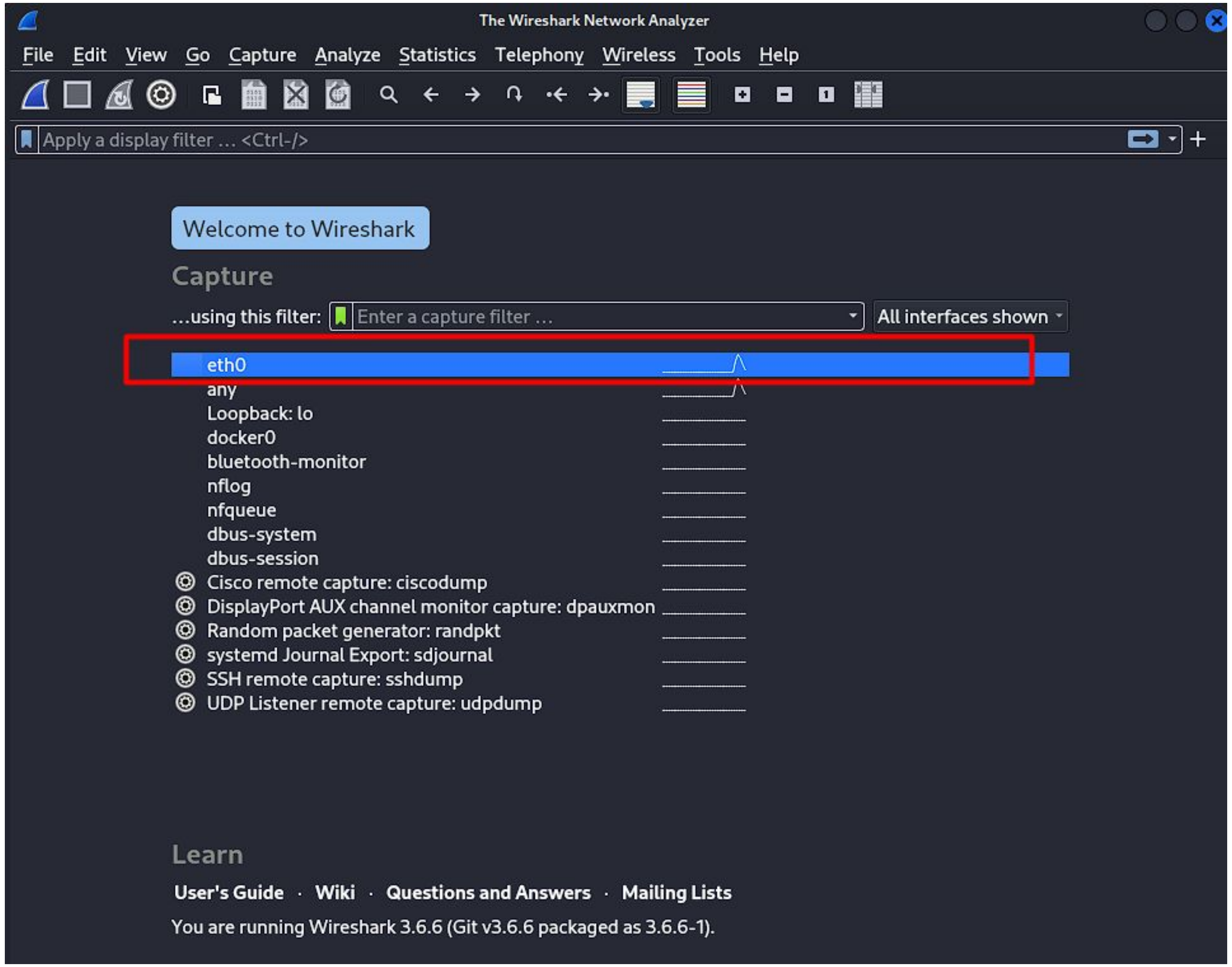
Characteristic	Switches	Bridges	Routers
Layer of Operation	Layer 2 (Data Link Layer)	Layer 2 (Data Link Layer)	Layer 3 (Network Layer)
Forwarding Basis	MAC Addresses	MAC Addresses	IP Addresses
Network Segmentation	Supports VLANs	Segments Collision Domains	Routes Between Networks
Example Devices	Ethernet Switch, Gigabit Switch	Ethernet Bridge, Wireless Bridge	Wired Router, Wireless Router

Protocol Header Analysis - Wireshark

Analyzing protocol headers using Wireshark involves capturing and inspecting the headers of packets transmitted over a network.

How?

- Select Interface



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown

eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

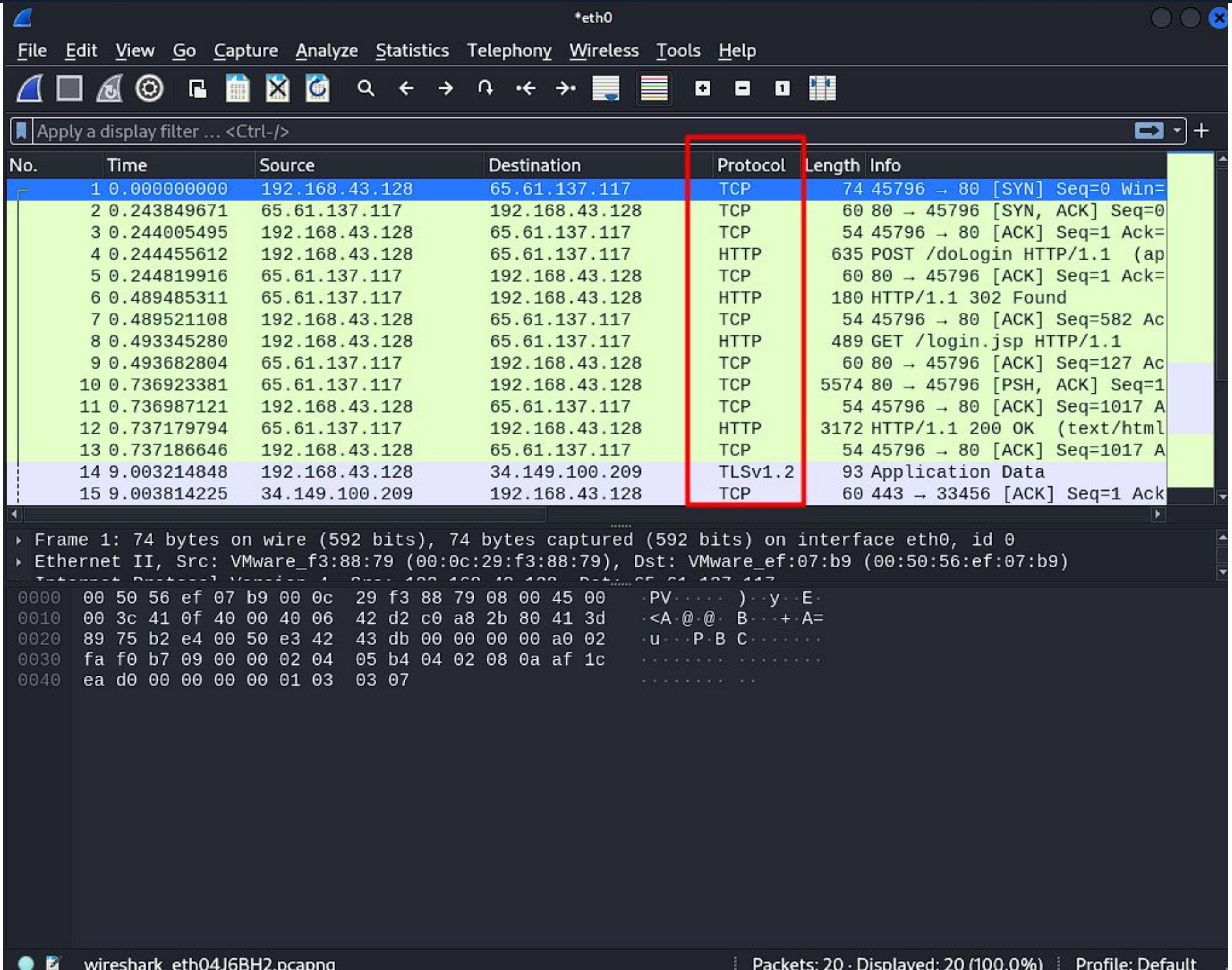
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.6 (Git v3.6.6 packaged as 3.6.6-1).

Protocol Header Analysis - Wireshark

- Filter Packets:

Use Wireshark's display filter to focus on specific protocols or addresses. For example, you can use filters like tcp, http, udp, or ip.addr == x.x.x.x to isolate packets of interest.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.128	65.61.137.117	TCP	74	45796 → 80 [SYN] Seq=0 Win=
2	0.243849671	65.61.137.117	192.168.43.128	TCP	60	80 → 45796 [SYN, ACK] Seq=0
3	0.244005495	192.168.43.128	65.61.137.117	TCP	54	45796 → 80 [ACK] Seq=1 Ack=
4	0.244455612	192.168.43.128	65.61.137.117	HTTP	635	POST /doLogin HTTP/1.1 (ap
5	0.244819916	65.61.137.117	192.168.43.128	TCP	60	80 → 45796 [ACK] Seq=1 Ack=
6	0.489485311	65.61.137.117	192.168.43.128	HTTP	180	HTTP/1.1 302 Found
7	0.489521108	192.168.43.128	65.61.137.117	TCP	54	45796 → 80 [ACK] Seq=582 Ac
8	0.493345280	192.168.43.128	65.61.137.117	HTTP	489	GET /login.jsp HTTP/1.1
9	0.493682804	65.61.137.117	192.168.43.128	TCP	60	80 → 45796 [ACK] Seq=127 Ac
10	0.736923381	65.61.137.117	192.168.43.128	TCP	5574	80 → 45796 [PSH, ACK] Seq=1
11	0.736987121	192.168.43.128	65.61.137.117	TCP	54	45796 → 80 [ACK] Seq=1017 A
12	0.737179794	65.61.137.117	192.168.43.128	HTTP	3172	HTTP/1.1 200 OK (text/html
13	0.737186646	192.168.43.128	65.61.137.117	TCP	54	45796 → 80 [ACK] Seq=1017 A
14	9.003214848	192.168.43.128	34.149.100.209	TLSv1.2	93	Application Data
15	9.003814225	34.149.100.209	192.168.43.128	TCP	60	443 → 33456 [ACK] Seq=1 Ack

```
› Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f3:88:79 (00:0c:29:f3:88:79), Dst: VMware_ef:07:b9 (00:50:56:ef:07:b9)
```

```
0000  00 50 56 ef 07 b9 00 0c  29 f3 88 79 08 00 45 00   ·PV·····  )··y··E·
0010  00 3c 41 0f 40 00 40 06  42 d2 c0 a8 2b 80 41 3d   ·<A·@·@·  B···+·A=
0020  89 75 b2 e4 00 50 e3 42  43 db 00 00 00 00 a0 02   ·u···P·B  C·······
0030  fa f0 b7 09 00 00 02 04  05 b4 04 02 08 0a af 1c   ········  ········
0040  ea d0 00 00 00 00 01 03  03 07                     ········  ··
```

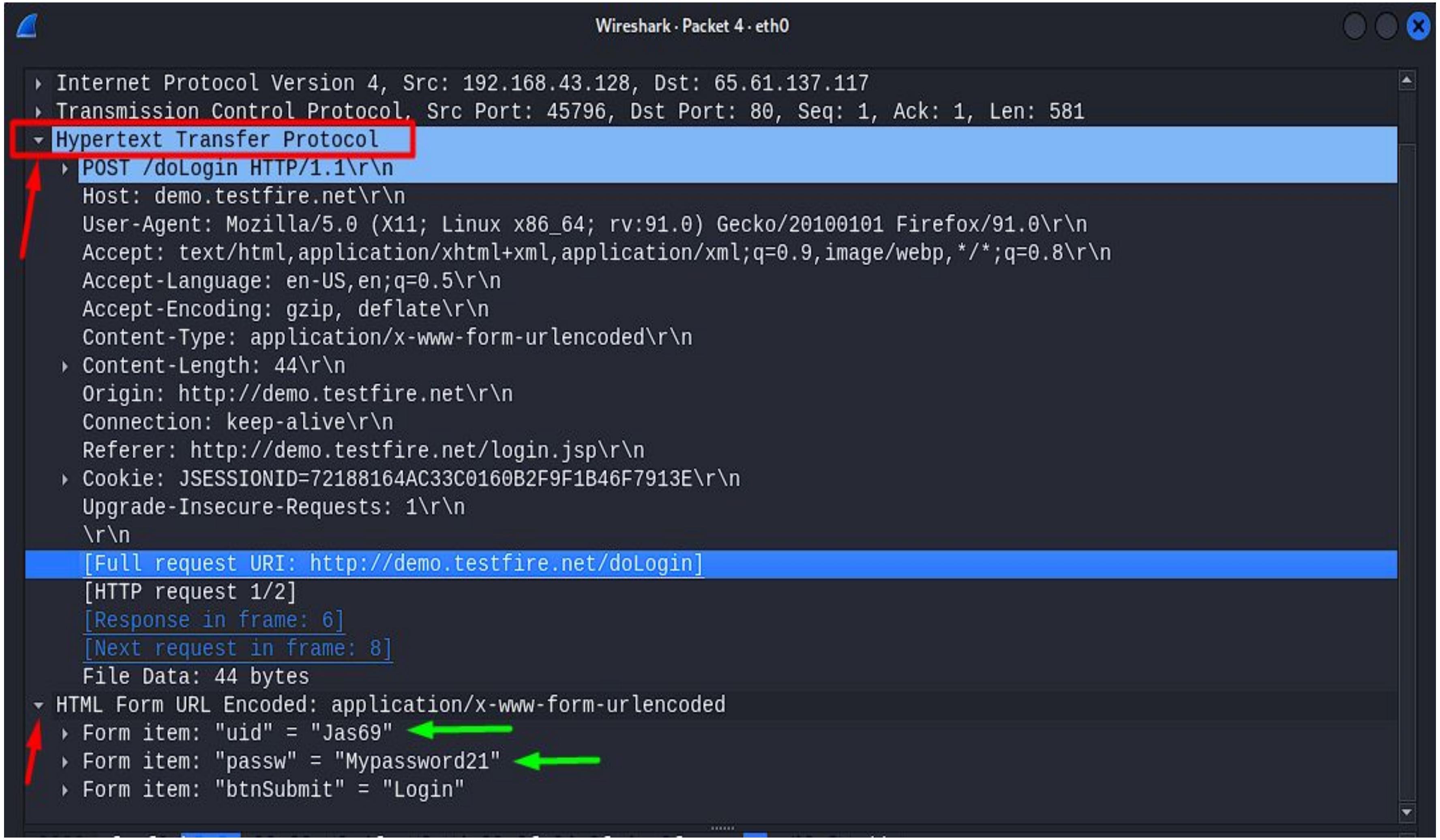
wireshark_eth04J6BH2.pcapng

Packets: 20 · Displayed: 20 (100.0%)

Profile: Default

Protocol Header Analysis - Wireshark

- Select a Packet
- Expand Protocol Layer
- View Header Fields



```
› Internet Protocol Version 4, Src: 192.168.43.128, Dst: 65.61.137.117
› Transmission Control Protocol, Src Port: 45796, Dst Port: 80, Seq: 1, Ack: 1, Len: 581
▾ Hypertext Transfer Protocol
  › POST /doLogin HTTP/1.1\r\n
    Host: demo.testfire.net\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  › Content-Length: 44\r\n
    Origin: http://demo.testfire.net\r\n
    Connection: keep-alive\r\n
    Referer: http://demo.testfire.net/login.jsp\r\n
  › Cookie: JSESSIONID=72188164AC33C0160B2F9F1B46F7913E\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://demo.testfire.net/doLogin]
    [HTTP request 1/2]
    [Response in frame: 6]
    [Next request in frame: 8]
    File Data: 44 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "uid" = "Jas69"
  › Form item: "passw" = "Mypassword21"
  › Form item: "btnSubmit" = "Login"
```

Intro to Security Engineering & Network Sec

Security Engineering is the discipline of designing, implementing, and maintaining systems and processes to ensure the confidentiality, integrity, and availability of information and systems

- ➔ Authentication
- ➔ Access Control,
- ➔ Data Confidentiality.
- ➔ Data Integrity
- ➔ Non-Repudiation
- ➔ Availability.

Intro to Security Engineering & Network Sec

Security Services:

- **Authentication:** Verifying the identity of users or systems to ensure secure access.
    - Logging into a computer system with a username and password.

- **Access Control:** Regulating and restricting user access to resources based on permissions.
    - A file server allowing only authorized users from the HR department to access sensitive employee data.

Security Services:

- **Data Confidentiality:** Safeguarding information from unauthorized access or disclosure.
  - Encrypting sensitive financial information during online transactions to prevent unauthorized users from reading it.

- **Data Integrity:** Ensuring the accuracy and reliability of data through prevention of unauthorized alterations.
  - Using checksums to verify that a downloaded file has not been altered or corrupted during the download process.

Intro to Security Engineering & Network Sec

Security Services:

- **Non-Repudiation:** Preventing individuals from denying their actions, confirming accountability.
  - Signing a digital document with a private key, providing proof that the sender cannot later deny sending it.

- **Availability:** Ensuring consistent and reliable access to resources and services.
  - A website ensuring uninterrupted access to its content despite heavy traffic or a distributed denial-of-service (DDoS) attack.

Security Attacks

Security attacks encompass a range of malicious activities aimed at exploiting vulnerabilities in computer systems, networks, or software to compromise the confidentiality, integrity, or availability of information.

- → ACTIVE
- → PASSIVE

Security Attacks

Active Security Attacks:

Active security attacks involve an intruder taking actions that manipulate or disrupt the normal operation of a system, network, or application. These attacks typically aim to compromise the confidentiality, integrity, or availability of the targeted resources. Here are examples of active security attacks:

- Denial-of-Service (DoS) Attack
- Man-in-the-Middle (MitM) Attack
- DNS Spoofing
- DNS Spoofing
- SQL Injection

Security Attacks

Passive Security Attacks:

Passive security attacks involve monitoring and capturing data without altering or disrupting the targeted systems. These attacks aim to gather sensitive information for unauthorized access or further exploitation. Here are examples of passive security attacks:

- ➔ Eavesdropping
- ➔ Traffic Analysis
- ➔ Packet Sniffing
- ➔ Wiretapping
- ➔ Passive DNS Spoofing

Denial Of Services (DoS)

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a system, network, or service by overwhelming it with a flood of illegitimate requests, thereby rendering it temporarily or indefinitely unavailable to legitimate users. The primary goal of a DoS attack is to exhaust the target's resources, such as bandwidth, processing power, or memory, causing a disruption in its ability to handle legitimate requests

➔ Single Source

➔ Limited Scale

Distributed Denial Of Services (DDoS)

A Distributed Denial of Service (DDoS) attack is an advanced and more potent form of a DoS attack, where multiple compromised systems, known as a botnet, work collaboratively to inundate a target with an overwhelming volume of traffic. DDoS attacks are more challenging to mitigate because they distribute the attack across multiple sources, making it difficult to discern and block the malicious traffic

➔ Multiple Source

➔ Scale & Intensity

Introduction to Key Cybersecurity Concepts

Vulnerability:

Definition: A vulnerability is a weakness or flaw in a system, network, application, or process that could be exploited to compromise its security.

Example: Unpatched software, misconfigured settings, or weak passwords can represent vulnerabilities in a system.

Threat:

Definition: A threat refers to a potential danger or a harmful event that can exploit vulnerabilities, leading to potential harm to a system or organization.

Example: Malware, hackers, or natural disasters are examples of threats that can pose risks to information systems.

Attack:

Introduction to Key Cybersecurity Concepts

Attack:

Definition: An attack is a deliberate action or series of actions that take advantage of vulnerabilities to compromise the integrity, confidentiality, or availability of a system.

Example: A hacker exploiting a vulnerability in a web application to gain unauthorized access and steal sensitive information.

Bug:

Definition: A bug is an unintentional coding error or flaw in software that can lead to unexpected behavior or vulnerabilities.

Example: A software bug might cause a program to crash or behave differently than intended, potentially creating security issues

Introduction to Key Cybersecurity Concepts

Exploit:

Definition: An exploit is a piece of software, code, or sequence of commands that takes advantage of a specific vulnerability to carry out a malicious action.
Example: An attacker using a known exploit to target a vulnerability in a web server and gain unauthorized access.
Interrelationships:

★ *Scenario: A software application (system) may contain a bug due to a coding error (vulnerability). If an attacker discovers this vulnerability, they can use an exploit to carry out an attack, posing a threat to the security of the system.*

Reference

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - https://www.nist.gov/cyberframework
- Cybersecurity & Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/
- Open Web Application Security Project (OWASP)
  - https://owasp.org/

Thank you