Information Security Lab
Week-12

PRERIT SHARMA
21103121

QUESTION 1:

ARP, TCP, DNS

QUESTION 2:

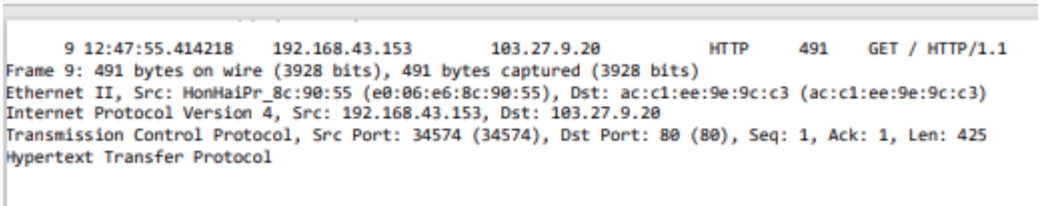
HTTP-GET : 12:47:55.414218	192.168.43.153	103.27.9.20	HTTP	491	GET / HTTP/1.1
HTTP-OK: 12:47:56.188990	103.27.9.20	192.168.43.153	HTTP	945	HTTP/1.1 200 OK (text/html)
Time taken = 0.774772

QUESTION 3:

Internet Protocol Version 4
Src(My Computer): 192.168.43.153
Dst(iitd.ac.in): 103.27.9.20

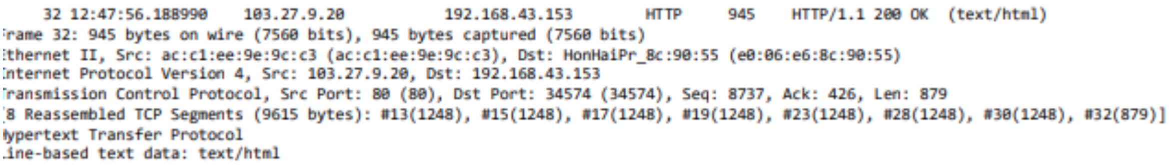
QUESTION 4:

GET



```
      9 12:47:55.414218    192.168.43.153        103.27.9.20           HTTP     491    GET / HTTP/1.1
Frame 9: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits)
Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: ac:c1:ee:9e:9c:c3 (ac:c1:ee:9e:9c:c3)
Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.20
Transmission Control Protocol, Src Port: 34574 (34574), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 425
Hypertext Transfer Protocol
```

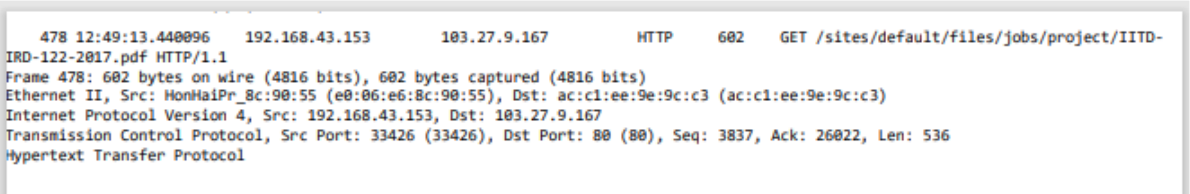
OK



```
    32 12:47:56.188990    103.27.9.20           192.168.43.153        HTTP     945    HTTP/1.1 200 OK  (text/html)
rame 32: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
thernet II, Src: ac:c1:ee:9e:9c:c3 (ac:c1:ee:9e:9c:c3), Dst: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55)
nternet Protocol Version 4, Src: 103.27.9.20, Dst: 192.168.43.153
ransmission Control Protocol, Src Port: 80 (80), Dst Port: 34574 (34574), Seq: 8737, Ack: 426, Len: 879
8 Reassembled TCP Segments (9615 bytes): #13(1248), #15(1248), #17(1248), #19(1248), #23(1248), #28(1248), #30(1248), #32(879)]
ypertext Transfer Protocol
ine-based text data: text/html
```

QUESTION 5:

HTTP-GET



```
   478 12:49:13.440096    192.168.43.153       103.27.9.167         HTTP     602    GET /sites/default/files/jobs/project/IITD-
IRD-122-2017.pdf HTTP/1.1
Frame 478: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits)
Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: ac:c1:ee:9e:9c:c3 (ac:c1:ee:9e:9c:c3)
Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.167
Transmission Control Protocol, Src Port: 33426 (33426), Dst Port: 80 (80), Seq: 3837, Ack: 26022, Len: 536
Hypertext Transfer Protocol
```

Packet number: 478

After successful download: Packet- 503
12:49:13.700007 103.27.9.167 192.168.43.153 HTTP 243 HTTP/1.1 200 OK (application/pdf)
[Time since request: 0.259911000 seconds]
Length- 243 [Frame 503: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)]

Week-13

QUESTION 1:

a) Filter used: ftp || ftp-data
Server: 10.121.70.151—-(Responds)
Client : 10.234.125.254—-(Requests)

b) FTP error code 530 specifically signifies a "Not Logged In" status or authentication failure in the FTP (File Transfer Protocol) communication

c) Filter used: ftp.request.command == "USER" && ftp.request.command != “PASS"
1397 attempts made in one minute

QUESTION 2:

a) This information allows you to analyze TCP connections in the captured data, providing insights into the volume of traffic between different endpoints, the duration of connections, and the amount of data exchanged.

QUESTION 4:

1) ARP Request (Who has...? Tell…):

- This type of ARP packet is a request sent by a device to discover the MAC address associated with a specific IP address on the network.
- For instance, in the packet Who has 169.254.255.255? Tell 10.0.2.1, a device is asking for the MAC address associated with IP 169.254.255.255 and telling its own IP 10.0.2.1.

ARP Reply (... is at …):

- This type of ARP packet is a response to an ARP request. It contains the information about the requested IP-to-MAC address mapping.
- For instance, in the packet 10.0.2.1 is at 00:26:08:e5:66:07, it states that the device with IP 10.0.2.1 has the MAC address 00:26:08:e5:66:07.

2) b) Port-Active Mode
Pass-Passive Mode
PORT 10,0,2,2,199,51

c) One significant vulnerability of the FTP protocol is its lack of encryption for data transmission. In a packet capture, FTP commands, usernames, passwords, and transferred files are often visible in plain text, making them susceptible to interception and potential exploitation by malicious actors. This lack of encryption exposes sensitive information, posing a security risk, especially when used over unsecured networks like the internet.

d) 1.SFTP(SSH File Transfer Protocol)
2. FTPS(FTP-SSL)

3) a) The domain name in the packet is clients4.google.com.

b)

- Strong Encryption: Utilize modern TLS versions and robust encryption algorithms to prevent eavesdropping.
- Perfect Forward Secrecy (PFS): Implement PFS to ensure security even if long-term keys are compromised.
- Disable SSL/TLS Compression: Prevent attacks by disabling compression vulnerable to exploits like CRIME and BREACH.
- Harden Server Configuration: Employ HSTS, disable weak protocols/ciphers, and enforce secure TLS configurations.
- SNI Encryption (in progress): Efforts to encrypt Server Name Indication (SNI) to enhance privacy during TLS handshakes.
- Content Security Policies (CSP): Use CSP headers to restrict content sources and mitigate cross-site scripting (XSS) risks.

4) a) Insecure Authentication Method: The browser's authentication relies on stored cookies or tokens for subsequent requests after login. If these are not adequately protected or are susceptible to theft or session hijacking, it poses a risk.

b) Session Hijacking: If an attacker gains access to the user's session token or cookie, they can impersonate the user by using these credentials to send requests, essentially taking control of the user's session without needing the actual username or password.

c) Preventive Measures: Users can protect against this by enabling two-factor authentication (2FA), regularly clearing browser cookies and cache, using VPNs or secure networks, and avoiding unsecured public Wi-Fi.

d) Activity on Facebook: Specific user actions or activities on Facebook, if visible in the packet capture, could include interactions such as posting, liking, commenting, browsing profiles, sending messages, or accessing certain features/pages.