Wireshark Demonstration

Austin Johns

Grand Canyon University

ITT306

Kris Peters

19 March 2021

**Screenshots**

Login Success

A screenshot of a computer

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Login Failure

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

Login Success captured by Wireshark

Graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Protocols**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol Initials | Full Name | Purpose | Type of Application Likely to Utilize the Protocol | Security Vulnerability to Wireshark |
| SMTP | Simple mail transfer protocol | Secure mail transition, send and receive messages | Mail and other transfer agents | Wireshark can filter all SMTP packets that pass through network communications |
| IMAP | Internet message access protocol | Sets a standard for protocol of accessing email messages from a server | Outlook, Gmail, Mail | Can help monitor and filter malicious activity towards a personal account |
| DNS | Domain Name System | Centralized standard for network naming protocols | All applications use DNS to recognize and communicate with networks | DNS IP Addresses are easy to fake. |
| SSH | Secure Shell | Encryption protocol for unsecured networks that allows for secured communication | SSH is used on unsecured networks and can be implemented into public networks | Interception is a main security risk |
| POP | Post office protocol | Protocol for receiving emails from a server | Used by email clients like Mail, Outlook, and Gmail. | Password is communicated over the network and can be intercepted with careful interception |
| FTP | File transfer protocol | Protocol for transferring files over a network securely | FTP is used between computers and between networks. | FTP is considered less secure because authentication is communicated without encryption. |
| TELNET | Telnet | Allows for text transfer between a local network or an online network. | Used to test servers and messaging platforms. Remote access is common with TELNET | When unencrypted, login information is communicated in plain text without protection. |