Linnaeus University
Computer Science
Ola Flygt

2021-11-07

2DV703 Mobile and Wireless Data Security

Assignment #1

A1. Browse the following list of terms and acronyms. These are typical terms from data communication and IT Security, and you should already be familiar with most of them. If not, search for and read materials that will help you understand them. If you lack knowledge about many of them, you probably don't have the prerequisites for the course!

7-layer reference model	Address resolution
Asymmetric Encryption	Authentication
Bandwidth	Block cipher
Broadcast	Category 5 cable
Certificate	Checksum
Classless addressing	CRC
CSMA/CD	Denial of service (DoS)
DHCP	Digital signature
DNS	Encryption key
Ethernet Frame	FTP
Hash function	HTTP Server
Firewall	IANA
Man-in-the middle attack	IP tunnel
Message Authentication code	Multiplexing
NAT	Parity bit
Promiscuous mode	Propagation delay
Public-key Encryption	Quality of Service
Router	Session key
SNMP	Switch
Symmetric encryption	TLS/SSL

A2. Read the articles "Navigating the Challenges with Wireless Security", "Wireless Security Survey 2016", "MOBILE SECURITY REPORT 2021 - pradeo" and "The Q1 2019 Mobile Threat Landscape Report". You will find them in the course site. Also read chapters 1 and 11 in the textbook "Wireless and Mobile Device Security".

Write a short report (3-4 pages) with the title "Challenges in Mobile and Wireless Security". Summarizing the most important aspects of each article and the textbook chapters. Add also a section with your own ideas on what the main challenges are today on the topic of Mobile and Wireless Security.

Submit the report in MyMoodle at latest Sunday 14 November.

We will discuss both your reports and the terms in part A1 on **Monday 15 November**.

Linnaeus University
Computer Science
Ola Flygt

2021-11-07

B. Each group should perform several practical tasks in the lab. The group should solve these tasks without cooperation with the other groups. Listed you will find the tasks that all groups should do with their respective devices:

Start by updating your groups wiki in MyMoodle that you can use to reference devices later (Password, IP, naming convention etc.). Include a TO-DO list and a system to mark done/to-do/partial etc. Also include relevant sources that you have used/could consider using to configure the devices. This wiki will be used during the whole course, and you will find it very useful when working in the lab!

Scenario
Your group is hired by a company where they recently found that the previous administrator had malicious intents and corrupted the configurations on the company's devices! The CTO have ordered all the devices to be restored to factory default configuration and start the work of setting up the systems from scratch.

You work as a group so you may split the work between group members, but at the end of each assignment, make sure that everyone knows how to configure all the devices and solve all challenges. Keep each other updated on all changes and discuss different solutions in the group before making any changes.

1. Make sure the provided hardware (Switch, Firewall and Access Point) is reset to factory default before starting (see provided information on the site for this) settings. Use the naming convention and make sure you write down all the configuration details (passwords, DHCP range, model name, port number etc.) in the group page. Also mark your equipment with labels.

2. Configure the Firewall with default settings to be able to connect to the Internet, separating the outside from the inside network with basic NAT and DHCP.

3. Setup the Switch on the inside interface of the firewall

4. Install one of the laptops as a server (choose any operating system) with services for at least FTP and HTTP. Add some content to the server making it possible to connect from different types of clients. For now, put the server on the inside network.

5. Install another computer as an internal server. This server will be used to distribute services in the network and should later act as a domain controller. Also make sure that at least one computer is able to connect to the console port of network devices (have a serial port).

Again, must write documentation for their configurations and put them in your wiki. Make subsections for configurations and documentation of the lab for different pieces of equipment.

Part B should be completed at latest **Friday 19 November.**