Network Protocol Research Assignment

Objectives

The objective of this lab is to allow the student to gain familiarity with functionality and security issues with network protocols as well as on attacks against their vulnerabilities.

Requirements:

Network Protocol Selection –Must be approved by the instructor before you can begin working on the assignment.

- Topic - Proposed network protocol your will be researching and demonstrating.
- Identify who will be working in your group (max 3)

Once approved, students are to discuss and demonstrate the approved network protocol. The students will produce a report with the following sections, as a minimum. Students will also prepare and deliver a presentation video based on the report. **Recommended, a live demonstration of the protocol functionality and security issues**.

- **All protocols must be approved by the instructor. No duplicate protocols will be allowed between students.**
- **To receive a mark, both the report and presentation video must be completed**

DELIVERABLE: REPORT (70%)

1. General description of the protocol and the security issues (30)
    a. Example points to include
        i. RFC reference(s)
        ii. How and why the protocol is used
        iii. Prevalence of the protocol
        iv. When was the protocol developed?
        v. How many revisions or versions are there?
        vi. Protocol vulnerabilities
        vii. Security issues/flaws
        viii. Common attacks
        ix. Etc.
2. Port number(s) used by the protocol (5)
3. Header structure (15)
    a. Describe all fields
4. Functionality of the protocol (20)
    a. Options
    b. Response codes
    c. Etc.
5. Sample communications (15)
6. Packet capture output (10)
   Any other known or potential flaws or issues. (in your own words) (5)

DELIVERABLE: PRESENTATION (30%)

1. Your team will prepare and deliver a presentation based on the report.
2. Your team will present a live demonstration of the protocol functionality and security issues to the instructor and class.
3. Every member is required to participate, you will have 15 minutes to demonstrate and discuss your protocol.
4. Attendance at other presentations is required, and failure to attend will result in a mark deduction

Possible protocols include, but are not limited to:

a. Bitcoin
b. Tor
c. WireGuard
d. BitTorrent
e. IP-Sec
f. RDP
g. RTMP
h. ECN
i. MPLS
j. XTP
k. QUIC

Exempt protocols that are covered in class/are depreciated, include, but are not limited to:

a. HTTP
b. HTTPs
c. FTP
d. ARP
e. TCP/UDP
f. SNMP
g. IMAP/POP3
h. ICMP
i. ETHERNET
j. IPv4/IPv6
k. DHCP
l. DNS
m. TLS/SSL

Administrivia:

1. All references must be cited correctly.
2. The report is to be formatted in formal report format (See Documentation Standards).