



Course: CSC 365 Network Security

Dated: 30-10-2025

Maximum Marks: 25

Allowed: 80-90 Minutes

- Make sure that you have signed the attendance sheet before leaving the examination room
- Return the question paper along with the answer sheet.
- Please attempt questions CLO wise. Mention question numbers

CLO-1: Explain security principles, network protocol vulnerabilities, associated attacks, and prevention methods.

Question 1 [11 points]:

- [02 point] Briefly discuss difference between X.509 and Web of trust certificates?
- [02 point] Discuss defense techniques to address phishing attack?
- [02 points] Explain how PGP arrange for security features such as source authentication, non-repudiation and message integrity?
- [02 points] Explain how the PGP manages situation where the users can have more than one Public/Private key pairs?
- [03] Briefly discuss the three protocols which helps reduces spam/phishing

CLO-2 : Apply network defense techniques to prevent security attacks [14 points].

Question 2 [3 points]:

CS 161 students are using a modified version of Piazza to discuss project questions! In this version, the names and profile pictures of the students who answer questions frequently are listed on a side panel on the website. The server stores a table of users with the following schema:

```
1 CREATE TABLE users (  
2     First TEXT,           -- First name of the user.  
3     Last TEXT,           -- Last name of the user.  
4     ProfilePicture TEXT,  -- URL of the image.  
5     FrequentPoster BOOLEAN, -- Are they a frequent poster?  
6 );
```

Q2.1 Assume that you are a frequent poster. When playing around with your account, you notice that you can set your profile picture URL to the following, and your image on the frequent poster panel grows wider than everyone else's photos:

ProfilePicture URL: `https://cs161.org/evan.jpg" width="1000`

This can be done using what kind of attack. Apply appropriate network defense techniques.

Question 2 [3 points]:

A session cookie is used by most websites in order to manage user logins. When the user logs in, the server sends a randomly-generated session cookie to the user's browser. The server also stores the cookie value in a database along with the corresponding username. The user's browser sends the session cookie to the server whenever the user loads any page on the site. The server then looks the session cookie up in the database and retrieves the corresponding username. Using this, the server can know which user is logged in.

Some web application frameworks allow cookies to be set by the URL. For example, visiting the URL `http://foobar.edu/page.html?sessionid=42`.

will result in the server setting the sessionid cookie to the value "42".

Q10.1 Can you spot an attack on this scheme?

Q10.2 Suppose the problem you spotted has been fixed as follows: foobar.edu now establishes new sessions with session IDs based on a hash of the tuple (username, time of connection). Is this secure? If not, what would be a better approach?

Question 3 [3 points]:

Recall that DHCP (Dynamic Host Configuration Protocol) is responsible for setting up configurations when a computer first joins a local network. Assume that Alice wants to connect to the network, but she's missing a configuration. You want to supply a forged configuration to Alice, causing packets that she intends to send to the network to be sent to you instead.

For this part, assume that your computer has IP address 10.10.10.66 and the network's router and DHCP server have IP address 10.10.10.5. There are no other machines on the network and there are no reserved or private IP addresses.

Q8.1 Alice broadcasts a request for a configuration to everyone.

What values of the assigned IP address and the router's IP address could you include in your response to Alice in order to cause packets that she intends to send to the network to be sent to you instead?

Q8.2 Alice broadcasts to everyone else on the LAN: "What is the MAC address of 10.10.10.88?" Recall that 10.10.10.88 corresponds to Bob's IP address.

What values for the IP and MAC address could you include in your response to Alice to cause her messages intended for Bob to be sent to you instead?

Q8.3 How would your spoofed response to Alice change if Bob was outside the LAN that you and Alice are both part of?

Question 4 [5 points]:

Analyze the email from President Donald Trump?

Here is the raw header:

```
Received: from CY1PR0701MB1819.namprd07.prod.outlook.com (10.163.42.152) by
SN1PR0701MB1822.namprd07.prod.outlook.com (10.162.100.151) with Microsoft
SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1240.13 via
Mailbox Transport; Wed, 12 Jul 2017 22:49:17 +0000
Received: from SN1PR0701CA0032.namprd07.prod.outlook.com (10.162.96.42) by
CY1PR0701MB1819.namprd07.prod.outlook.com (10.163.42.152) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
15.1.1261.13; Wed, 12 Jul 2017 22:49:16 +0000
Received: from BY2NAM01FT042.eop-nam01.prod.protection.outlook.com
(2a01:111:f400:7e42::203) by SN1PR0701CA0032.outlook.office365.com
(2a01:111:e400:5173::42) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1261.13 via
Frontend Transport; Wed, 12 Jul 2017 22:49:16 +0000
Authentication-Results: spf=none (sender IP is 148.163.152.157)
smtp.mailfrom=loki.ist.unomaha.edu; unomaha.edu; dkim=none (message not
signed) header.d=none; unomaha.edu; dmarc=none action=none
header.from=whitehouse.gov;
Received-SPF: None (protection.outlook.com: loki.ist.unomaha.edu does not
designate permitted sender hosts)
Received: from mx0b-00261b01.pphosted.com (148.163.152.157) by
BY2NAM01FT042.mail.protection.outlook.com (10.152.68.172) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
15.1.1240.9 via Frontend Transport; Wed, 12 Jul 2017 22:49:15 +0000
```