Nova Southeastern University
College of Computing and Engineering

Assignment 4
ISEC 660 Advanced Network Security

Winter 2021
Due date: 4/11/2021
Total Points: 100

Notes:
1. Please include your name in EVERY document you submit.
2. Please sign and submit the "Certification of Authorship" form (located in Canvas) along with your solutions.

Section I. Reading

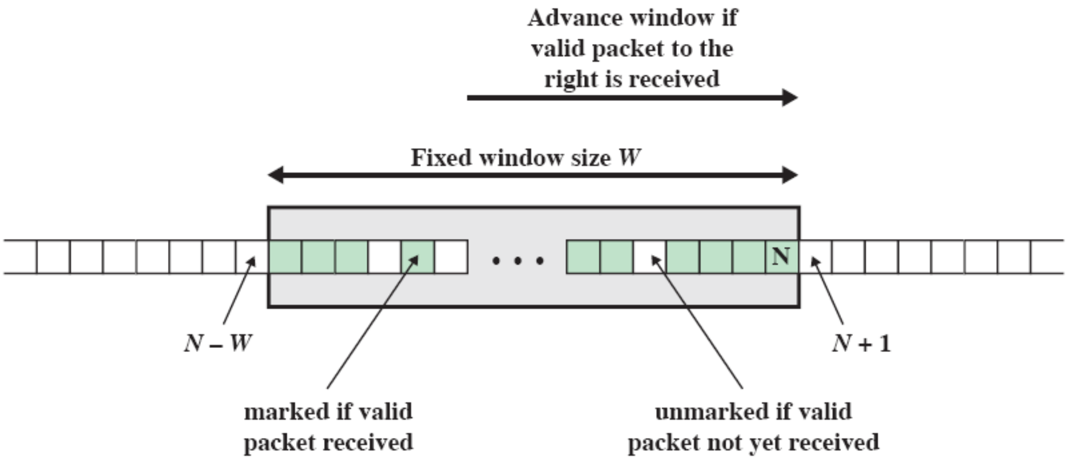
Chapters 8, 9, 22, 23, 24, additional materials (see questions below)

Section II. Questions (70 points, all questions are equally weighted)

2.1 Network Security (Main Reference: Chapter 22) (10 points)

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The Sequence Number field in the IPsec authentication header is designed to thwart such attacks. Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IPsec authentication document dictates that the receiver should implement a window of size *W*, with a default of *W*=64. The right edge of the window represents the highest sequence number, *N*, so far received from a valid packet. For any packet with a sequence number in the range from *N*–*W*+1 to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked (see Figure below).

2.1.1 What are the differences between sequence numbers in IPsec and the sequence numbers in TCP?
2.1.2 Deduce from the figure how processing proceeds when a packet is received and explain how this counters the replay attack.


Advance window if valid packet to the right is received
Fixed window size W
N
$N - W$
$N + 1$
marked if valid packet received
unmarked if valid packet not yet received

2.2 Network Security (Main Reference: Chapter 23) (10 points)

Using your web browser, visit a secure website (i.e., one whose URL starts with "https"). Examine the details of the X.509 certificate used by the website. This is usually accessible by selecting the padlock symbol. Referring to Figure 23.3 ("X.509 Formats"), answer the following questions with details.

a. Identify the key elements in the certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.
b. State whether this is a CA or end-user certificate, and why.
c. Indicate whether the certificate is valid or not, and why.
d. State whether there are any other obvious problems with the algorithms used in the certificate.

2.3 Network Security (Main Reference: Chapter 24) (10 points)

In IEEE 802.11, open system authentication simply consists of two communications. An authentication is requested by the client, which contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.
2.3.1 What are the benefits of this authentication scheme?
2.3.2 What are the security vulnerabilities of this authentication scheme?

2.4 Review the following document (NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing) and briefly answer the following questions. (40 points)

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Note: You don't have to refer to additional materials to answer the following answers. If you do, please include a list of references in your submission.

2.4.1 What are the main deployments models in cloud computing? What are the main service models in cloud computing?

2.4.2 What are the main governance issues in cloud computing?

2.4.3 Briefly explain the following security and privacy laws that govern cloud security: HIPAA, Clinger-Cohen Act, Privacy Act, E-Government Act, and FISMA.

2.4.4 What are the main attack vectors on multi-tenancy in virtual machine-based cloud infrastructures?

2.4.5 What are the general concerns on public cloud outsourcing?

Section III. Practical assignment (30 points)

Snort (https://www.snort.org/) is a powerful open source network-based intrusion detection/prevention system (IDS/IPS) that has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

In this assignment, you are required to download and install the software, and run a few test cases based on the rule sets provided by the user community. Note that the assignment covers only some basic features of Snort. You are highly recommended to explore more advanced features.

Steps:

1. Download the software from https://www.snort.org/. The software supports multiple platforms including Windows OS, Linux/Unix (most preferable), and Mac OS. Make sure that you install the correct version on your computer.
2. Install the latest ruleset on your computer. You will need to register in order to download a complete rule set.
3. Test your program including its configuration, the whitelist, and run a few test cases.
4. Insert your own rules into the *local.rules* file and test them out. Some rules may be better tested when you deploy your computer to the DMZ zone of your home/office network so that it can be accessed directly from the external network. Some tests may need to be initiated from a different computer.

For more information, please refer to the following URLs.

https://www.youtube.com/watch?v=RwWM0srLSg0 (how to install Snort on Windows)

https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort https://www.snort.org/documents

Answer the following questions.

3.1 Briefly test and explain the following rules. Show screenshots of your test.

```
Rule #1:
alert udp $HOME_NET any -> any any (msg:”UDP Request”; sid:1000001;)

Rule #2:
alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:”HTTP Request”;
sid:1000002;)
```

3.2 Briefly explain the following rules. Testing is recommended by not mandatory.

```
Rule #1:
alert udp $HOME_NET any -> any 53 (msg:"APP-DETECT DNS request for
potential malware SafeGuard to domain 360safe.com"; flow:to_server;
byte_test:1,!&,0xF8,2; content:"|07|360safe|03|com|00|";
fast_pattern:only; metadata:policy max-detect-ips drop, service dns;
reference:url,en.wikipedia.org/wiki/360_Safeguard;
reference:url,research.zscaler.com/2011/05/is-360cn-evil.html;
reference:url,www.alexa.com/siteinfo/360safe.com;
reference:url,www.virustotal.com/en/domain/360safe.com/information/;
classtype:trojan-activity; sid:28070; rev:3;)

Rule #2:
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"APP-DETECT
Absolute Software Computrace outbound connection - 209.53.113.223";
flow:to_server,established; content:"Host|3A| 209.53.113.223|0D 0A|";
fast_pattern:only; http_header; content:"TagId: "; http_header;
metadata:policy max-detect-ips drop, policy security-ips drop, ruleset
community, service http;
reference:url,absolute.com/support/consumer/technology_computrace;
reference:url,attack.mitre.org/techniques/T1014;
reference:url,www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-
Kamluk-Computrace-Backdoor-Revisited.pdf;
reference:url,www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-
Ortega-DeactivateRootkit-PAPER.pdf; classtype:misc-activity; sid:32845;
rev:3;)

Rule #3:
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"PROTOCOL-ICMP
Information Reply undefined code"; icode:>0; itype:16; metadata:ruleset
community; classtype:misc-activity; sid:416; rev:10;)
```

3.3 Assume your organization’s security policy requires blocking of all access to *Youtube.com* with working computers. Write a local rule that can log violations to this policy.

3.4 Assume your organization’s security policy requires that any request to a remote web server *http://www.malicious.com* should be closely monitored. Write a rule that logs every 10th request from internal network to this web server on a 60 second interval.

3.5 Based on your experience, how will you evaluate Snort? In what aspects could the tool be improved?