NWEN 405 Assignment #2 2017

Short Answer Revision Questions (50%)

a) [5 marks] Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?

b) [5 marks] Define the terms false positive and false negative. Give an example of both in the context of an intrusion detection system monitoring network traffic for evidence of potential intrusions.

c) [5 marks] List and briefly define the three broad categories of classification approaches used by anomaly detection systems.

d) [5 marks] List three design goals for a firewall.

e) [5 marks] What is the difference between a packet filtering firewall and a stateful inspection firewall?

f) [5 marks] How does an IPS differ from a firewall?

g) [5 marks] What are the two key elements that must be identified in order to implement a buffer overflow?

h) [5 marks] List and briefly describe some of the defenses against buffer overflows that can be implemented when running existing, vulnerable programs.

i) [5 marks] Define the difference between *software quality and reliability* and *software security*.

j) [5 marks] State the similarities and differences between command injection and SQL injection attacks.

k) [5 marks] Define input fuzzing. State where this technique should be used.

l) [5 marks] Give an example of a security problem that can arise due to careless use of environment variables by shell scripts. Describe the functionality of the shell script, how careless use of the environment variable can be exploited and outline the potential effect of a successful exploitation.

Practical component (50%)

Squid is the de-facto proxy webserver (application layer firewall) used in many organizations to filter, primarily, HTTP access and restrict access to specific resources. It is also widely used as a caching proxy.

You are provided with two Lubuntu virtual machines. Use one of the virtual machines as the proxy server and the other Lubuntu VM and your host Windows machines as the clients. The Squid server is

already installed on the Lubuntu machines (You will only need to configure on one of the VMs). You may check its status using the following command:

```
$service squid status
```

In this assignment, you are required to write a rule for the following scenarios:

1. Write a rule to block HTTP access to any clients accessing any websites with URLs containing a predefined list of keywords, during peak hours. The peak hours are between 8-11 am and 3-5 pm on Weekdays. The keywords are in a file called blockedkeywords.txt on your local drive. The rule should block any websites having any instance of the words (lower letter, UPPER LETTER) [2 Marks]

2. Write a rule to block website access to all "Internet Explorer" browsers attempting to access Internet from Windows Machines. Other browsers such as Chrome, Firefox, Safari, and any other browsers on Linux machines should be allowed to access the Internet. [2 Marks]

3. Write a rule to authorize internet access to clients in your subnet, by asking for their username and passwords. The usernames and passwords are saved in a file on local drive. The rule should also only authorize users located on your local subnet identified by their respective IP addresses or subnet mask. For instance if David and James are legitimate users with proper credentials, they system should only grant them access if they provide proper user name and password and only if they are connecting to the proxy from the local subnet or from a list of selected IP addresses only (e.g. 192.168.1.3, 192.168.1.4) [2 Marks]

4. Write a rule to block access to all facebook, twitter and youtube domains to your Linux (Lubuntu) client only, and redirect the host to a custom page displaying the organization's policy. The policy states that access to these social media sites are restricted. [2 Marks]

5. Write a rule to block a specific client (choose any Lubuntu or Windows) with a specific MAC address from downloading .js, and .pdf files. [2 Marks]

Report Requirements

The report should consist of the following pages:

1. Cover Page with your name, student ID
2. Associated rule for each task
3. Screenshot of your custom page delivered to the client in task 4

Resources:

Squid's official website provides extensive documentation for a large number of configuration scenarios. Many online sources are also available at your disposal.

http://www.squid-cache.org/Doc/config/

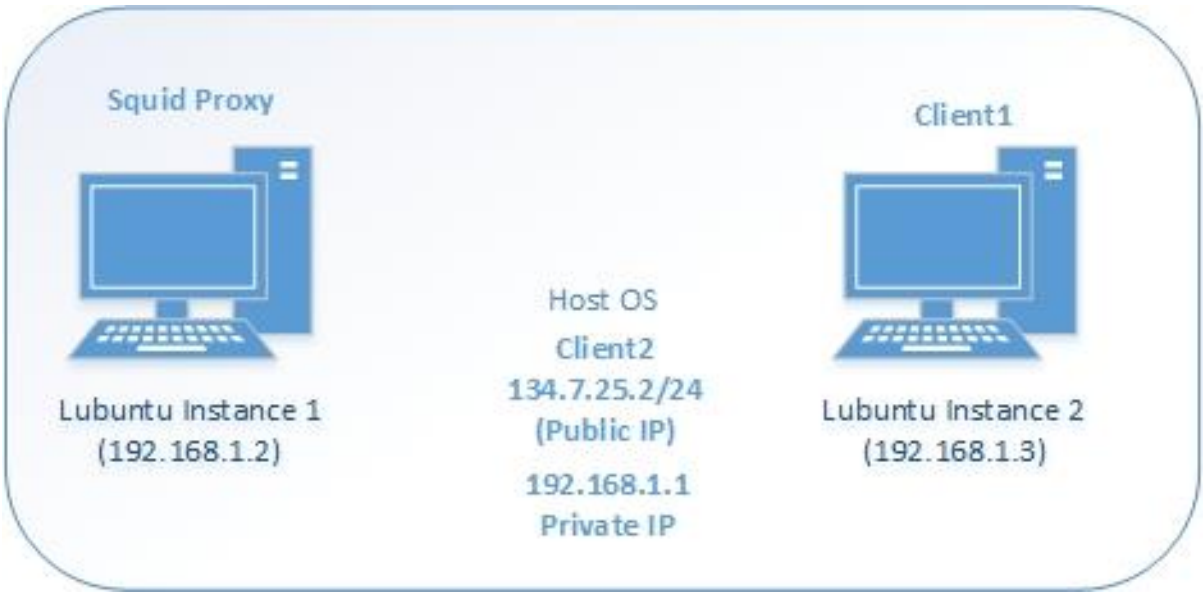
You are provided with a Debian-based operating system virtual machine (Lubuntu). The Lubuntu system has squid and required libraries installed. You may install it using the following commands:

```
$apt-get install squid3

$apt-get install apache2-utils
```

You are free to use any other Linux distributions or operating systems. The username and password for the Lubuntu virtual machines are: "**nwen405**"

You may run the Squid server on a single instance of Lubuntu while another instance and the host machine work as the clients, see figure 1. In such a scenario the IP address of the system with Squid server running Lubuntu Instance 1, 192.168.1.2) becomes the IP address of the proxy server and is used as an input in the proxy settings of the other client's browsers (Client1) and host operating system (client2). (You can define the port number in Squid configuration)



You may also run a different setup by running three instances of Lubuntu, assigning one to your squid server and others to clients.

Instructions:

- The Squid configuration file is located at /etc/squid/squid.conf
- You can define the port squid uses by placing “http_port 3128” at the beginning of the config file (without double quotations)
- Once you add your ACLs and rules into the squid configuration file, you will need to restart the squid service for changes to take effect. This can be done using the command

```
#service squid restart
```

- It is general practice to follow an “allow-then-deny-all” approach which means, you allow http_access to selected objects identified through ACLs, place specific restrictions and finally deny for all

The simplest form of configuration can be:

```
http_port 3128


#acl mylocalnet src 130.195.24.0/24
acl myhost src 192.168.159.129

http_access deny mylocalnet
http_access allow myhost
http_access deny all
```

The above configuration assigns the local host (192.168.159.129) to an ACL called myhost and subsequently allows http_access. It also assigns 130.195.24.0/24 subnet to an ACL called mylocalnet and blocks http_access to all the hosts within that subnet. Finally it denies access to everyone else.

Once your configuration file is written, restart the squid service and check its status through:

```
$service squid restart

$service squid status
```

The service should be Active (running). If your rules are not properly defined, squid notifies you accordingly.

```
enphiniti@enphiniti2020: ~
enphiniti@enphiniti2020:~$ service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
   Active: active (running) since Mon 2016-12-19 09:07:53 IST; 5h 43min ago
     Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/squid.service
           ├─ 994 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─ 996 (squid-1) -YC -f /etc/squid/squid.conf
           ├─1191 (logfile-daemon) /var/log/squid/access.log
           └─4542 (pinger)

Dec 19 09:07:53 enphiniti2020 squid[631]: 2016/12/19 09:07:53| WARNING: Could no
Dec 19 09:07:53 enphiniti2020 squid[631]: 2016/12/19 09:07:53| WARNING: Could no
Dec 19 09:07:53 enphiniti2020 squid[994]: Squid Parent: will start 1 kids
Dec 19 09:07:53 enphiniti2020 squid[994]: Squid Parent: (squid-1) process 996 st
Dec 19 09:07:53 enphiniti2020 squid[631]:    ...done.
Dec 19 09:07:53 enphiniti2020 systemd[1]: Started LSB: Squid HTTP Proxy version
Dec 19 09:08:00 enphiniti2020 systemd[1]: Reloading LSB: Squid HTTP Proxy versio
Dec 19 09:08:00 enphiniti2020 squid[1175]:  * Reloading Squid HTTP Proxy configu
Dec 19 09:08:00 enphiniti2020 squid[1175]:    ...done.
Dec 19 09:08:00 enphiniti2020 systemd[1]: Reloaded LSB: Squid HTTP Proxy version
lines 1-20/20 (END)
```

Finally input the IP address and port number of the machine running squid service into clients and your setup is ready to be tested with additional rules.