DITISS QUESTION PAPER
NDC AND PKI – LAB
TOTAL EXAM DURATION – 2 HRS

Total Marks – 60 Total Number of Questions – 3

NDC

Total Marks: 40

QUESTION 1

25 Marks

Set up a Nagios server and monitor the following private services on a remote Linux host:

CPU Usage
- Generate a Warning alert when CPU usage is 70% or higher.
- Generate a Critical alert when CPU usage is 80% or higher.

Virtual Memory
- Generate a Warning alert when virtual memory usage is 70% or higher.
- Generate a Critical alert when virtual memory usage is 90% or higher.

Processes
- Generate a Warning alert when the process count exceeds 50.
- Generate a Critical alert when the process count exceeds 80.

Logical Disk Usage
- Generate a Warning alert when logical disk usage is 70% or higher.
- Generate a Critical alert when logical disk usage is 90% or higher.

Additionally, configure the Nagios server to send email alerts to exam@shuharilabs.local whenever the state of the remote Linux host changes.

Dependencies

- Nagios Core

```
apache2 apache2-utils autoconf gcc libc6 libgd-dev make php python3
tree unzip wget libkrb5-dev openssl libssl-dev
```

- Nagios Plugins

```
automake autotools-dev bc build-essential dc gawk gettext libmcrypt-
dev libnet-snmp-perl libssl-dev snmp
```

- NCPA on Linux Host

```
libsqlite3-0
```

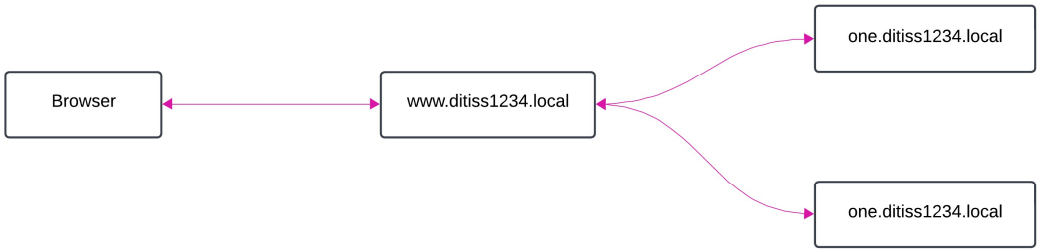
Mark Distribution

- Configure Nagios Server – 2 Marks
- CPU Usage – 2 Marks
- Virtual Memory – 2 Marks
- Processes – 2 Marks
- Logical Disk Usage – 2 Marks
- Email Notification – 15 Marks

QUESTION 2

15 Marks

- Configure load balancing using Squid as per the following network diagram.



- System Details
  - www.ditiss1234.local
    - Running Squid on Port 80
  - one.ditiss1234.local
    - Running Apache on Port 8080
  - two.ditiss1234.local
    - Running Apache on Port 8080
- Note:
  - Replace 1234 in the domain name with the last four digit of your PRN Number.
  - DNS hostnames (Example: https://www.ditiss1234.local) should be used instead of IP address.

PKI

Total Marks: 20

QUESTION 1 - Configure Apache and Set Up Certificates Using XCA

1) Configure Apache on a Debian machine

- Set up a virtual host to serve a website accessible via the URL:
  - https://www.ditiss1234.local
- Note: Replace 1234 with the last four digits of your PRN number.

2) Using XCA, perform the following certificate setup:

- Create a Root Certificate Authority (Root CA)
  - Generate and self-sign a Root CA certificate.
- Create a Subordinate Certificate Authority (Sub CA)
  - Issue the Sub CA certificate using the Root CA.
- Issue a TLS Server Certificate
  - Use the Sub CA to issue a certificate for the domain: www.ditiss1234.local

3) Configure Apache to Use the Issued TLS Certificate

- Place the private key and certificate in appropriate directories.
- Update the Apache virtual host configuration to enable HTTPS using the issued certificate.

4) Test the Setup

- Access the website via a browser using the domain: https://www.ditiss1234.local
- Ensure the browser shows a valid HTTPS connection

- Note:
  - Always use DNS hostnames (e.g., https://www.ditiss1234.local) instead of IP addresses.
  - Ensure /etc/hosts or a local DNS server maps www.ditiss1234.local to your server's IP for testing.