NM-E: AfNOG 2011 – Dar es Salaam, Tanzania

Final Exam

Network Analysis

To find the response time from your machine to a remote machine could you use the **ping** command?

A. Yes
B. No

To find the route that an IP packet follows from your server to a remote server could you use the **netstat** command?

A. Yes
B. No

To show all IPv4 interfaces that are listening on your server what command could you use?

A. lsof -i
B. netstat
C. lsof
D. netstat 127.0.0.1
E. ping localhost

Network Monitoring and Management

Network Monitoring and Management includes the following topics (choose all that apply)

A. Detect problems in the network whey they occur.
B. See long-term patterns and tendencies to help plan for network expansion and increased resources, if necessary.
C. In order to automatically generate tickets when unusual events happen.
D. Create adequately formed relational database tables.
E. Fulfill service levels agreed upon in SLAs.
F. All of the above

Which of the following packages best helps us to detect jitter in network connections?

A. Smokeping
B. Nagios
C. Cacti
D. RANCID
E. NetFlow

Could you measure how much available disk space a remote server has available using Cacti?

A. Yes
B. No

Which of the following software packages could you use to determine if a router is available or down?

A. Cacti
B. Smokeping
C. Nagios

D. Swatch
E. All of the above

What does SNMP mean?

A. Simple Network Management Protocol
B. Service for Network Management Project
C. Simple NetBios Management Protocol
D. Simplified Network Monitoring Protocol
E. Serious New Measuring Project

Is SNMP version 2 protocol encrypted?

A. Yes
B. No

What is a difference between version 2c and version 3 of SNMP:

A. The type of authentication used and the availability of encryption.
B. The information provided by network equipment when questioned via SNMP.
C. None of the above.

In version 3 of SNMP can you protect (pick the best answer):

A. Authentication via user and password using a hash such as MD5 or SHA
B. The returned data via DES encryption
C. Both of the above are possible

IPERF can be used to measure network bandwidth?

A. Yes
B. No

A ticket management system is useful because:

A. It acts like a database of problems that have occurred.
B. It maintains a record of client contact from start to finish.
C. It automatically notifies a group of engineers when a monitoring sysetm has detected a problem.
D. It helps to see patterns to plan for future expansion.
E. All of the above.

One can use Netflow to determine the source of a DDoS attack?

A. Yes
B. No

Netflow only works on Cisco routers

A. Yes
B. No

A “data flow” is defined as a unidirectional sequence of packets that have in common:

A) The same IP source and destination address
The same layer 3 protocol number
The same source and destination port
The same Service Type octect
The same input interface index (ifindex)

➔ Question continues on the following page…

B) Same IP source and destination address
The same layer 3 protocol number
The same source and destination port
The same SNMP protocol version

C) The same Service Type octect
The same input interface index (ifindex)
The same CPU use
The same packet and MTU size

Choose the correct answer above

The RT+Mailgate program allows Cacti, Nagios, Smokeping and other programs to automatically generate tickets:

A. Yes
B. No

Can RANCID specify who committed an error upon making a change to a configuration file for a router?

A. Yes
B. No

Can SWATCH (the Simple log WATCHer) do the following tasks?

A. Notify if a specific user attempts to connect to a router?
B. Determine the processing delay for outoing network packets on a server?
C. Measure the jitter between two network devices on the network?
D. Wake you before someone initiates a DDoS attack against your network?
E. Calculate the maximum bandwidth utilized by one of your clients?

The following 3 lines of configuration for syslog on a router allow what?

```
logging 10.0.0.8
logging facility local6
logging trap errors
```

A. Send messages to 10.0.0.8 of facility local6 with “error” level notifications (level 3)
B. Send messages to 10.0.0.8 of facility local6 with “error” level notifications and lesser priority (level 3 to 7)
C. Send messages to 10.0.0.8 of facility local6 with “error” level notifications and higher priority (level 3 to 0)

What SNMP command would you use to get all the values of the available OIDs for a particularl device that implements SNMP?

A. snmpwalk
B. snmpstatus
C. snmpget
D. snmpset
E. snmptrap