**Assignment 20%. Guidelines. Hardcopy+Softcopy submission. Group of 2 students**

Question No = [((StudentID1 + StudentID2) % 10)]. Extra mark (1 mark out of 20) if partner is from different sex, nationality or race. This is to promote diversity among students.

Due date : 23:59 hour. 16th June 2024.

1. Front cover. Pls print and fill up this form.

|  |  |  |  |
| --- | --- | --- | --- |
| Name1 |  | ID1 |  |
| Name2 |  | ID2 |  |
| Tut Day |  | Tut Time |  |
| Tut Section |  |  |  |
| Ques No |  |  |  |
| Packet No |  | X Value |  |
| MAC Address |  |  |  |
|  |  |  |  |

1. Submit a staple report with
2. No need color printing no need plastic. Just staple will do.
3. Print out the screen shot (output) that prove the username/password/error code etc. Or any text that proves the requirement for the question. Since, most output is text, just cut and paste it on notepad and print out the text inside a box in your word doc as shown in Question 2. Rather than printing the whole screen shot (Which will kill your printer toner).
4. Proof that the install server is operating and configured correct
5. Demo during tutorial hour. Please bring along your hardcopy during demo.

General Grading Policy: Everybody start with full mark. Each mistake there will be mark deduction.

**List of Question.**

1. Setup a Webserver using apache. Create a username and password where someone can login from another machine.

Setup the error log. Download various penetration tools and attack your webserver.

Grading: 1 different HTTP code = 1 mark

Capture the login packet during the login process and show the username and password.(5 marks)

The capture packets must come from the server you configured.

1. Setup a FTP Server where someone can login and upload and download files from another machine. Create a username and password where someone can login from another machine.

Setup the error log. Download various penetration tools and attack your ftp server.

Grading: 1 different FTP error code = 2 mark

Capture the login packet during the login process and show the username and password. (5 marks). The capture packets must come from the server you configured.

1. Configure the multiple layer2 switches in any way you like so that it will pop up some error message in the console. 1 mark for each different error message.

E.g. below

|  |
| --- |
| %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with Switch FastEthernet0/1 (1). |

1. Configure the multiple routers in any way you like so that it will pop up some error message in the console. 1 mark for each different error message.
2. Setup a telnet in a router via GNS so that a user can login via telnet. Capture all the login process and show the username and password. Repeat the process with SSH. The capture packets must come from the router you configured.
3. Setup a TFTP Server which required username and password. Default TFTP Server does not require any username and password. Capture all the packet during the login process. Show the username and password from the packet capture file.
4. Set up a DHCP Server in a router using GNS, capture all the packets when a client PC requesting a DHCP address directly from a router (trace1). And also traffic forwarded via ip helper address (trace2). Show me the packet trace in wireshark.
5. Setup an email client (non http) to retrieve your email from an email POP3/IMAP/SMTP server. Capture the login process and show the username and password. Then, send an email with a simple subject “11111111111111”, textMsg: “22222222222222”. Capture the email message and show ““11111111111111”, textMsg: “22222222222222” in your packet trace.
6. Setup the GNS configuration. Set/Configure a network with a link using RIPv2 and OSPF authentication process between the router interface. Capture all the packet related to RIPv2 authentication and OSPF Authentication.
7. Use Packet tracer to send and receive mail between users. You suppose to generate as many different type of email errors as possible. 1 mark for each different error.