CIS 192 – Practice Test 3 – Spring 2010 Name _____

Each question worth 2 points:

1. The Domain Name System was created from the work led by: (circle best answer)
   a) Andrew Tridgell
   b) Paul Mockapetris
   c) Radia Perlman
   d) Gabriel "Sylar" Gray

2. What is the difference between an iterative DNS query and a recursive DNS query? How could you demonstrate the type of queries (recursive or iterative) done by a DNS client (the resolver) vs. the type of queries done by a DNS server using our class VM's?

   Difference: _____

   _____

   _____

   Demonstrate by: _____

   _____

   _____

   _____

   _____

   _____

3. Locate the "." zone file on Hershey used by the installed DNS software. Look for the root server housed in Japan and operated by WIDE. What is the fully qualified domain name and IP address of that Japanese root server according to Hershey's zone file?

   FQDN: _____

   IP Address: _____

4. The Network File System (NFS): (circle best answer)
   a) Resolves hostnames into IP addresses
   b) Serves web pages on the Internet in a secure manner
   c) Allows file sharing between Linux, Windows and Apple systems
   d) Allows a system to mount a remote directory

5. Which exported directory on Hershey has access restricted to the systems in room 2501 (172.30.1.0/24) and the CIS Lab (172.30.4.0/24)?

_____

6. A firewall was inadvertently clobbered on a CentOS (Red Hat) system preventing remote access to the CUPS service. It now has only the following:

```
[root@arwen ~]# iptables -nL RH-Firewall-1-INPUT --line-numbers
Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source         destination
1    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0      0.0.0.0/0      icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0      0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0      0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0      224.0.0.251    udp dpt:5353
6    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0      state RELATED,ESTABLISHED
7    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:22
8    REJECT     all  --  0.0.0.0/0      0.0.0.0/0      reject-with icmp-host-
prohibited
[root@arwen ~]#
```

What complete iptables command(s) would **insert** the necessary rules for remote access to the CUPS service*?*

_____

_____

7. One of the main goals of the Samba software is to: (circle best answer)
   a) Assign IP addresses to clients wanting to connect to a network
   b) Provide file and printer services in a mixed OS environment
   c) Provide a graphical UI for system administration management tools on HP-UX
   d) Provide encryption for tax returns being filed over serial cable connections

8. What is the name of the printer being shared by the Samba service on Hershey?

_____

9. Your organization has decided to set SELinux to enforcing mode on all systems. This caused access problems to the Samba docs share on a system named Celebrian. Users can no longer access the share with SELinux set to enforcing mode. You review the share information and see the following:

```
From smb.conf:
   [docs]
        comment = Public documents
        path = /var/shares/docs
        guest ok = Yes
```

A long lising of the directory being shared:

```
[root@celebrian var]# ls -ldZ shares/docs
drwxr-xr-x  cis192 users root:object_r:var_t              shares/docs
```

What single command would fix this problem so users could again access the share with SELinux set to enforcing mode*?*

_____

10. Which destination port is used to access a POP server: (circle best answer)
    a) 25
    b) 587
    c) 110
    d) 143

11. What MUA is installed on Hershey?

    _____

12. On Hershey what file would you edit and what line number would you modify to reconfigure sendmail to use a different alias file? (You can assume the make would be done and the service restarted after your changes were made)

    File to edit (use absolute pathname): _____

    Line number to modify: _____

13. The Network Information Service (NIS) software: (circle best answer)
    a) was developed and licensed by Nintendo
    b) is RPC (Remote Procedure Call) based and uses the port mapper (portmap)
    c) is both a user interface and a programming language
    d) was licensed by Microsoft as the underlying engine powering Active Directory

14. What is the name of the NIS domain that Hershey is the NIS server for?

    _____

15. What are the two NIS maps on Hershey that hold the domain wide hosts information for the NIS domain Hershey is serving? (give the absolute filenames)

    _____

    _____

Extra credit

16. (2 point) What command was typed on Arwen (172.30.4.110) that resulted in this Wireshark capture?

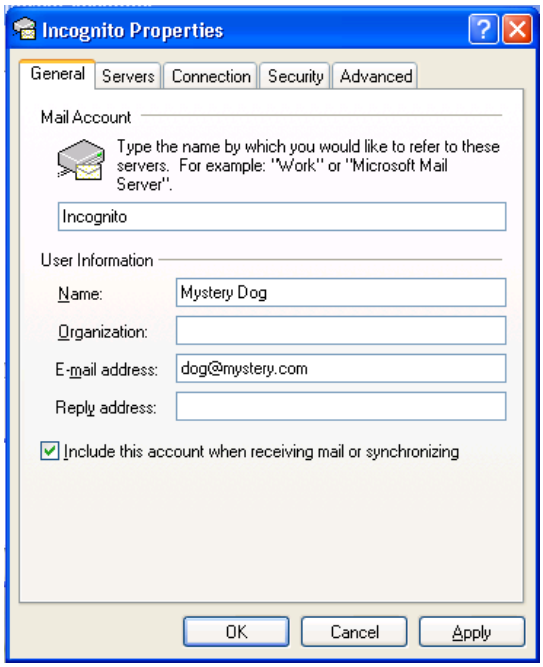
No. .	Time	SIP	SP	DIP	DP	Protocol	Info
90	621.862664	172.30.4.110	59976	207.62.187.54	53	DNS	Standard query A mail.hayrocket.com
91	622.003915	207.62.187.54	53	172.30.4.110	59976	DNS	Standard query response A 208.113.200.50
92	622.005380	172.30.4.110	46219	207.62.187.54	53	DNS	Standard query A mail.hayrocket.com
93	622.132943	207.62.187.54	53	172.30.4.110	46219	DNS	Standard query response A 208.113.200.50
94	622.155975	172.30.4.110	37755	208.113.200.50	143	TCP	37755 > imap [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
95	622.300005	208.113.200.50	143	172.30.4.110	37755	TCP	imap > 37755 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 M
96	622.300054	172.30.4.110	37755	208.113.200.50	143	TCP	37755 > imap [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=12
97	622.367688	208.113.200.50	143	172.30.4.110	37755	IMAP	Response: * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDRE
98	622.367721	172.30.4.110	37755	208.113.200.50	143	TCP	37755 > imap [ACK] Seq=1 Ack=93 Win=5888 Len=0 TSV=1
99	622.422470	208.113.200.50	143	172.30.4.110	37755	IMAP	Response: S SORT QUOTA IDLE STARTTLS] Courier-IMAP r
100	622.422511	172.30.4.110	37755	208.113.200.50	143	TCP	37755 > imap [ACK] Seq=1 Ack=228 Win=6912 Len=0 TSV=

---

17. (1 point) On a CentOS 5.2 system what type of DNS queries are used by the client resolver when attempting to resolve hostnames into IP addresses? (circle one)

    a) Iterative
    b) Recursive
    c) Ad-hoc
    d) Wildcard

18. (4 points) Someone, who is trying to disguise his identity, configures his MUA with fake identification as follows:



This person then sends you an unsolicited email. You view the email and headers as shown below:

Return-Path: <dog@mystery.com>
X-Original-To: rich@hayrocket.com
Delivered-To: rsimms@spaceymail-mx1.g.dreamhost.com
Received: from mail.cruzio.com (mail.cruzio.com [63.249.95.37])
by spaceymail-mx1.g.dreamhost.com (Postfix) with ESMTP id 58307CE77F
for <rich@hayrocket.com>; Sat, 16 May 2009 20:51:06 -0700 (PDT)
Received: from shrekster (dsl-63-249-103-107.dhcp.cruzio.com [63.249.103.107])
by mail.cruzio.com with SMTP id n4H3p3CI050144
for <rich@hayrocket.com>; Sat, 16 May 2009 20:51:05 -0700 (PDT)
Message-ID: <03C11112625C44FEAC1FB1033FF9A951@shrekster>
From: "Mystery Dog" <dog@mystery.com>
To: <rich@hayrocket.com>
Subject: Who am I
Date: Sat, 16 May 2009 20:51:03 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0006_01C9D668.06DF9A70"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5579

By examining the email message headers, fill in the blanks below:

Name of computer used to create the message: _____
IP Address of the computer used to create the message: _____
MUA that created the email (name of product): _____
MTA that sent the email (fully qualified hostname): _____