Lab 05 Template – Ethan Roepke

1. **Screenshot of detailed information about bind9 package in apt**
   (10 points)

```
root@desktop:/home/eroepke# sudo -s
root@desktop:/home/eroepke# apt show bind9
Package: bind9
Version: 1:9.18.12-0ubuntu0.22.04.3
Priority: optional
Section: net
Origin: Ubuntu
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Debian DNS Team <team+dns@tracker.debian.org>
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Installed-Size: 983 kB
Pre-Depends: init-system-helpers (>= 1.54~)
Depends: adduser, bind9-libs (= 1:9.18.12-0ubuntu0.22.04.3), bind9-utils (= 1:9.18.12-0ubuntu0.22.04
.3), debconf | debconf-2.0, dns-root-data, iproute2, lsb-base (>= 3.2-14), netbase, libc6 (>= 2.34),
 libcap2 (>= 1:2.10), libjson-c5 (>= 0.15), liblmdb0 (>= 0.9.7), libmaxminddb0 (>= 1.3.0), libnghttp
2-14 (>= 1.3.0), libssl3 (>= 3.0.0~~alpha1), libuv1 (>= 1.4.2), libxml2 (>= 2.7.4), zlib1g (>= 1:1.1
.4)
Suggests: bind-doc, dnsutils, resolvconf, ufw
Breaks: bind (<< 1:9.13.6~)
Replaces: bind (<< 1:9.13.6~)
Homepage: https://www.isc.org/downloads/bind/
Task: dns-server
Download-Size: 260 kB
APT-Manual-Installed: yes
APT-Sources: http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages
Description: Internet Domain Name Server
 The Berkeley Internet Name Domain (BIND 9) implements an Internet domain
 name server.  BIND 9 is the most widely-used name server software on the
 Internet, and is supported by the Internet Software Consortium, www.isc.org.
 .
 This package provides the server and related configuration files.

N: There is 1 additional record. Please use the '-a' switch to see it
root@desktop:/home/eroepke#
```

2. **Screenshot of debsums command**
   (10 points)

```
root@ns1:/home/eroepke# debsums sl
/usr/games/sl                                                    OK
/usr/share/doc/sl/README                                       FAILED
/usr/share/doc/sl/README.Debian                                  OK
/usr/share/doc/sl/README.jp                                      OK
/usr/share/doc/sl/changelog.Debian.gz                            OK
/usr/share/doc/sl/copyright                                      OK
/usr/share/man/de.UTF-8/man6/LS.6.gz                             OK
/usr/share/man/de.UTF-8/man6/sl.6.gz                             OK
/usr/share/man/de/man6/LS.6.gz                                   OK
/usr/share/man/de/man6/sl.6.gz                                   OK
/usr/share/man/ja.UTF-8/man6/LS.6.gz                             OK
/usr/share/man/ja.UTF-8/man6/sl.6.gz                             OK
/usr/share/man/ja/man6/LS.6.gz                                   OK
/usr/share/man/ja/man6/sl.6.gz                                   OK
/usr/share/man/man6/LS.6.gz                                      OK
/usr/share/man/man6/sl.6.gz                                      OK
root@ns1:/home/eroepke#
```

3. **Screenshots of four successful <u>external</u> forward lookups on your infrastructure**

(5 points)

```
root@ns1:/home/eroepke# dig ns1.student126.230.com +noall +answer
ns1.student126.230.com. 1800    IN      A       105.148.172.200
root@ns1:/home/eroepke# dig www.student126.230.com +noall +answer
www.student126.230.com. 1800    IN      A       105.148.172.202
root@ns1:/home/eroepke# dig mail.student126.230.com +noall +answer
mail.student126.230.com. 1800   IN      A       105.148.172.204
root@ns1:/home/eroepke# dig www2.student126.230.com +noall +answer
www2.student126.230.com. 1800   IN      A       105.148.172.206
root@ns1:/home/eroepke#
```

4. Screenshots of four successful <u>external</u> reverse lookups on your infrastructure

(5 points)

```
root@ns1:/home/eroepke# dig -x 105.148.172.200 +noall +answer
200.172.148.105.in-addr.arpa. 1800 IN   PTR     ns1.student126.230.com.
root@ns1:/home/eroepke# dig -x 105.148.172.202 +noall +answer
202.172.148.105.in-addr.arpa. 1800 IN   PTR     www.student126.230.com.
root@ns1:/home/eroepke# dig -x 105.148.172.204 +noall +answer
204.172.148.105.in-addr.arpa. 1800 IN   PTR     mail.student126.230.com.
root@ns1:/home/eroepke# dig -x 105.148.172.206 +noall +answer
206.172.148.105.in-addr.arpa. 1800 IN   PTR     ww2.student126.230.com.
root@ns1:/home/eroepke# _
```

5. Screenshots of four successful <u>external</u> forward lookups on on another students infrastructure

(5 points)

```
root@ns1:/home/eroepke# dig ns1.student120.230.com +noall +answer
ns1.student120.230.com. 836     IN      A       81.161.135.200
root@ns1:/home/eroepke# dig www.student120.230.com +noall +answer
www.student120.230.com. 238     IN      A       81.161.135.202
root@ns1:/home/eroepke# dig mail.student120.230.com +noall +answer
mail.student120.230.com. 606    IN      A       81.161.135.204
root@ns1:/home/eroepke# dig www2.student120.230.com +noall +answer
www2.student120.230.com. 428    IN      A       81.161.135.206
root@ns1:/home/eroepke# _
```

6. Screenshots of four successful <u>external</u> reverse lookups on another students infrastructure

(5 points)

```
root@ns1:/home/eroepke# dig -x 13.14.1.200 +noall +answer
200.1.14.13.in-addr.arpa. 900   IN      PTR     ns1.student202.230.com.
root@ns1:/home/eroepke# dig -x 13.14.1.202 +noall +answer
202.1.14.13.in-addr.arpa. 900   IN      PTR     www.student202.230.com.
root@ns1:/home/eroepke# dig -x 13.14.1.204 +noall +answer
204.1.14.13.in-addr.arpa. 900   IN      PTR     mail.student202.230.com.
root@ns1:/home/eroepke# dig -x 13.14.1.206 +noall +answer
206.1.14.13.in-addr.arpa. 900   IN      PTR     www2.student202.230.com.
```

7. Screenshots of eight successful <u>internal</u> forward lookups on your personal infrastructure from your ns2

(10 points)

```
root@ns2:/home/eroepke# dig ns2.student126.230.com. +noall +answer
ns2.student126.230.com. 1792    IN      A       192.168.1.200
root@ns2:/home/eroepke# dig desktop1.student126.230.com. +noall +answer
desktop1.student126.230.com. 1800 IN    A       192.168.1.201
root@ns2:/home/eroepke# dig www.student126.230.com. +noall +answer
www.student126.230.com. 1800    IN      A       192.168.1.202
root@ns2:/home/eroepke# dig mail.student126.230.com. +noall +answer
mail.student126.230.com. 1800   IN      A       192.168.1.204
root@ns2:/home/eroepke# dig ldap.student126.230.com. +noall +answer
ldap.student126.230.com. 1800   IN      A       192.168.1.205
root@ns2:/home/eroepke# dig www2.student126.230.com. +noall +answer
www2.student126.230.com. 1800   IN      A       192.168.1.206
root@ns2:/home/eroepke# dig ws.student126.230.com. +noall +answer
ws.student126.230.com.  1800    IN      A       192.168.1.207
root@ns2:/home/eroepke# dig splunk.student126.230.com. +noall +answer
splunk.student126.230.com. 1800 IN      A       192.168.1.208
root@ns2:/home/eroepke# _
```

8. Screenshots of eight successful <u>internal</u> reverse lookups on your personal infrastructure from your ns2

(10 points)

```
root@ns2:/home/eroepke# dig -x 192.168.1.200 +noall +answer
200.1.168.192.in-addr.arpa. 1762 IN     PTR     ns2.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.201 +noall +answer
201.1.168.192.in-addr.arpa. 1768 IN     PTR     desktop1.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.202 +noall +answer
202.1.168.192.in-addr.arpa. 1773 IN     PTR     www.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.204 +noall +answer
204.1.168.192.in-addr.arpa. 1800 IN     PTR     mail.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.205 +noall +answer
205.1.168.192.in-addr.arpa. 1800 IN     PTR     ldap.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.206 +noall +answer
206.1.168.192.in-addr.arpa. 1800 IN     PTR     ww2.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.207 +noall +answer
207.1.168.192.in-addr.arpa. 1800 IN     PTR     ws.student126.230.com.
root@ns2:/home/eroepke# dig -x 192.168.1.208 +noall +answer
208.1.168.192.in-addr.arpa. 1800 IN     PTR     splunk.student126.230.com.
root@ns2:/home/eroepke#
```

9. Take a screenshot of a forward lookup on another student's ldap machine (<u>ldap.studentXX.230.com</u>) from your ns1.

(10 points)

```
root@ns1:/home/eroepke# dig ldap.student26.230.com. +noall +answer
root@ns1:/home/eroepke#
```

10. Did the query in question 6 resolve? Why or why not? Be specific.

(10 points)

When we do a forward lookup on anothers student ldap machine from ns1, we will return nothing. However if we run the command without the +noall +answer, it does not say NXDOMAIN so this indicates that the query did resolve. This would resolve even though the the ldap is specified in ns2, but it runs through firewall with same IP which will allow us to query.

11. Screenshot of Nagios showing ns1 and n2 information all green
(20 points total, 10 points for ns1, 10 points for ns2)

Student 126 (student126)

Host	Services	Actions
desktop1.student126.230.com	desktop1 ssh	
ldap.student126.230.com	ldap Bezos ldap Gates ldap Jobs ldap Musk ldap Zuckerberg ldap service	
mail.student126.230.com	dns MX mail pop secure imap secure imap login secure smtp	
ns1.student126.230.com	dns mail dns ns1 dns www dns www2 reverse dns mail reverse dns ns1 reverse dns www reverse dns www2	
ns2.student126.230.com	dns desktop1 dns ldap dns ws reverse dns desktop1 reverse dns ldap reverse dns ws	
www.student126.230.com	www http www https www login	
www2.student126.230.com	www2 django www2 ssh	