Linux Network Systems Administration - Commands and Expected Outputs

# 1. Aspect - Description

|  |
| --- |
| **Command**  Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only) |
| **Expected Output**  Requirement (Measurement Only) |

# 21. IP Fowarding: IPv4 & IPv6 forwarding is enabled

|  |
| --- |
| **Command**  $ sysctl -p |
| **Expected Output**  > net.ipv4.ip\_forward = 1 > net.ipv6.conf.all.forwarding = 1 |

# 22. Firewall: Traffic to WAN uses masquerade NAT

|  |
| --- |
| **Command**  $ timeout 2 bash -c "echo -e '\x1dclose\x0d' | telnet 1.1.1.20 22" |
| **Expected Output**  > Trying 1.1.1.20... Connected to 1.1.1.20. Escape character is '^]'.  telnet> close Connection closed. |

# 26. Firewall: Firewall rules are well designed

|  |
| --- |
| **Command**  nft list ruleset |
| **Expected Output**  table ip nat {  chain prerouting {  type nat hook prerouting priority dstnat; policy accept;  iif "ens192" tcp dport 80 dnat to 10.1.20.20  iif "ens192" tcp dport 443 dnat to 10.1.20.20  iif "ens192" tcp dport 53 dnat to 10.1.20.20  iif "ens192" udp dport 53 dnat to 10.1.20.20  iifname { "wg0", "ens224" } tcp dport 80 redirect to :82  }   chain postrouting {  type nat hook postrouting priority srcnat; policy accept;  oif "ens192" masquerade  } } table ip filter {  chain input {  type filter hook input priority filter; policy drop;  iif "lo" accept  ct state established,related accept  iifname { "wg0", "ens224", "ens256" } accept  iifname "ens192" udp dport 1500 accept  icmp type { echo-reply, echo-request } limit rate 4/second accept  iifname "ens161" accept  }   chain forward {  type filter hook forward priority filter; policy drop;  ct state established,related accept  iifname { "ens224", "ens256" } oif "ens192" accept  iifname { "wg0", "ens224" } oif "ens256" accept  iifname "wg0" oif "ens224" accept  ip saddr 10.1.20.10 ip daddr 10.1.10.10 tcp dport 389 accept  ip daddr 10.1.20.20 tcp dport { 80, 443 } accept  ip daddr 10.1.20.20 tcp dport 53 accept  ip daddr 10.1.20.20 udp dport 53 accept  }   chain output {  type filter hook output priority filter; policy accept;  } } table ip6 nat {  chain prerouting {  type nat hook prerouting priority dstnat; policy accept;  iifname { "wg0", "ens224" } tcp dport 80 redirect to :82  } } table ip6 filter {  chain input {  type filter hook input priority filter; policy drop;  iif "lo" accept  ct state established,related accept  iifname { "wg0", "ens224", "ens256" } accept  iifname "wg0" oif "ens224" accept  ip6 daddr 2001:db8:1111::1 udp dport 1500 accept  ip6 daddr 2001:db8:1001:10::1 tcp dport 82 accept  }   chain forward {  type filter hook forward priority filter; policy drop;  ct state established,related accept  iifname { "wg0", "ens224", "ens256" } oif "ens192" accept  iifname { "wg0", "ens224" } oif "ens256" accept  iifname "wg0" oif "ens224" accept  ip6 daddr 2001:db8:1001:20::20 tcp dport { 80, 443 } accept  ip6 daddr 2001:db8:1001:20::20 tcp dport 53 accept  ip6 daddr 2001:db8:1001:20::20 udp dport 53 accept  }   chain output {  type filter hook output priority filter; policy accept;  } } |

# 29. Backup: /dev/sdb has been added to /etc/fstab

|  |
| --- |
| **Command**  $ cat /etc/fstab |
| **Expected Output**  > # /etc/fstab: static file system information. # # Use 'blkid' to print the universally unique identifier for a # device; this may be used with UUID= as a more robust way to name devices # that works even if disks are added and removed. See fstab(5). # # systemd generates mount units based on this file, see systemd.mount(5). # Please run 'systemctl daemon-reload' after making changes here. # # <file system> <mount point> <type> <options> <dump> <pass> /dev/mapper/debian--vg-root / ext4 errors=remount-ro 0 1 # /boot was on /dev/sda2 during installation UUID=567cbd87-0262-4e06-b19b-68a69dd383fc /boot ext2 defaults 0 2 /dev/mapper/debian--vg-swap\_1 none swap sw 0 0 /dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0 /dev/sr1 /media/cdrom1 udf,iso9660 user,noauto 0 0 /dev/sr2 /media/cdrom2 udf,iso9660 user,noauto 0 0 /dev/sr3 /media/cdrom3 udf,iso9660 user,noauto 0 0 /dev/sr4 /media/cdrom4 udf,iso9660 user,noauto 0 0 UUID=485f4ce8-1f70-4c31-a2ab-4a5fb9602f56 /opt/backup ext4 defaults 0 0 |

# 30. SSH: Openssh option TrustedUserCAKeys is populated

|  |
| --- |
| **Command**  $ sshd -T |
| **Expected Output**  > trustedusercakeys /etc/ssh/ca.key.pub |

# 31. SSH: user root from ha-prx01 can ssh as root using the signed key

|  |
| --- |
| **Command**  $ timeout 2 bash -c 'ssh -vv -o StrictHostKeyChecking=no root@10.1.20.10 "lsb\_release -is" 2>&1 | grep "Server accepts"' |
| **Expected Output**  > debug1: Server accepts key: /root/.ssh/root.key-cert.pub ED25519-CERT SHA256:utUmDuUa+2a+I3G/lqCBsMM+MHa9LCqXMrh0GFH34Yg explicit |

# 32. Backup: Backup script style

|  |
| --- |
| **Command**  $ rm -rf /opt/backup/\* ; bash /opt/backup.sh $ find /opt/backup/ -name dovecot.conf -o -name main.cf -o -name dovecot.index\* |
| **Expected Output**  > /opt/backup/mailboxes/mailboxes/jamie/Maildir/dovecot.index.cache /opt/backup/dovecot/dovecot/dovecot.conf /opt/backup/postfix/postfix/main.cf |

# 46. Web Server: main.html is served when the root page is opened

|  |
| --- |
| **Command**  $ curl -s --connect-timeout 2 http://127.0.0.1/ 2>&1 |
| **Expected Output**  web01 print the following output: > ID=7ecb4e033421b96f88e2111fe97cdad4ddceacc6 |

# 47. Web Server: 404.html is served when an invalid path is given

|  |
| --- |
| **Command**  $ curl -s --connect-timeout 2 http://127.0.0.1/loremipsum 2>&1 |
| **Expected Output**  web01 print the following output: > Sorry, but something went wrong |

# 55. Ansible can connect to web02

|  |
| --- |
| **Command**  cd /opt/ansible/ && timeout 10 ansible -m ping all |
| **Expected Output**  web02 | SUCCESS => {  "ansible\_facts": {  "discovered\_interpreter\_python": "/usr/bin/python3"  },  "changed": false,  "ping": "pong" } |

# 56. Webserver serves required web pages (index, 404, whoami)

|  |
| --- |
| **Command**  $ curl -s --connect-timeout 2 http://127.0.0.1/ 2>&1 $ curl -s --connect-timeout 2 http://127.0.0.1/invalid 2>&1 $ curl -s --connect-timeout 2 http://127.0.0.1/whoami 2>&1 |
| **Expected Output**  The output:from web02 contains following strings: > ID=7ecb4e033421b96f88e2111fe97cdad4ddceacc6 > Sorry, but something went wrong > web02 |