Team –

a. Suraj Bhatia
b. Soumya Mohanty

1. Why were the Linux accounts you created added to the `sudo` group?

   Groups are used to give or restrict access to files, folders and privileges or permissions to a certain set of users.

   sudo stands for super user do. The sudo command provides a mechanism for granting administrator privileges which are ordinarily only available to root users, to normal users. A root user on a Linux system is the user with the maximum privileges by default. The root user privileges act as an extra layer of security.

   By adding a new user to the sudo group we can give the user administrator privileges without having to modify the sudoers file. The new user will now have the privileges of the root user while running the commands.

2. What is the purpose of the `sudo(8)` command? What advantages does it have over the `su(1)` command?

   The purpose of the sudo command is to grant administrative privileges which are ordinarily only available to the root user, to a normal user.

   While sudo runs a single command with root privileges, su launches another shell instance with privileges of the intended user. Both these commands are used to grant root privileges to the user in different manners.

   Advantages of sudo over su are:

   a. When sudo command is used it asks for the password of the current user account, on the other hand su forces one to share the root password or the password of any other user account (to which the current user intends to switch to).
   b. Also, sudo doesn't activate the root shell and runs a single command, whereas the su command starts a new shell instance, this is advantageous only if we have multiple commands to run, else is a security threat.
   c. The use of sudo command also adds records to a log file(/var/log/auth.log), so if some malicious activity is noticed it can be easily investigated.

3. What it the purpose of the option `-sha256` when generating the certificate csr.

   OpenSSL is a general purpose cryptography library that provides an open source implementation of the Secure Socket Layer(SSL) and Transport Layer Security (TSL).

   We used OpenSSL to generate an RSA private key and a Certificate Signing Request (CSR). In a public key infrastructure (PKI) system a CSR must be created before requesting or purchasing a SSL certificate.

   Users first need to generate a key and then the CSR which they need to submit to the Certificate Authority (CA). The CA can then issue the SSL certificate (CRT).

When we created the CSR we specified the option -sha256. This option specifies that we wish to use the Secure Hash Algorithm (SHA-2) with a digest (hash value) of 256 bits. SHA-256 is a hash function computed using 32-bit words.

A hash function or digest such as this is used to convert an input of arbitrary length into an output of fixed length, which is known as the hash of the input. This output can be used in place of the original input.

This is used so that given a message digest, it is hard to find an input that has the same message digest. It should also be hard to find two inputs that have the same message digest.

The -sha256 option used in the command while creating the Certificate Signing Request accomplishes these tasks for us.

4. What are the network settings for the Linux router and the Windows server?

   Linux VM acting as a NAT router has two interfaces –

   a. eth0 192.168.254.15 which is a Bridged adapter

   b. eth1 10.0.100.1 which is NAT adapter

```
team@nslabu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ac:61:59
          inet addr:192.168.254.15  Bcast:192.168.254.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feac:6159/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:342751 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38895 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:326526167 (326.5 MB)  TX bytes:2725435 (2.7 MB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:b0:56:6f
          inet addr:10.0.100.1  Bcast:10.0.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb0:566f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:320205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1743317 (1.7 MB)  TX bytes:306304431 (306.3 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 7e:e5:a9:05:f5:b7
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::7ce5:a9ff:fe05:f5b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:345 errors:0 dropped:0 overruns:0 frame:0
          TX packets:329 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:76229 (76.2 KB)  TX bytes:25305 (25.3 KB)
```

The default routes for the Linux VM are as shown below -

```
team@nslabu:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.254.2   0.0.0.0         UG    0      0        0 eth0
10.0.0.0        *               255.255.255.0   U     0      0        0 tap0
10.0.100.0      *               255.255.255.0   U     0      0        0 eth1
192.168.254.0   *               255.255.255.0   U     0      0        0 eth0
team@nslabu:~$
```

For the Windows VM, we have only one interface for which the default gateway is eth1 of Linux VM -

Properties

Name:	Ethernet
Description:	Intel(R) PRO/1000 MT Desktop Adapter
Physical address (MAC):	08:00:27:ed:60:e4
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	1000/1000 (Mbps)
DHCP enabled:	No
IPv4 address:	10.0.100.2/24
IPv6 address:	
Default gateway:	10.0.100.1
DNS servers:	10.0.0.254, 8.8.8.8
DNS domain name:	
DNS connection suffix:	
DNS search suffix list:	
Network name:	Network 2
Network category:	Public
Connectivity (IPv4/IPv6):	Connected to Internet / Connected to unknown network

5. Provide the output of your manual run of openvpn, the IP address of strawman.nslab, and the ping output.

OpenVPN was run by the following command –

$ sudo openvpn –config /etc/openvpn/openvpn.conf

```
Fri Sep 22 00:44:21 2017 library versions: OpenSSL 1.0.2g  1 Mar 2016, LZO 2.08
Fri Sep 22 00:44:21 2017 WARNING: No server certificate verification method has been enabled.  See http://openvpn.net/howto.h
tml#mitm for more info.
Fri Sep 22 00:44:21 2017 Socket Buffers: R=[163840->163840] S=[163840->163840]
Fri Sep 22 00:44:21 2017 UDPv4 link local: [undef]
Fri Sep 22 00:44:21 2017 UDPv4 link remote: [AF_INET]129.10.115.58:1195
Fri Sep 22 00:44:22 2017 TLS: Initial packet from [AF_INET]129.10.115.58:1195, sid=a24225e5 2e0d8608
Fri Sep 22 00:44:22 2017 VERIFY OK: depth=1, C=US, ST=MA, L=Boston, O=NEU, CN=chimera CA, emailAddress=amirali@ccs.neu.edu
Fri Sep 22 00:44:22 2017 VERIFY OK: depth=0, C=US, ST=MA, O=NEU, CN=hercules.ccs.neu.edu, emailAddress=amirali@ccs.neu.edu
Fri Sep 22 00:44:22 2017 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Sep 22 00:44:22 2017 WARNING: this cipher's block size is less than 128 bit (64 bit).  Consider using a --cipher with a l
arger block size.
Fri Sep 22 00:44:22 2017 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Sep 22 00:44:22 2017 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Fri Sep 22 00:44:22 2017 WARNING: this cipher's block size is less than 128 bit (64 bit).  Consider using a --cipher with a l
arger block size.
Fri Sep 22 00:44:22 2017 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Fri Sep 22 00:44:22 2017 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Fri Sep 22 00:44:22 2017 [hercules.ccs.neu.edu] Peer Connection Initiated with [AF_INET]129.10.115.58:1195
Fri Sep 22 00:44:24 2017 SENT CONTROL [hercules.ccs.neu.edu]: 'PUSH_REQUEST' (status=1)
Fri Sep 22 00:44:24 2017 PUSH: Received control message: 'PUSH_REPLY,dhcp-option DNS 10.0.0.254,route-gateway 10.0.0.254,ping
 10,ping-restart 120,ifconfig 10.0.0.2 255.255.255.0'
Fri Sep 22 00:44:24 2017 OPTIONS IMPORT: timers and/or timeouts modified
Fri Sep 22 00:44:24 2017 OPTIONS IMPORT: --ifconfig/up options modified
Fri Sep 22 00:44:24 2017 OPTIONS IMPORT: route-related options modified
Fri Sep 22 00:44:24 2017 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Sep 22 00:44:24 2017 TUN/TAP device tap0 opened
Fri Sep 22 00:44:24 2017 TUN/TAP TX queue length set to 100
Fri Sep 22 00:44:24 2017 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Fri Sep 22 00:44:24 2017 /sbin/ip link set dev tap0 up mtu 1500
Fri Sep 22 00:44:24 2017 /sbin/ip addr add dev tap0 10.0.0.2/24 broadcast 10.0.0.255
Fri Sep 22 00:44:24 2017 Initialization Sequence Completed
```

For finding the hostname-IP address translation of strawman.nslab, we found out the DNS server in the network that will provide us with this information. The IP address of the DNS server we get is 10.0.0.254

```
team@nslabu:~$ nmcli dev show | grep DNS
IP4.DNS[1]:                             10.0.0.254
IP4.DNS[2]:                             8.8.8.8
IP4.DNS[3]:                             8.8.4.4
IP4.DNS[4]:                             192.168.77.2
IP4.DNS[1]:                             10.0.0.254
IP4.DNS[2]:                             8.8.8.8
IP4.DNS[3]:                             8.8.4.4
team@nslabu:~$
```

Then we execute a dig command asking this DNS server the IP address for strawman.nslab. We get the below result with the IP address as 10.0.0.32.

We also ping the machine to confirm our openvpn connection has been established.

```
team@nslabu:~$ sudo dig @10.0.0.254 strawman.nslab

; <<>> DiG 9.10.3-P4-Ubuntu <<>> @10.0.0.254 strawman.nslab
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23654
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;strawman.nslab.                        IN      A

;; ANSWER SECTION:
strawman.nslab.         86400   IN      A       10.0.0.32

;; AUTHORITY SECTION:
nslab.                  86400   IN      NS      paiute.nslab.
nslab.                  86400   IN      NS      wishram.nslab.

;; ADDITIONAL SECTION:
paiute.nslab.           86400   IN      A       10.0.0.254
wishram.nslab.          86400   IN      A       10.0.0.253

;; Query time: 20 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Sep 19 13:55:10 EDT 2017
;; MSG SIZE  rcvd: 134

team@nslabu:~$ ping 10.0.0.32
PING 10.0.0.32 (10.0.0.32) 56(84) bytes of data.
64 bytes from 10.0.0.32: icmp_seq=1 ttl=64 time=19.1 ms
64 bytes from 10.0.0.32: icmp_seq=2 ttl=64 time=13.4 ms
64 bytes from 10.0.0.32: icmp_seq=3 ttl=64 time=11.7 ms
64 bytes from 10.0.0.32: icmp_seq=4 ttl=64 time=12.0 ms
^C
--- 10.0.0.32 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 11.790/14.103/19.188/3.003 ms
team@nslabu:~$
```

The other way was using nmap, we get a list of machines connected to the 10.0.0.0/24 network -

```
team@nslabu:~$ nmap 10.0.0.0/24

Starting Nmap 5.50 ( http://nmap.org ) at 2017-09-20 19:38 EDT
Nmap scan report for 10.0.0.1
Host is up (0.00014s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
110/tcp  open  pop3
143/tcp  open  imap
993/tcp  open  imaps
995/tcp  open  pop3s
4000/tcp open  remoteanything

Nmap scan report for 10.0.0.32
Host is up (0.069s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap scan report for 10.0.0.113
Host is up (0.067s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS

Nmap scan report for 10.0.0.124
Host is up (0.069s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap scan report for 10.0.0.252
Host is up (0.068s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
6000/tcp open  X11

Nmap done: 256 IP addresses (5 hosts up) scanned in 4.54 seconds
```

6. When running the command `ping google.com`, explain how the ICMP packet flows. State all the links/interfaces travelled by this packet when the command is run on (1) the Linux VM, (2) the Windows VM.

   For Linux machine that is acting as a NAT router, we have two interfaces –

   a. eth0 192.168.254.15 which is a Bridged adapter

   b. eth1 10.0.100.1 which is NAT adapter

   The interface eth0 is facing the public internet while eth1 is connected to the internal network which has the Windows VM.

   So when we do a ping from the Linux VM, the ping is associated from eth0 and the packet is sent through the default gateway of 192.168.254.2.

```
team@nslabu:~$ traceroute google.com
traceroute to google.com (172.217.10.110), 30 hops max, 60 byte packets
 1  192.168.254.2 (192.168.254.2)  0.432 ms  0.223 ms  0.414 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

   As for the Windows VM, there is only one interface 10.0.100.2 for which the default gateway is Linux VM interface eth1 10.0.100.1. When a ping command is run, the packets are forwarded to this interface, which are then forwarded to default gateway 192.168.254.2 through eth0.

```
PS C:\Users\Administrator> ping 10.0.100.1

Pinging 10.0.100.1 with 32 bytes of data:
Reply from 10.0.100.1: bytes=32 time<1ms TTL=64
Reply from 10.0.100.1: bytes=32 time=1ms TTL=64
Reply from 10.0.100.1: bytes=32 time=1ms TTL=64
Reply from 10.0.100.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator> TRACERT.EXE google.com

Tracing route to google.com [172.217.10.110]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.0.100.1
  2     1 ms     1 ms     1 ms  192.168.254.2
  3     *        *        *     Request timed out.
  4    24 ms    16 ms    15 ms  96.120.68.73
  5   217 ms    14 ms    14 ms  96.108.155.13
  6    20 ms    16 ms    16 ms  be-98-ar01.needham.ma.boston.comcast.net [68.85.106.13]
  7   308 ms    23 ms    27 ms  be-7015-cr02.newyork.ny.ibone.comcast.net [68.86.90.217]
  8   148 ms    25 ms    22 ms  hu-0-12-0-6-pe02.111eighthave.ny.ibone.comcast.net [68.86.87.246]
  9   139 ms    29 ms    21 ms  50.248.116.186
 10     *        *        *     Request timed out.
 11    36 ms    26 ms    24 ms  216.239.62.146
 12   226 ms    23 ms    22 ms  216.239.62.159
 13   117 ms    23 ms    21 ms  lga34s15-in-f14.1e100.net [172.217.10.110]

Trace complete.
PS C:\Users\Administrator>
```