Network Administration/System Administration (NTU CSIE, Spring 2024) Homework #0

B12902110 呂承諺

Network Administration

1 True/False

1. **True**. A VPN creates an encrypted tunnel between you and the VPN service provider. All of your internet traffic is routed to the VPN server first and then reach other sites, so it looks like you're connected to the internet from the VPN server. Sites will see the VPN server's IP address instead.

   References:

   - What is a VPN and Can it Hide My IP Address? | McAfee

2. **False**. With techniques such as port forwarding or protocols such as the Port Control Protocol (PCP), and proper support from the NAT device, we can still actively initiate connections to internal devices behind the NAT.

   References:

   - Network address translation - Wikipedia
   - NAT traversal - Wikipedia
   - Port Control Protocol - Wikipedia
   - Port forwarding - Wikipedia

3. **False**. Software such as pfSense can be used to implement gateways. Besides routing packets, a gateway can also provide services like NAT or DHCP. A gateway usually connects LAN and WAN, and it ensures that data are correctly transmitted.

   References:

   - pfSense - Wikipedia
   - Gateway (telecommunications) - Wikipedia

4. **True**. This site uses HTTP instead of HTTPS, so data is transmitted in plain text, including the submitted HTML form.

   References:

   - HTTP - Wikipedia
   - HTML form - Wikipedia

5. **False**. It may be possible without DNS, but it is impossible to directly connect to the server without NAT because the client only has a private IP, which is not in the same subnet as the server.

6. **False**. A DDoS attack is an attempt to kill a service by sending a lot of traffic to it. It could be defended by firewalls or traffic monitoring.

   References:

   - What is a distributed denial-of-service (DDoS) attack? | Cloudflare
   - Denial-of-service attack - Wikipedia

7. **False**. Triple DES is an counterexample. It has a mode that uses 168-bit keys, but due to the meet-in-the-middle attack, it only has 112 bits worth of effective security.

   References:

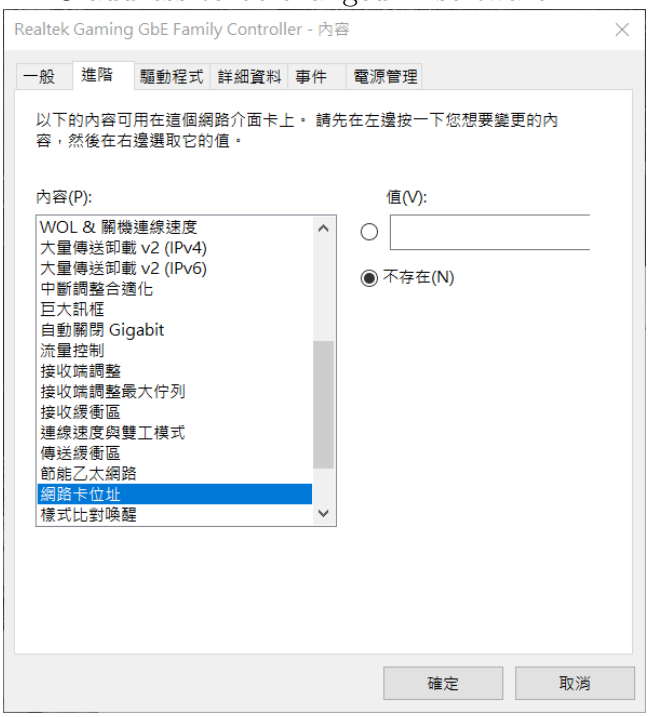
   - Triple DES - Wikipedia
   - My friend 黃昱翔 gave me an idea of this.

2 ChatGPT

1. Only partially correct.

   (a) Every network interface controller (NIC) has a hardcoded MAC address that cannot be changed, this is true.

   (b) Although the hardware MAC address cannot be changed, many drivers allow the MAC address to be changed in software.



   (c) We could in theory completely rely on MAC addresses to identify devices on the internet, as a typical MAC address contains 48 bits, making random clashes extremely rare. However, this could reduce configurability. For example, we now use IP addresses and subnet masks to conveniently configure subnets, but if we use MAC addresses instead, we would have to maintain an exhaustive list of MAC addresses for every device in the subnet.

(d) Besides, if a "device" has multiple NICs installed, it can have multiple MAC addresses, one per NIC.

References:

- MAC spoofing - Wikipedia
- Can you change the MAC address of a network card? - Quora
- MAC address - Wikipedia

2. Mostly incorrect at first, totally incorrect at the end.

   - 4G is a cellular network technology *generation*, consisting of various standards. In these standards, some specify the frequency bands to be used, and others define thresholds for data speeds. So we wouldn't say 4G is a data speed nor say it's a frequency.
   - We usually use c to denote the speed of light in vacuum.

   References:

   - 4G - Wikipedia
   - LTE frequency bands - Wikipedia
   - Speed of light - Wikipedia

3. Mostly correct.

   (a) It's true that IPv4 uses 32 bits to represent an address, and that it has already faced the problem of address exhaustion. However, this means that all blocks of available IPv4 addresses have been assigned, and there may still be unused addresses in many of the blocks. Plus, we can recycle unused addresses and reuse them, so its not mandatory for new devices to use IPv6.

   (b) There are still plenty of services that only support IPv4, so new devices still need IPv4 connectivity in order to access those services.

   (c) Another thing is that IPv4 is usually more convenient to configure and sufficient in LANs. Anyway, IPv4 is still and will continue to be widely in use.

   (d) It's correct that IPv6 uses 128 bits to represent an address.

   References:

   - Internet Protocol version 4 - Wikipedia
   - IPv4 address exhaustion - Wikipedia
   - IPv6 - Wikipedia

3 Short Answer

1. (a) **DHCP**: Dynamic Host Configuration Protocol. An application-layer protocol that can automatically assign network configurations, such as IP addresses, subnet masks, and default gateways, to devices.

   (b) **VLAN**: Virtual Local Area Network. A technology that groups devices so that they appear as if they are in their own network segment, even if they're connected to the same physical network. Can enhance performance or security.

(c) **Switch**: A network device that (usually) operates on the data link layer. It connects devices together and transmit network packets to the correct device by identifying the packet's destination MAC address.

(d) **Broadcast storm**: Broadcasting means sending a packet that will be received by every device in a given network. A broadcast strom happens when too many broadcast or multicast packets are flooding the network. This can happen if a switching loop exists in the network.

References:

- Dynamic Host Configuration Protocol - Wikipedia
- VLAN - Wikipedia
- Network switch - Wikipedia
- Broadcast storm - Wikipedia
- Broadcasting (networking) - Wikipedia
- Switching loop - Wikipedia

2. These are all valid IPv4 addresses but reserved for special purposes.

   (a) Address block `0.0.0.0/8` is reserved for *this network* in software.

   (b) The address `::1` is reserved for the *loopback address*, which loops any traffic back to the host itself.

   (c) Address block `2001:db8::/32` is reserved for use in documentation and example code.

   References:

   - Reserved IP addresses - Wikipedia

3. The 5 layers from top to bottom are:

   (a) **Application layer**: This layer includes protocols that applications use to exchange data between each other, such as SSH and HTTPS.

   (b) **Transport layer**: This layer determines how to devices communicate and transfer data. TCP and UDP are the two primary protocols here.

   (c) **Internet layer**: This layer is responsible for routing network packets across networks. IPv4 and IPv6 are protocols of this layer.

   (d) **Link layer**: This layer includes protocols that operate on nodes of the local network segment (link), such as the Address Resolution Protocol (ARP). Network traffic in this layer is not routed to other networks.

   (e) **Physical layer**: This layer handles the physical transmission of data through a medium, including electrical and mechanical specifications, such as 1000BASE-T and the physical part of IEEE 802.11.

   References:

   - TCP/IP protocols - IBM Documentation
   - Internet protocol suite - Wikipedia
   - Transport layer - Wikipedia

- Internet layer - Wikipedia
- Link layer - Wikipedia
- Physical layer - Wikipedia

4. (a) **TCP**: An internet protocol in the transport layer that transfers data reliably and in order. A connection has to be established between the client and the server before data transmission can begin. It utilizes acknowledgements, data retransmission, etc. to ensure correctness of data.

   (b) **UDP**: An internet protocol in the transport layer that transfers data less reliably. It is connectionless and doesn't guarantee correctness of data.

   (c) TCP:

   - Advantages: More reliable.
   - Disadvantages: Higher latency.
   - Example: When we *SSH* into CSIE's workstation.

   UDP:

   - Advantages: Lower latency, useful for time-critical applications.
   - Disadvantage: Less reliable.
   - Example: When we perform a *DNS* query.

   References:

   - Transmission Control Protocol - Wikipedia
   - User Datagram Protocol - Wikipedia
   - TCP vs UDP: Differences Between TCP & UDP Protocols | Avast

5. (a) **LDAP/LDAPS**: Lightweight Directory Access Protocol/LDAP over SSL

   - Manage directory information services over IP.
   - A directory contains information of objects like users, groups, and devices. A common use of this protocol is maintaining a centralized storage of user credentials.
   - LDAPS is essentially LDAP with encryption.
   - Default port: 389 for LDAP, 636 for LDAPS.

   (b) **SMTP**: Simple Mail Transfer Protocol

   - Send emails over the internet.
   - Default port: 465, 587, or traditionally 25.

   (c) **SNMP**: Simple Network Management Protocol

   - Monitor and manage devices in an IP network.
   - Gather system status information and configure settings remotely.
   - Default port: 161 and 162.

   (d) **HTTP/HTTPS**: Hypertext Transfer Protocol/HTTP over SSL

   - Transfer hypermedia resources, such as HTML.
   - HTTPS is HTTP with encryption.
   - Default port: 80 for HTTP, 443 for HTTPS.

   References:

- Lightweight Directory Access Protocol - Wikipedia
- Simple Mail Transfer Protocol - Wikipedia
- Simple Network Management Protocol - Wikipedia
- HTTP | MDN
- HTTPS - Wikipedia

4 Command Line Utilities

1. To find the IP addresses of the domain names, we run `dig DOMAIN_NAME` to perform DNS queries.

   (a) www.ntu.etu.tw → 140.112.8.116

   (b) csie.ntu.edu.tw → 140.112.30.26

   To find the domain names IP addresses, we run `dig -x ADDRESS` to perform reverse DNS lookup queries.

   (a) 140.112.30.25 → printing.csie.ntu.edu.tw

   (b) 140.112.161.176 → if176.aca.ntu.edu.tw

   References:

   - linux - What's the reverse DNS command line utility? - Server Fault
   - man page of `dig`

2. NTU VPN

   (a) 140.112.77.110. We can see this in the VPN client software or Windows control panel details.

   (b) We use `nslookup` to query IPs and use `tracert` to find out the route.
   Before connecting to VPN (using Wi-Fi ntu_peap):

   - DNS server IP: 140.112.254.4
   - Route to DNS server: refer to the figure below

```
C:\Users\user>nslookup csie.ntu.edu.tw
伺服器:  dns.ntu.edu.tw
Address:  140.112.254.4

未經授權的回答:
名稱:    csie.ntu.edu.tw
Address:  140.112.30.26


C:\Users\user>tracert dns.ntu.edu.tw

在上限 30 個躍點上
追蹤 dns.ntu.edu.tw [140.112.254.4] 的路由:

  1     7 ms     4 ms     3 ms  10.99.0.253
  2     1 ms     1 ms     1 ms  192.168.203.251
  3     2 ms     2 ms     2 ms  wl127.cc.ntu.edu.tw [140.112.4.254]
  4     1 ms     1 ms     1 ms  140.112.0.170
  5     2 ms     1 ms     1 ms  140.112.254.28
  6     2 ms     2 ms     3 ms  dns.ntu.edu.tw [140.112.254.4]

追蹤完成。
```

After connecting to VPN:

- DNS server IP: 140.112.254.4
- Route to DNS server: refer to the figure below

```
C:\Users\user>nslookup csie.ntu.edu.tw
伺服器:  dns.ntu.edu.tw
Address:  140.112.254.4

未經授權的回答:
名稱:    csie.ntu.edu.tw
Address:  140.112.30.26


C:\Users\user>tracert dns.ntu.edu.tw

在上限 30 個躍點上
追蹤 dns.ntu.edu.tw [140.112.254.4] 的路由:

  1     3 ms     1 ms     1 ms  10.200.200.200
  2     2 ms     1 ms     1 ms  ip4-126.vpn.ntu.edu.tw [140.112.4.126]
  3     1 ms     1 ms     1 ms  140.112.0.210
  4     3 ms     1 ms     2 ms  140.112.254.28
  5     2 ms     1 ms     3 ms  dns.ntu.edu.tw [140.112.254.4]

追蹤完成。
```

(c) Run `nmap 140.112.30.158 -p-` to scan for all open ports.

```
C:\Users\user>nmap 140.112.30.158 -p-
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-22 05:10 台北標準時間
Nmap scan report for 140.112.30.158
Host is up (0.000071s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE    SERVICE
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
4444/tcp  filtered krb524
6667/tcp  filtered irc
18763/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 5.45 seconds
```

Run `nc 140.112.30.158 18763` to see the message.

```
gpwaob92679@HP-LAPTOP: /mnt/c/Users/user
$ nc 140.112.30.158 18763
NASA{P4-3_Y0u_Found_M3!}
```

References:

- How to Check (Scan) for Open Ports in Linux | Linuxize

System Administration

1 Super Auto Penguin!

Steps

1. Login with the provided credentials.
2. Run `sudo ./p1-checker`. We can see the flag in standard output.

Flag `NASA{P1_I_4m_r00t!}`

2 Read the manual plz

Steps

1. Run `man pacman`.
2. We discover the flag at the end of the first paragraph of the *DESCRIPTION* section.

Flag `NASA{P2_P4CM4N_1$_TH3_M4N}`

3 Telepathy

Steps

1. Run `sudo pacman -Sy openssh`. The package `openssh-9.6p1-1` is updated to `openssh-9.6p1-3`.

```
[nasa-intern@tux-penguin ~]$ pacman -Q openssh
openssh 9.6p1-1
[nasa-intern@tux-penguin ~]$ sudo pacman -Sy openssh
:: Synchronizing package databases...
 core                                          129.5 KiB   563 KiB/s 00:00 [#######################################################] 100%
 extra                                           8.3 MiB  2.73 MiB/s 00:03 [#######################################################] 100%
resolving dependencies...
looking for conflicting packages...

Packages (1) openssh-9.6p1-3

Total Download Size:   1.12 MiB
Total Installed Size:  5.50 MiB
Net Upgrade Size:      0.55 MiB

:: Proceed with installation? [Y/n]
:: Retrieving packages...
 openssh-9.6p1-3-x86_64                       1148.7 KiB  3.09 MiB/s 00:00 [#######################################################] 100%
(1/1) checking keys in keyring                                            [#######################################################] 100%
(1/1) checking package integrity                                          [#######################################################] 100%
(1/1) loading package files                                               [#######################################################] 100%
(1/1) checking for file conflicts                                         [#######################################################] 100%
(1/1) checking available disk space                                       [#######################################################] 100%
:: Processing package changes...
(1/1) upgrading openssh                                                   [#######################################################] 100%
:: Running post-transaction hooks...
(1/4) Reloading system manager configuration...
(2/4) Reloading user manager configuration...
(3/4) Creating temporary files...
(4/4) Arming ConditionNeedsUpdate...
[nasa-intern@tux-penguin ~]$ pacman -Q openssh
openssh 9.6p1-3
[nasa-intern@tux-penguin ~]$
```

2. Run `sudo systemctl start sshd` to start the `openssh` service.
3. Run `ip addr` to get the IP address of the virtual machine. In my case its `192.168.15.138`.

```
[nasa-intern@tux-penguin ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:1d:25:81 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.15.138/24 metric 100 brd 192.168.15.255 scope global dynamic ens33
       valid_lft 1541sec preferred_lft 1541sec
    inet6 fe80::20c:29ff:fe1d:2581/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[nasa-intern@tux-penguin ~]$
```

4. Run `ssh 192.168.15.138` on the host machine and login. (I'm using VMWare workstation.)

```
nasa-intern@tux-penguin:~

C:\Users\user>ssh nasa-intern@192.168.15.138
nasa-intern@192.168.15.138's password:
Last login: Wed Feb 21 21:43:15 2024
[nasa-intern@tux-penguin ~]$
```

References

- pacman - ArchWiki
- arch linux - Update only one package with pacman - Unix & Linux Stack Exchange
- systemd - ArchWiki
- Is there any Linux command that I can use to show all the network interfaces except ifconfig - Super User

4 Sudden Airdrop?

Steps

1. Run `unzip airdrop.tar.gz.zip` to get `airdrop.tar.gz`.
2. Run `tar xzf airdrop.tar.gz` to get the `airdrop` folder.
3. Navigate through `~/airdrop` with commands `cd` and `ls -al`. We reach `~/airdrop/p4` and discover a file named `flag`.
4. Run `cat flag` to obtain the flag. (Working directory: `~/airdrop/p4`)

Flag `NASA{P4_Matryoshka_Files}`

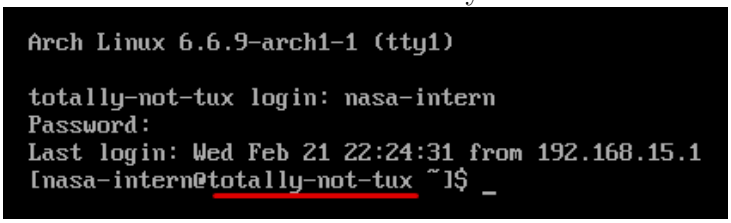
References

- command line - How to unzip a zip file from the Terminal? - Ask Ubuntu
- linux - Opening a .tar.gz file with a single command - Stack Overflow

5 Shifting Identity

Steps

1. Run `sudo nano /etc/hostname` and change the hostname to `totally-not-tux`.
2. Run `sudo reboot` to reboot the system.



3. Run `sudo usermod -c "Definitely Legit Guy" nasa-intern` to change the full name of this account.
4. Run `./security` to obtain the flag. (Working directory: `~/airdrop`)

Flag `NASA{P5_Th3_5PY_1s_AmOnG_U5}`

References

- 如何更改 Linux 作業系統的主機名稱 (hostname) ? | MagicLen
- Change user info on the command line - Unix & Linux Stack Exchange

6 DIY Friendship

Steps

1. Run `sudo useradd coolguy`.
2. Run `sudo groupadd friends`.
3. Run `sudo usermod -aG friends nasa-intern` and `sudo usermod -aG friends coolguy`.
4. Run `./friendship-test` to obtain the flag. (Working directory: `~/airdrop/p6`)

Flag `NASA{P6_W3_4r3_fri3nd5_n0t_f00d}`

References

- How to create, delete, and modify groups in Linux | Enable Sysadmin

7 Access Denied

Steps

1. Run `chmod 710 p7`. (Working directory: `~/airdrop`)
2. Run `./pentester` to obtain the flag. (Working directory: `~/airdrop/p7`)

Flag `NASA{P7_I5_th1s_TH3_h0m3w0rk_f0ld3er?}`

References

- chmod - Wikipedia
- How are r– directory permissions supposed to work on Linux? - Server Fault

8 Careless Cool Cat Commentator

Steps Consult `cowsay`'s man page and run `ls /usr/share/cows` to search for the most likely cowfile to use. `cow-and-dragon` seems to be it.

Flag

- Black and white: `NASA{P8_cowsay -f dragon-and-cow "Hello there!"}`
- Rainbow color:

  ```
  NASA{P8_cowsay -f dragon-and-cow "My name is RTX 4090" | lolcat}
  ```

References

- Add Colorful Cows to Your Terminal –Gregory Schier
- man page of `cowsay` and `lolcat`
- I overheard my friend 李承瑜 saying "cowsay".

9 Careless Cool Cat Commentator

Steps Run:

```
sed s/gentoo//g book |
  tr "aFS9PoUYXyQEvDfc7bVqW5hg)s18NeziB6xt0(RJjumM{Zkw3d4CGnT}rOLKH2lpAI"
    "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789(){}" |
  grep NASA
```

(Working directory: `~/airdrop/p9`)

Flag `NASA{P9_I_Prefer_Arch}`

References

- shell script - Using 'sed' to find and replace - Unix & Linux Stack Exchange
- man page of `sed`, `tr`, and `grep`

10 Directory Maze

Steps

1. Run `find . -name '*NASA*'`. (Working directory: `~/airdrop/p10`)
2. We obtain the flag in `./maze/W/A/E/NASA{P10_DO_YOU_F1ND_DA_W43}`.

Flag `NASA{P1O_DO_YOU_F1ND_DA_W43}`

References

- 在 Linux 下使用 find 指令查詢目錄與檔案的速查筆記 | The Will Will Web
- man page of `find`

11 Loop de Loop

Steps

1. (a) Run `./loop`. (Working directory: `~/airdrop/p11`)
   (b) Press Ctrl + Z to suspend the program.
   (c) Run `fg` to resume the program and obtain the first flag.
2. (a) Switch to tty2 by pressing Ctrl + Shift + F2.
   (b) Run `killall loop`.
   (c) Switch back to tty1 and obtain the second flag.
3. (a) Switch to tty2 and run `killall -s SIGKILL loop`.
   (b) Switch back to tty1 and confirm that the process has been killed.

```
[nasa-intern@totally-not-tux airdrop]$ cd p11
[nasa-intern@totally-not-tux p11]$ ./loop
I have occupied your terminal. Try to kill me, I dare you!
^Z
[1]+  Stopped                 ./loop
[nasa-intern@totally-not-tux p11]$ fg
./loop
You suspended me, but I'm back!
But I will show some mercy and give you flag 1:
NASA{P11_1_d1d_y0u_g3t_th3_51gn4l?}
I'm not going to terminate that easily!
But I will show some mercy and give you flag 2:
NASA{P11_2_1_wi1l_b3_b4ck}
Killed
```

Flag

1. `NASA{P11_1_d1d_y0u_g3t_th3_51gn4l?}`
2. `NASA{P11_2_1_wi1l_b3_b4ck}`
3. `NASA{P11_3_killall -s SIGKILL loop}`

References

- vlc - How to Pause/Resume a process in Linux - Stack Overflow
- linux - How to switch between tty and xorg session - Unix & Linux Stack Exchange
- bash - How can I kill a process by name instead of PID, on Linux? - Stack Overflow
- man page of `killall`
- signal(7) - Linux manual page

12 The Final Showdown

Steps

1. (a) Run `command -v vim`, which outputs `alias vim='nano'`. We suspect that code somewhere is setting suspicious bash aliases.
   (b) Run `nano ~/.bashrc`, and we see some malicious aliases at lines 13 to 15.
   (c) Remove those lines and re-login. Now `vim` and `vi` works.
2. (a) But after tens of seconds, a strange message appears with a piece of ASCII art.
   (b) With hints from the problem description and observations of system behavior, the message seems to appear every minute. After searching the internet, we suspect that a malicious task is scheduled to run every minute.
   (c) Dive into `/etc/cron.d` and inspect the file `minute`. Here we see that line 5 is malicious: `*/1 * * * * root /usr/src/nano_gang/check.sh`.
   (d) Remove that line and re-login. Now the message and ASCII art no longer appears, and `~/.bashrc` doesn't revert to the dirty version anymore.

References

- 9.7. Scheduling Tasks with cron and atd