U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – DATA & ANALYSIS CENTER

CYBER EXPERIMENTATION & ANALYSIS DIVISION
Mr. Juan Ulloa
Dr. Oscar A. Perez

PANEL INTRODUCTIONS

Who are we?

Combat Capability Development Command
Data & Analysis Center (DEVCOM DAC)

What do we do?

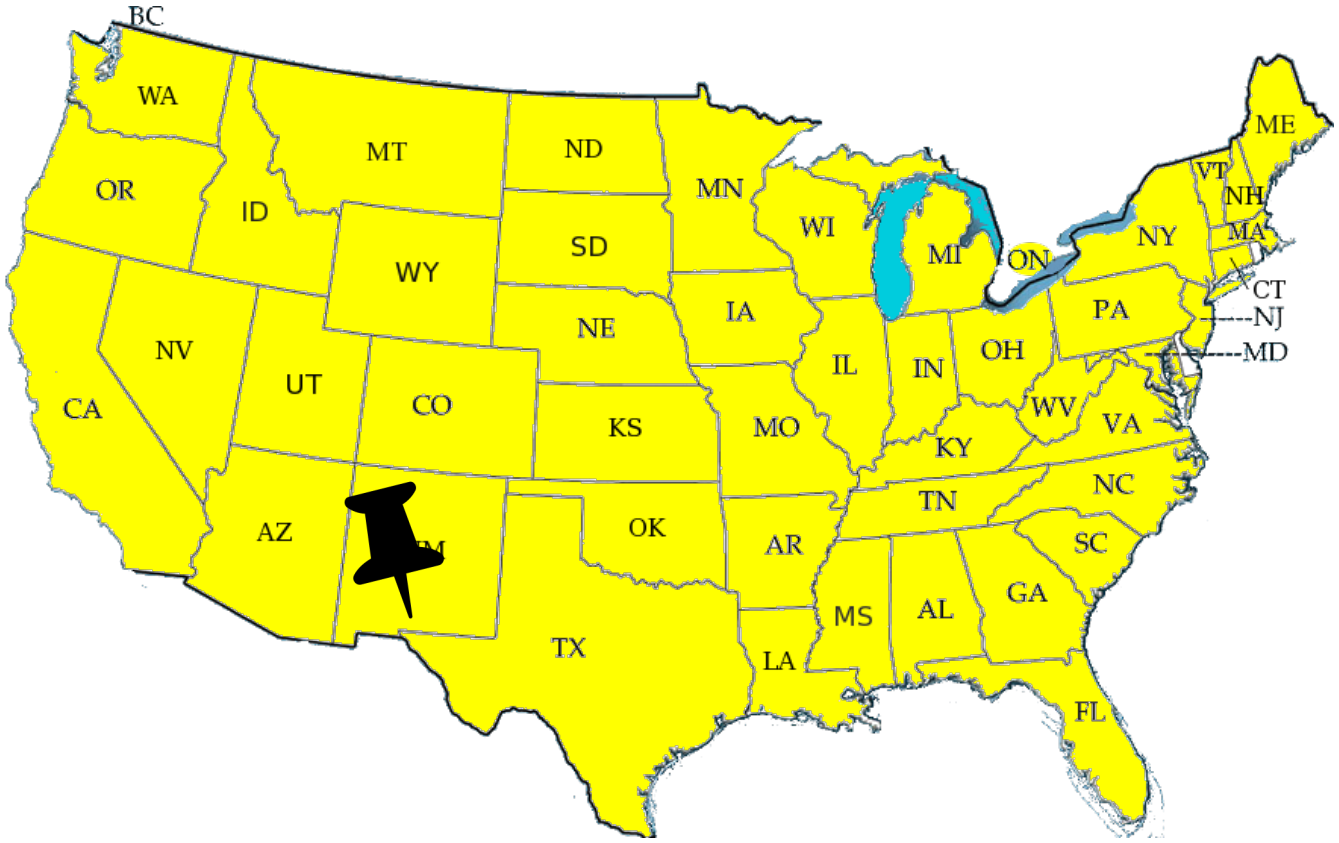
Cybersecurity Analysis

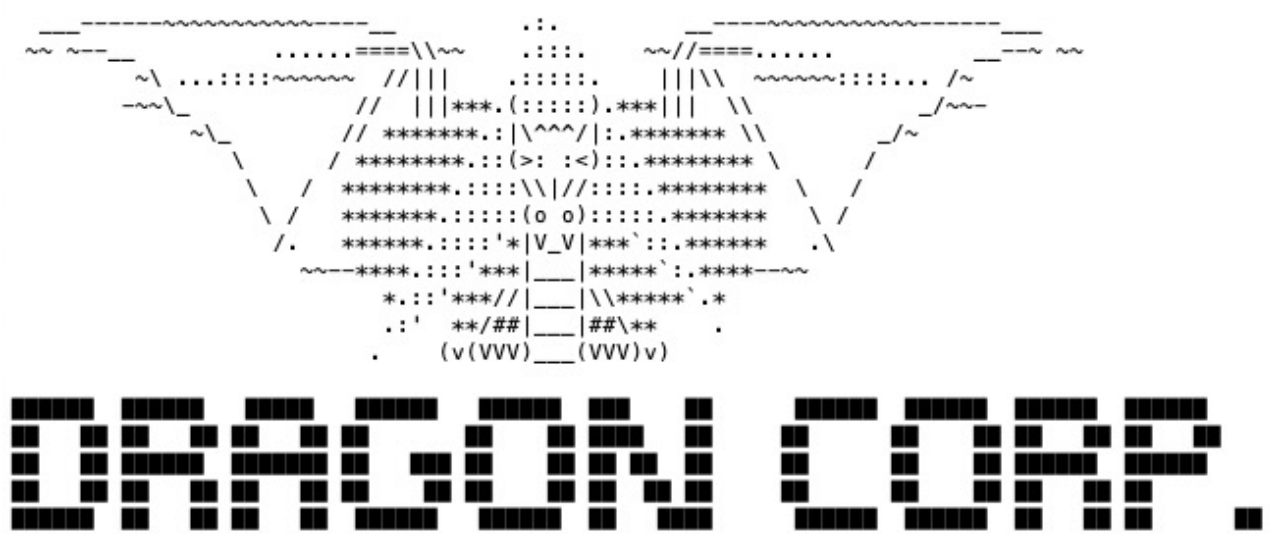
What did we study?

Computer Science
Electrical Engineering

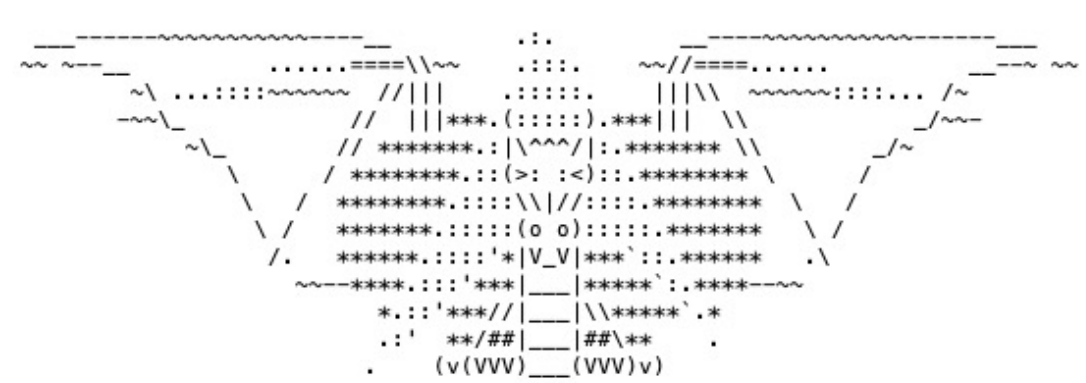
Where are we located?

New Mexico in the border with Texas





Capture the Flag by OP



DRAGON CORP.

In order for everybody to coexist these are the

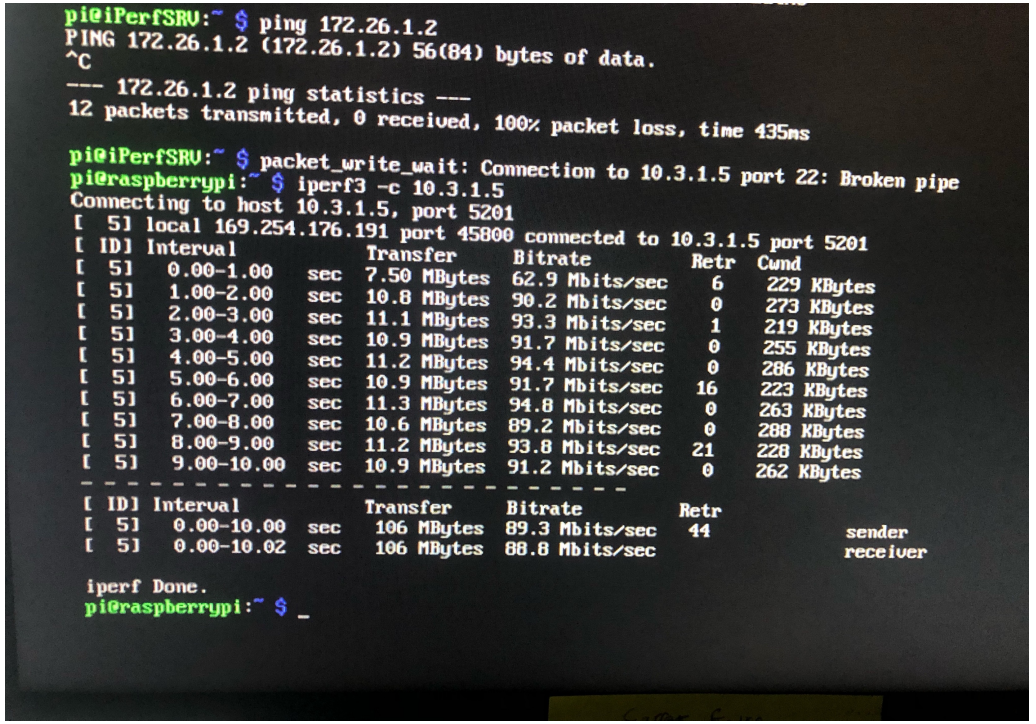
Rules of engagement:

1. Do not turn off Gatekeeper Firewall
2. Only complete your mission (but you can always help your friends without driving the keyboard)
3. Only perform the graceful shutdown

COMMAND LINE

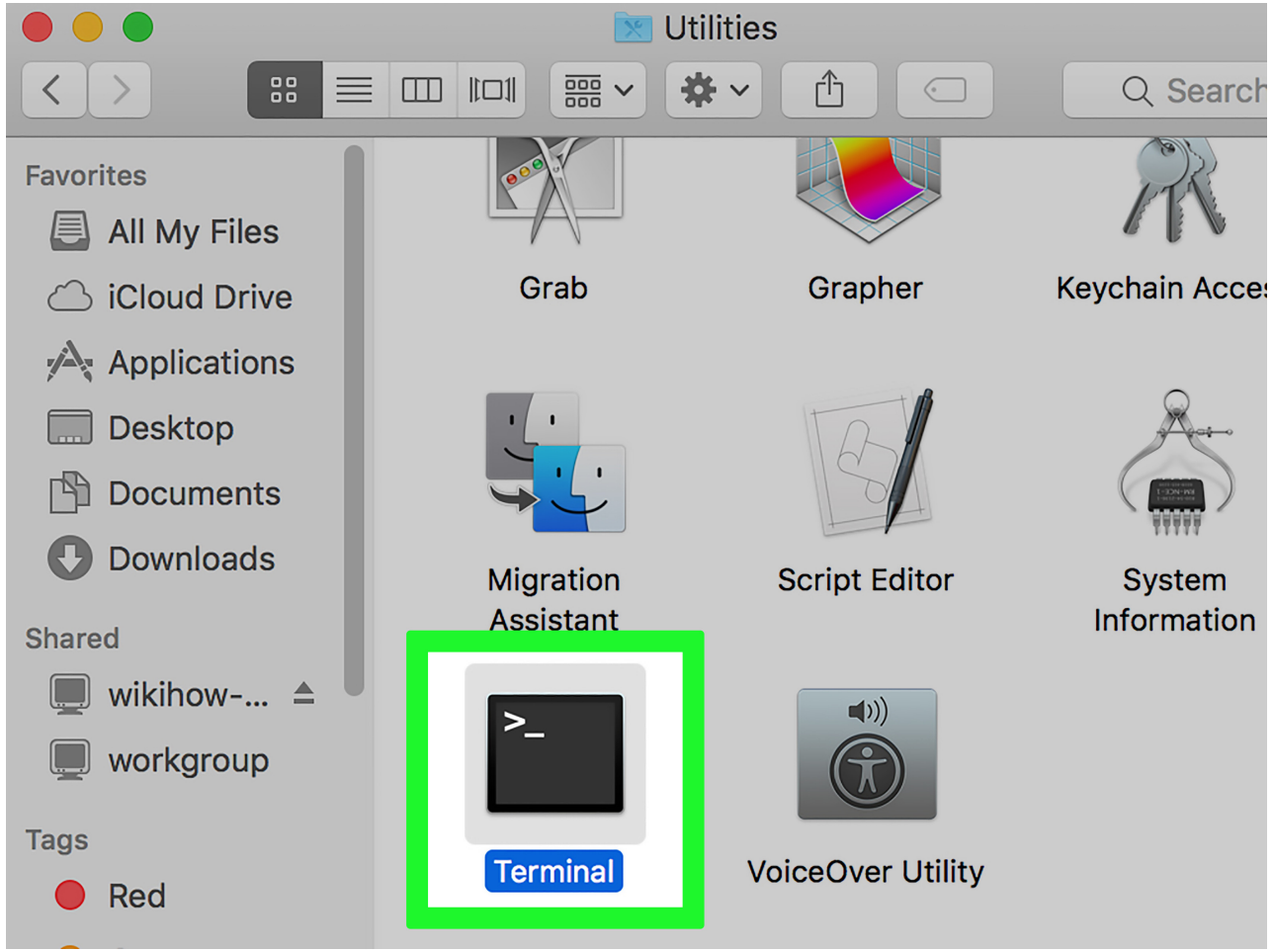
- The command prompt is a program utilized to send direct instruction to a computer system, generally with out security restrictions.

- Many cybersecurity tools are built to work only on the command prompt window as these Specialized tools do not have a graphical user interface (GUI).

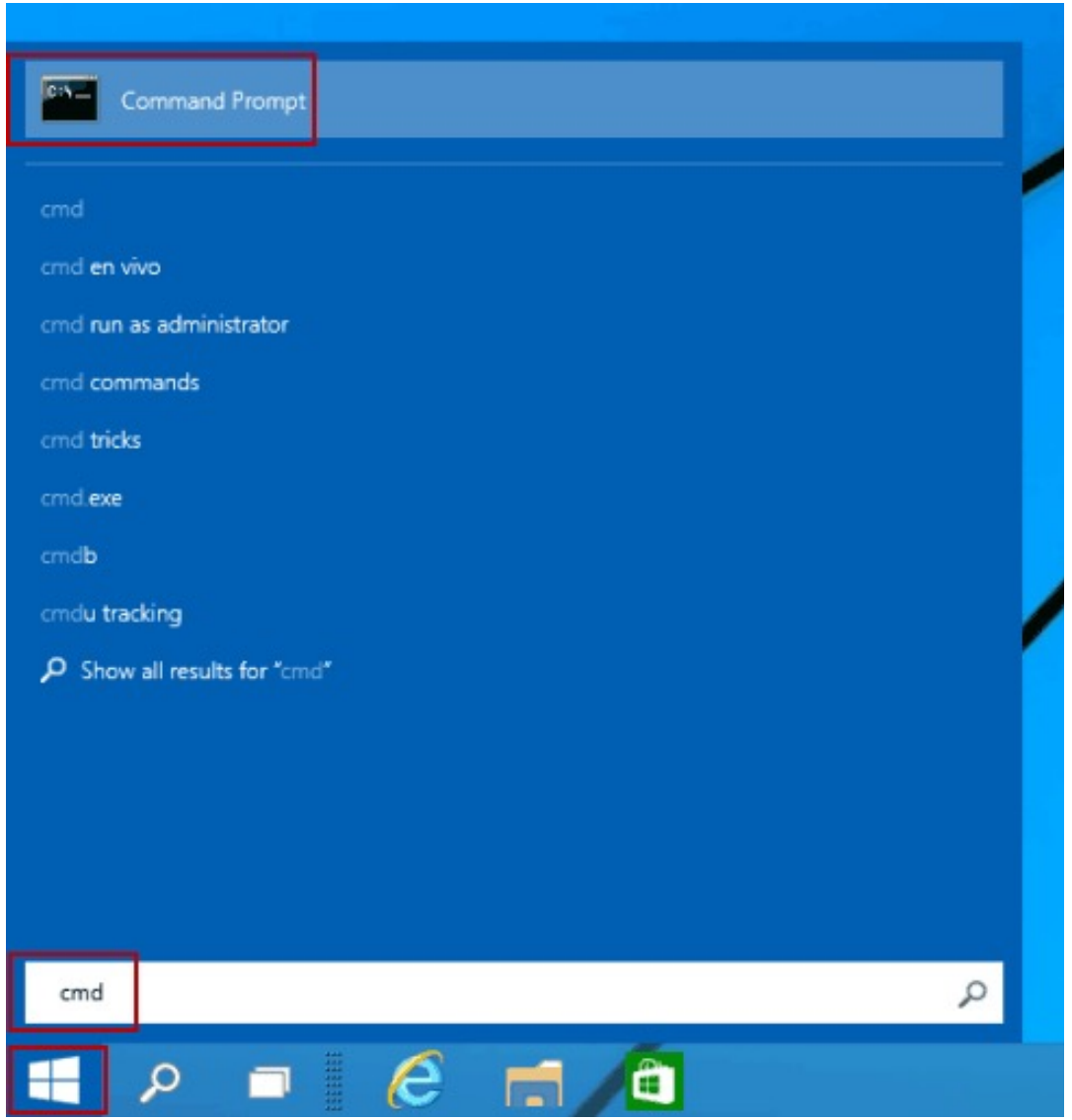


HOW TO OPEN THE COMMAND PROMPT IN OSX AND IN WINDOWS

OS X



Windows



COMMAND LINE USED FOR CYBERSECURITY

WHAT IS PING

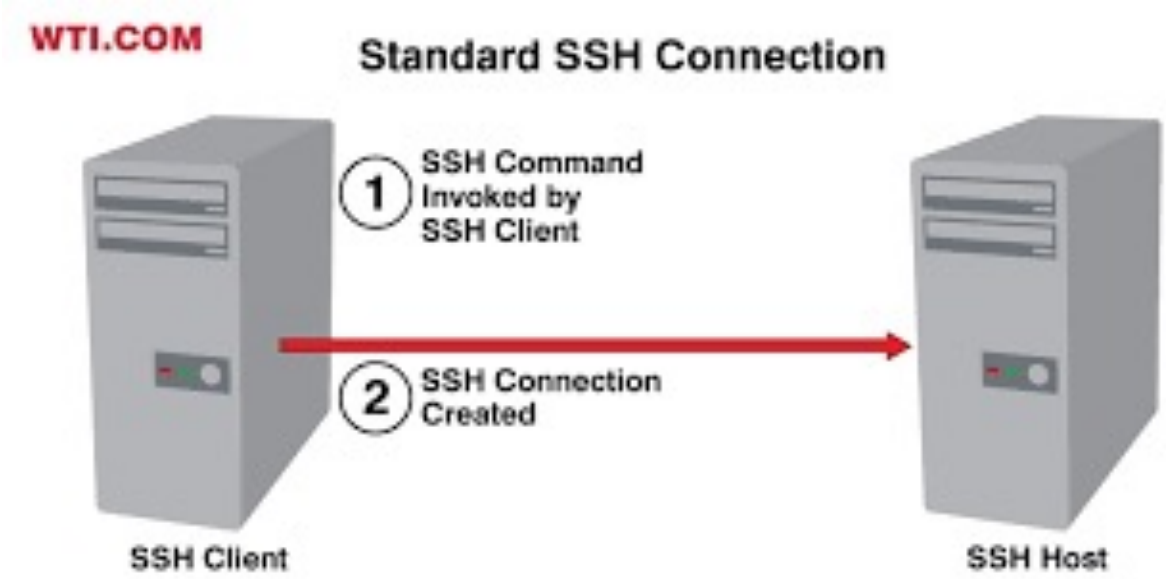
- The ping command is used when we want to test whether a connection to a remote resource is possible. Usually this will be a website on the internet, but it could also be for a computer on your home network if you want to check if it's configured correctly. Ping works using the ICMP protocol


```
drache2015 — ping google.co
Last login: Wed Mar 10 15:34:40 on ttys000
drache2015@mbp-2019 ~ % ping google.com
PING google.com (142.250.138.100): 56 data bytes
64 bytes from 142.250.138.100: icmp_seq=0 ttl=107 time=31.698 ms
64 bytes from 142.250.138.100: icmp_seq=1 ttl=107 time=36.814 ms
64 bytes from 142.250.138.100: icmp_seq=2 ttl=107 time=27.477 ms
64 bytes from 142.250.138.100: icmp_seq=3 ttl=107 time=28.058 ms
64 bytes from 142.250.138.100: icmp_seq=4 ttl=107 time=34.891 ms
64 bytes from 142.250.138.100: icmp_seq=5 ttl=107 time=36.173 ms
64 bytes from 142.250.138.100: icmp_seq=6 ttl=107 time=26.531 ms
64 bytes from 142.250.138.100: icmp_seq=7 ttl=107 time=28.863 ms
64 bytes from 142.250.138.100: icmp_seq=8 ttl=107 time=27.734 ms
64 bytes from 142.250.138.100: icmp_seq=9 ttl=107 time=64.109 ms
```

WHAT IS SSH

- SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. In addition to providing secure network services, SSH refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.

HOW TO USE SSH TO CONNECT TO A REMOTE HOST



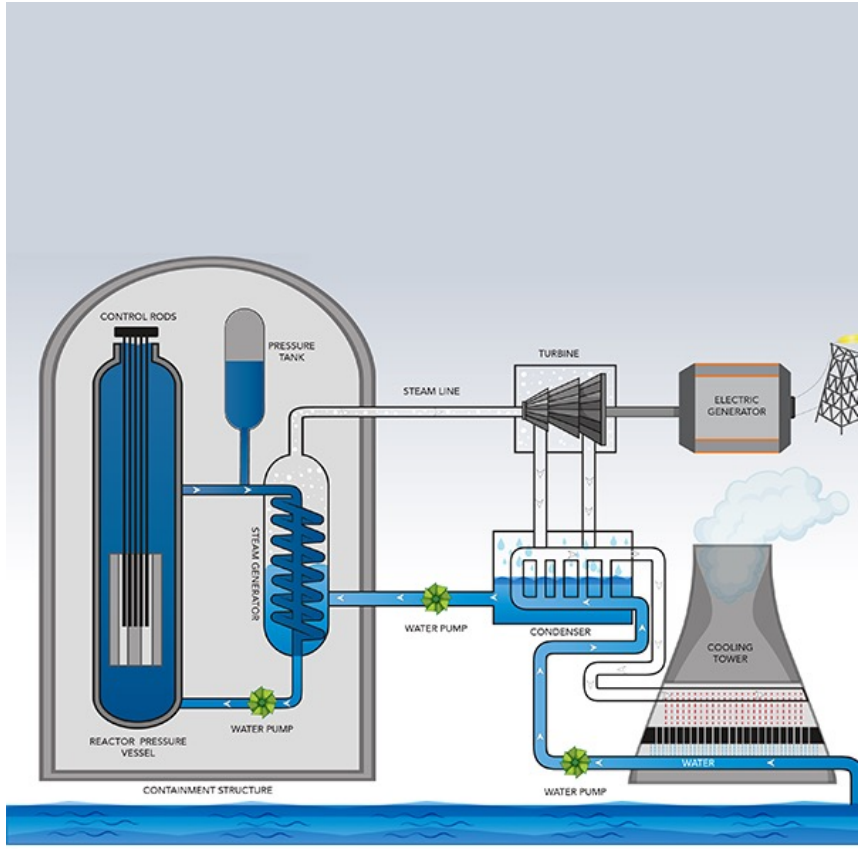
CYBER SECURITY HANDS ON ACTIVITY

Cyber physical Mission:
There has been a data breach and many logins and passwords from people working on the nuclear plant (containing several nuclear reactors) close to your city (Dragon City) were filtered to the internet. You as a cybersecurity professional are hired to make sure that the nuclear reactor is safe and it can not be shutdown from the outside.

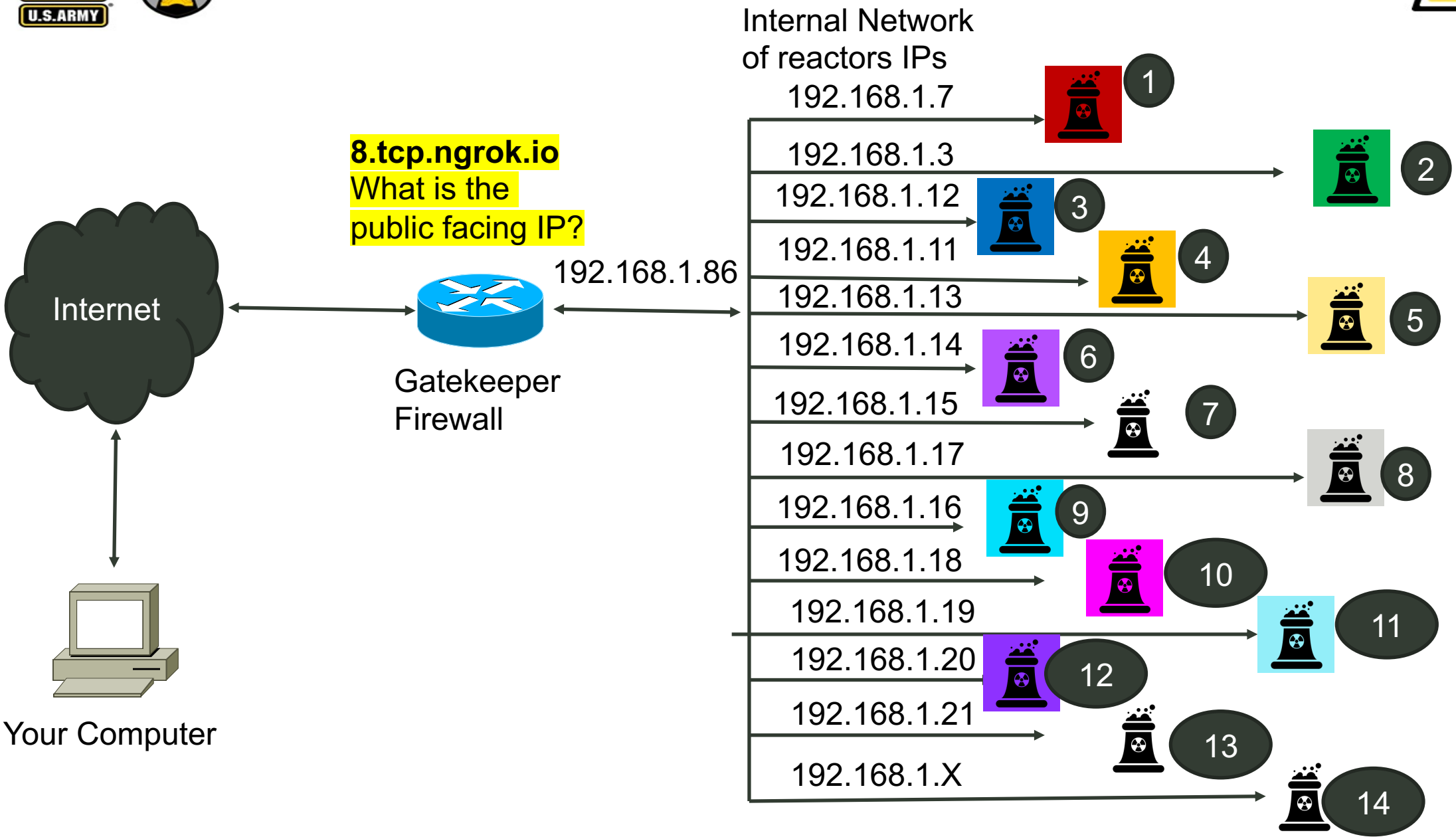
Among the information on the internet you stumble across the following:

IP of the gatekeeper firewall protecting the nuclear reactors: 8.tcp.ngrok.io and the open port is 13993
It was also leaked the fact that RASPBERRY Pis are used as controllers and the password leaked was: “@RI2017!!!” where I is a lowercase L

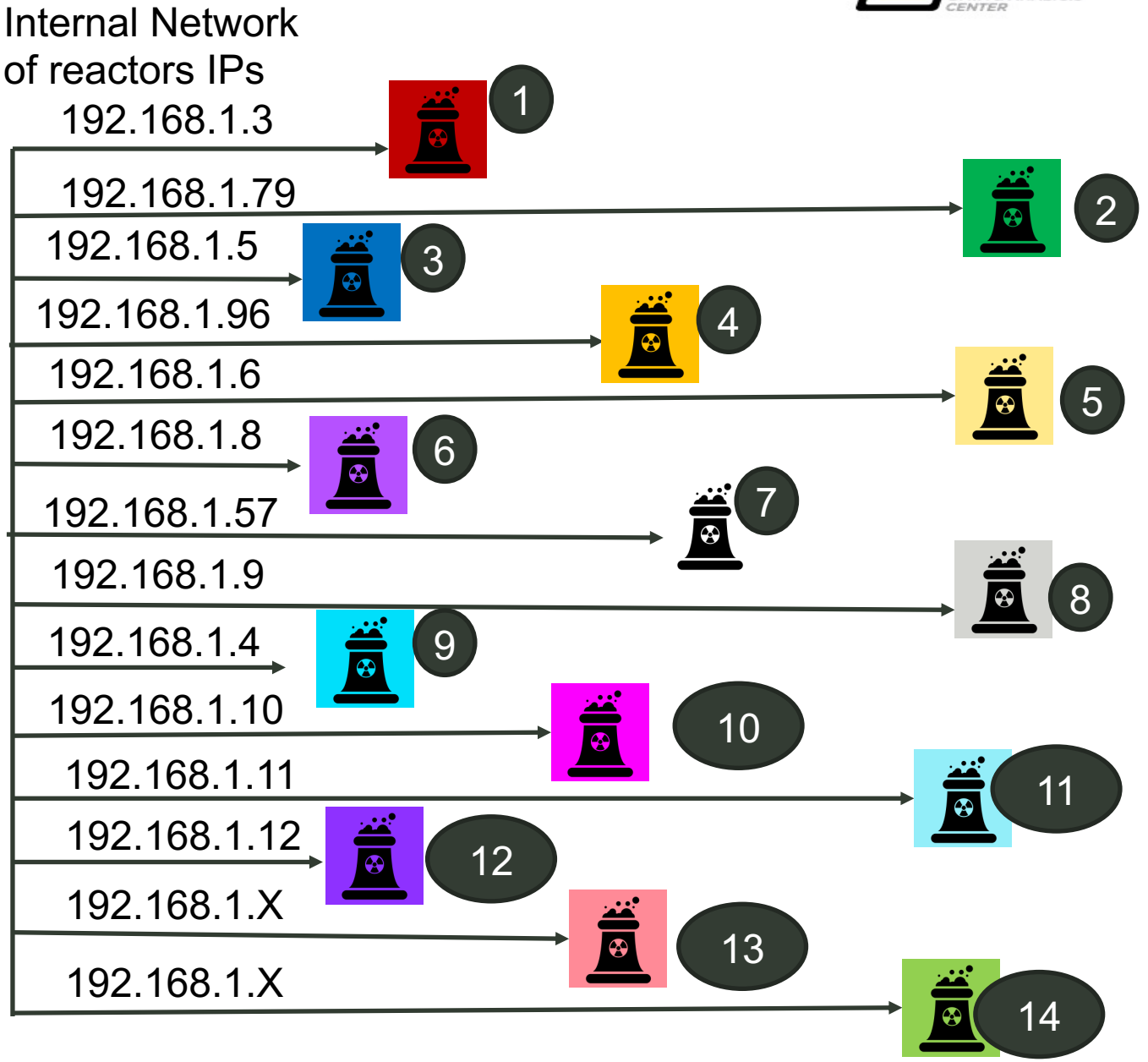
Default credentials for RASPBERRY Pis can be found by a simple google search



NETWORK DIAGRAM AFTER USING NMAP



NETWORK DIAGRAM AFTER USING NMAP



CYBER SECURITY HANDS ON ACTIVITY 2

Important commands, usage and syntax:

ping, ping is one of the most used network troubleshooting commands.
It basically checks for the network connectivity between two nodes.

```
ping google.com
```

ssh, is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption.

```
ssh -p 11282 pi@3.19.130.43
```

```
ssh pi@192.168.1.X
```

← **X** is the last number of the IP of your nuclear reactor

Running a python script

```
python poweroff.py
```

EXERCISE SETUP

--Connect Pis and start them up
--make sure a monitor and a keyboard are connected.

ping google.com

ssh -p 15888 pi@3.22.53.161

ssh pi@192.168.1.X ← **X** is the last number of the IP of your nuclear reactor

python poweroff.py

SPECIAL MISSIONS WORTH POINTS

Mission 1:
Create a new folder with your name in the Documents directory
Copy lightup.py to a new folder with **your name** inside “~/Documents” folder. Change the name of the copied file to lighthacked.py 5 points

Mission 2:
reverse engineer the new file **lighthacked.py** to make your RBP color change to RGB (184, 134, 11). 10 points

Mission 3:
Copy the /etc/shadow with the name **pass.txt** file to your newly directory in mission 1. 5 points

Mission 4:
List all of the users with an account on this system based on the pass.txt file. 15 points

Mission 5:
Find the password of the user Ariana Gibbs 15 points

Mission 6:
Describe mission 6

Mission 7:
Describe mission 7

Mission 8:
Describe mission 8

Mission 9:
Describe mission 9

CLOSING REMARKS AND STUDENT QUESTIONS

- Are there any questions from the students?

QUESTION 1

Why is Cybersecurity Important?

A) Because it helps Cybercriminals
B) Because it studies the virtual sky
C) Because it protects your information
D) Because it studies the earth

C) Cybersecurity is a part of Science that focuses on the protection of information by securing an electronic system to prevent or mitigate an attack from a bad actor.

QUESTION 2

Hackers need to know a lot about computers.

A) True
B) False

B) False, social engineering attacks don't require too many technical expertise.

QUESTION 3

What is the name of the most famous Ransomware?

A) Bad Rabbit
B) WannaCry
C) GoldenEye
D) Locky

B) WannaCry

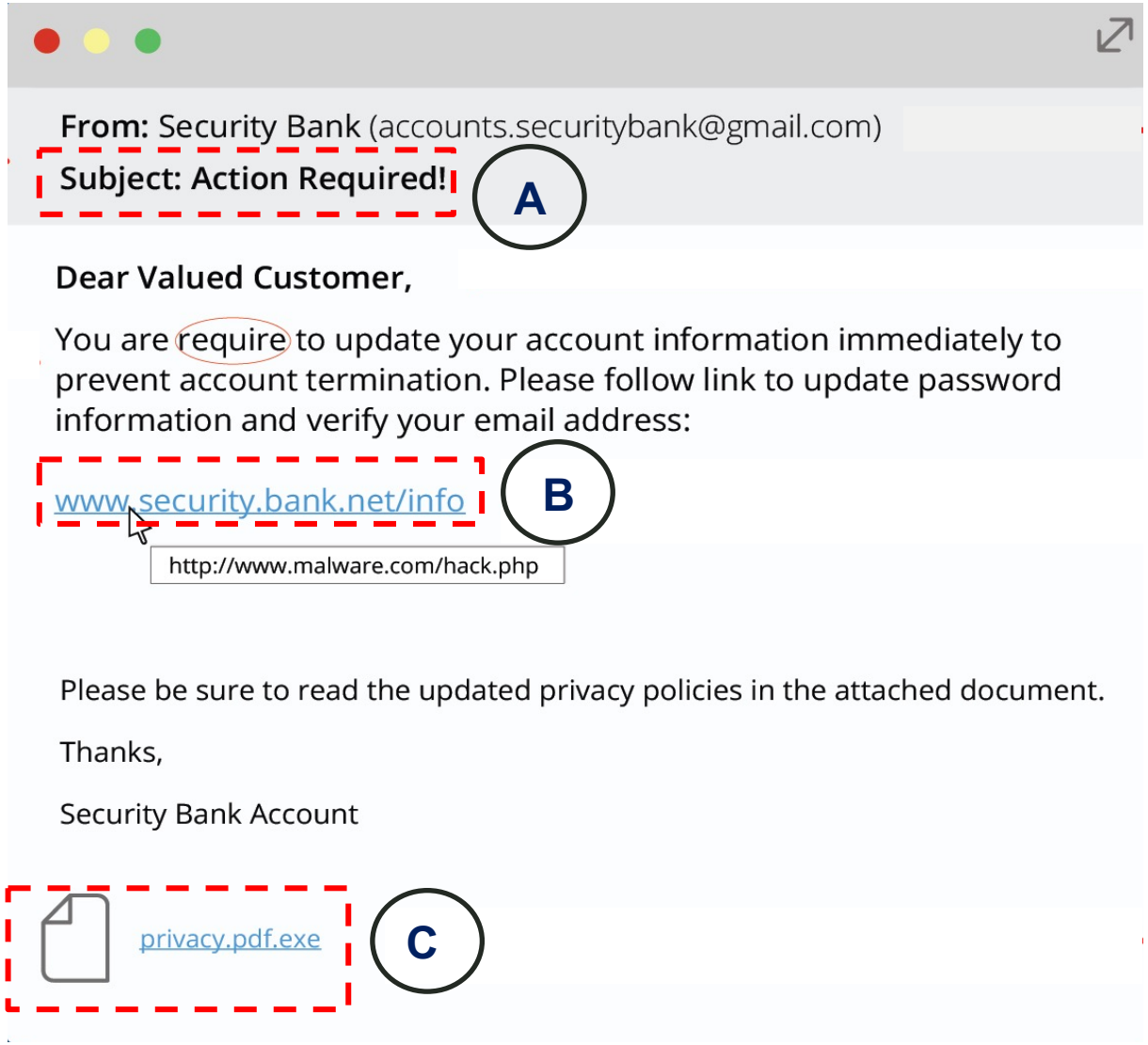
QUESTION 4

Military systems cannot be the target of a cyber-attack?

A) True
B) False

B) False

QUESTION 5



Which of the following is an example of a phishing attack?

A) A sense of urgency caused by the subject " Action Required!"

B) A link in the email pointing to a website different from what is displayed on the email

C) An unexpected attachment

D) All of the above

D) All of the above

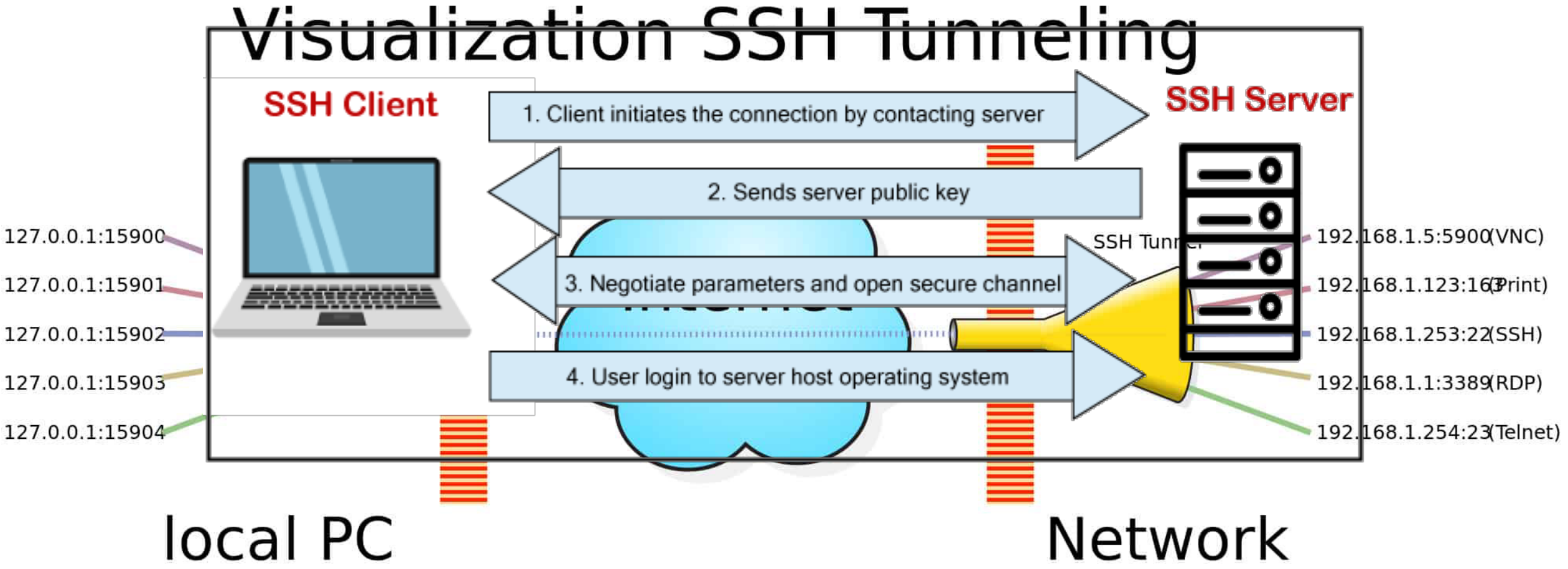
QUESTION 6

Which of the following statements is NOT a good way of protecting yourself from Ransomware?

A) Keep your computing devices up to date
B) Only install trusted software
C) Give out your personal information when asked
D) Avoid clicking on links from strangers

C) Give out your personal information when asked

HOW TO USE SSH TO CONNECT TO A REMOTE HOST



SOURCES

- https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
- https://www.cybintsolutions.com/cyber-security-facts-stats/
- https://enterprise.comodo.com/how-ransomware-spreads.php
- https://www.unitrends.com/solutions/ransomware-education
- https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom
- https://www.cybersecuritydegrees.com/features/resources-for-high-school-students-interested-in-cyber-security/

News Sources

1. https://kvia.com/news/new-mexico/2020/06/30/nmsu-investigates-cyber-attack-on-university-foundation/
2. https://www.ktsm.com/crime/online-instruction-leaves-students-and-parents-vulnerable-to-cyber-crime-fbi-says/
3. https://kvia.com/news/education/2020/02/25/gadsden-schools-computer-network-is-latest-hit-by-ransomware-attack/

HANDS-ON RESOURCES

1. https://www.hacksplaining.com/lessons
2. https://tutorials.cyberaces.org/tutorials.html
3. https://nice-challenge.com/

NEWS SOURCES

1. https://cbs4local.com/news/local/fbi-investigating-cyber-security-threats-from-virtual-learning-warns-about-more
2. https://www.ktsm.com/local/el-paso-news/gadsden-isd-has-shut-down-its-internet-system-due-to-ransomware/
3. https://spectrumlocalnews.com/tx/san-antonio/news/2020/07/23/cybersecurity-schools-online-learning
4. https://infimasec.com/blog/new-mexico-school-district/

DATA USAGE in the US

1. https://decisiondata.org/news/report-the-average-households-internet-data-usage-has-jumped-38x-in-10-years/
2. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/
3. https://www.howtogeek.com/222740/how-to-the-monitor-the-bandwidth-and-data-usage-of-individual-devices-on-your-network/

Bandwidth Calculator

1. https://broadbandnow.com/bandwidth-calculator

INTERNET PROTOCOLS

1. SSH https://www.youtube.com/watch?v=z7jVOenqFYk
2. Ping https://www.youtube.com/watch?v=m_6Aztlq4yM