Welcome to week 2, Network potocols

Congratulations on the progress you've made so far!
In this section, you'll learn about how
networks operate using tools and protocols.
These are the concepts that you'll use every
day in your work as a security analyst.
The tools and protocols you'll learn in this section of
the program will help you protect
your organization's network from attacks.
Did you know that malicious actors can take advantage of
data moving from one device to another on a network?
Thankfully, there are tools and
protocols to ensure the network
stays protected against this type of threat.
As an example, I once identified an attack
based solely on the fact they were
using the wrong protocol.
The network traffic volumes were right, and it
was coming from a trusted IP,
but it was on the wrong protocol,
which tipped us off enough to shut down
the attack before they caused real damage.
First, we'll discuss some common network protocols.
Then we'll discuss virtual private networks, or VPNs.
And finally, we'll learn about
firewall security zones and proxy servers.
Now that you have an idea of where we're
headed, let's get started.

Network protocols

Networks benefit from having rules.
Rules ensure that data sent over
the network gets to the right place.
These rules are known as network protocols.
Network protocols are a set of
rules used by two or more devices on
a network to describe the order of
delivery and the structure of the data.

Let's use a scenario to demonstrate
a few different types of network protocols
and how they work together on a network.
Say you want to access your favorite recipe website.
You go to the address bar at the top of
your browser and type in the website's address.
For example: www.yummyrecipesforme.org.
Before you gain access to the website,
your device will establish
communications with a web server.
That communication uses a protocol called
the Transmission Control Protocol, or TCP.
TCP is an internet communications protocol that allows
two devices to form a connection and stream data.

TCP also verifies both devices
before allowing any further communications to take place.
This is often referred to as a handshake.
Once communication is established using a TCP handshake,
a request is made to the network.
Using our example, we have requested
data from the Yummy Recipes For Me server.
Their servers will respond to that request and send
data packets back to
your device so that you can view the web page.

As data packets move across the network,
they move between network devices such as routers.
The Address Resolution Protocol, or ARP, is used to
determine the MAC address of
the next router or device on the path.
This ensures that the data gets to the right place.
Now the communication has been
established and the destination device is known,
it's time to access the Yummy Recipes For Me website.

The Hypertext Transfer Protocol Secure, or HTTPS, is
a network protocol that provides a secure method of
communication between client and website servers.
It allows your web browser to securely send a request
for a webpage to the Yummy Recipes For Me server
and receive a webpage as a response.

Next comes a protocol called the
Domain Name System, or DNS,
which is a network protocol that translate

internet domain names into IP addresses.
The DNS protocol sends
the domain name and the web address to
a DNS server that retrieves
the IP address of the website you were trying to access,
in this case, Yummy Recipes For Me.
The IP address is included as a destination address for
the data packets traveling to
the Yummy Recipes For Me web server.
So just by visiting one website,
the device on your networks are
using four different protocols:
TCP, ARP, HTTPS, and DNS.

These are just some of the protocols
used in network communications.
To help you learn more about the different protocols,
we'll discuss them further
in an upcoming course material.

But how do these protocols relate to security?
Well, on the Yummy Recipes For Me website example,
we used HTTPS, which is
a secure protocol that
requests a webpage from a web server.
HTTPS encrypts data using
the Secure Sockets Layer and Transport Layer Security,
otherwise known as SSL/TLS.
This helps keep the information secure from
malicious actors who want to steal valuable information.

That's a lot of information and
a lot of protocols to remember.
Throughout your career as a security analyst,
you'll become more familiar with
network protocols and use them in your daily activities.

Revision #1
Created 2023-06-29 05:05:32 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai