zumaroc

Day 1

ZROC102

Module 2: Introduction to SOC Analysis

Table of Contents

What is SOC?

Security Operation Center (SOC) is a centralized unit that constantly monitors and analyzes the security of an organization.
The main purpose of the SOC team is to analyze, detect and respond against cyber security incidents by using technology, people and processes.

The SOC acts like a hub or central command post, collecting telemetry data from the entire enterprise IT infrastructure, including networks, devices, appliances, and information storage, regardless of where these assets are located.

Types Of SOC

We can classify the types of security operations centers into five broad categories:

❖ In-house SOC:
The company has its own cybersecurity team. Companies considering setting up an in-house SOC should have a budget to support continuity.

❖ Virtual SOC:
Security teams do not have their own facilities and often work remotely in different locations.

❖ Co-Managed SOC:
The Co-Managed SOC consists of internal SOC staff working with an external Managed Security Service Provider (MSSP). Adjustment is very important for this type of model.

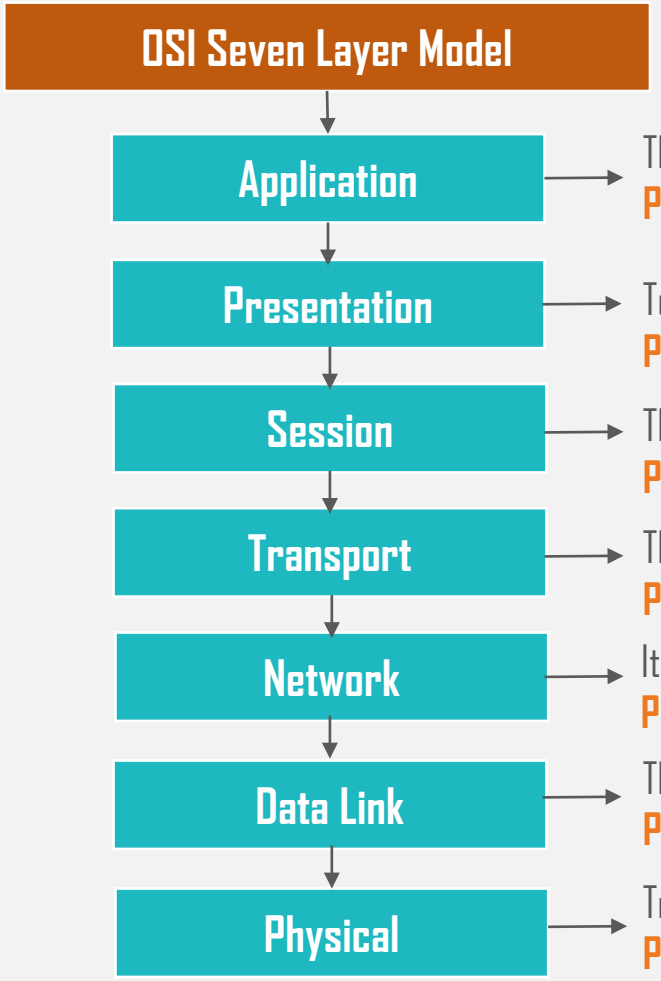
❖ Command SOC:
A high-level group that oversees small SOCs in large areas. Organizations using this model include large telecommunications providers and defense agencies.

Introduction to Networking

The OSI (Open Systems Interconnection) Model is a framework to demonstrate the theory behind computer networking. The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

The OSI 7-layer model is still widely used, as it helps visualize and communicate how networks performs, and helps isolate and troubleshoot networking problems.

Networking : OSI Seven Layers



This allows access to the network resources. It transmits and receives in Data.
Protocols: HTTP, FTP, IRC, SSH, DNS

To encrypt, translate and compress data. It transmits and receives in Data.
Protocols: SSL, SSH, IMAP, FTP, MPEG, JPEG

This establishes, manages, and terminates connection. It transmits and receives in Data.
Protocols: API's, WinSock, Sockets

This provides reliable processes for message and error delivery. It transmits and receives in Segments.
Protocols: TCP, UDP

It moves packets from source to destination to provide internetworking. It transmits and receives in Packets.
Protocols: IP, IPsec, ICMP

This organizes bits into frames and provides hop-to-hop delivery. It transmits and receives in Frames.
Protocols: Ethernet, Switch, Brides, PPP

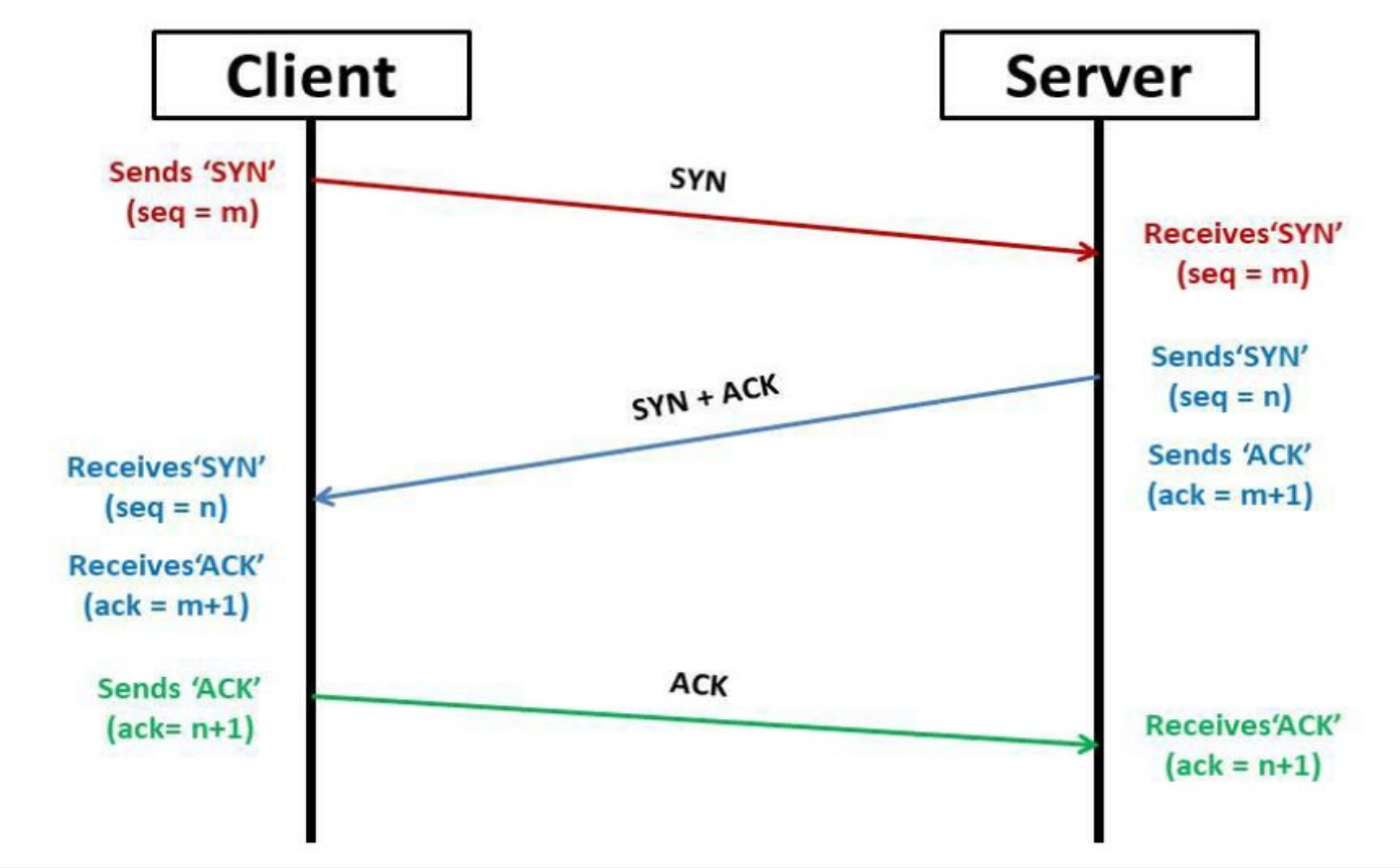
Transmits bits over a medium. It transmits and receives in Bits.
Protocols: Fiber, Wireless, Hubs, Repeater

Networking: The TCP/IP Model

The TCP/IP model consists of four layers: Application, Transport, Internet and Network Interface. Between them, these cover the same range of functions as the seven layers of the OSI Model.

The TCP/IP takes its name from the two most important of these: the Transmission Control Protocol that controls the flow of data between two endpoints, and the Internet Protocol, which controls how packets are addressed and sent. There are many more protocols that make up the TCP/IP suite

Networking: The TCP/IP Model



When a connection attempt is made, the computer first sends a special request to the remote server indicating that it wants to initialize a connection.

This request contains something called a ***SYN*** (short for ***synchronize***) bit, which essentially makes first contact in starting the connection process. The server will then respond with a packet containing the SYN bit, as well as another "acknowledgement" bit, called ***ACK***. Finally, the computer will send a packet that contains the ACK bit by itself, confirming that the connection has been setup successfully. With the three-way handshake successfully completed, data can be reliably transmitted between the two computers. Any data that is lost or corrupted on transmission is re-sent, thus leading to a connection which appears to be lossless.

Networking: Ping

The ping command is used when we want to test whether a connection to a remote resource is possible. Theis can be a website on the internet, 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, which is one of the slightly less well-known TCP/IP protocols.

The basic syntax for ping is: `ping <target>`

In this example we are using ping to test whether a network connection to Google is possible:

```
→  ~ ping google.com
PING google.com (216.58.223.238) 56(84) bytes of data.
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=1 ttl=115 time=32.1 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=2 ttl=115 time=39.6 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=3 ttl=115 time=43.6 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 32.064/38.430/43.645/4.797 ms
```

Any questions about syntax can be answered using the man page for ping: `man ping`

Networking: Traceroute

The internet is made up of many, many different servers and end-points, all interconnected. This means that, in order to get to the content, you want, you first need to go through a bunch of other servers.

Traceroute allows you to see each of these connections - it allows you to see every intermediate step between your computer and the resource that you requested.

The basic syntax for traceroute on Linux is this: `traceroute <destination>`

```
→  ~ traceroute google.com
traceroute to google.com (216.58.223.238), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  2.064 ms  3.098 ms  3.081 ms
 2  * * *
 3  10.109.1.30 (10.109.1.30)  46.198 ms  54.138 ms  55.721 ms
 4  10.109.4.254 (10.109.4.254)  55.152 ms  56.737 ms  56.726 ms
 5  10.2.254.108 (10.2.254.108)  56.116 ms 10.2.254.109 (10.2.254.109)  56.101 ms 10.2.254.108 (10.2.254.108)  56.085 ms
 6  * * 10.2.253.72 (10.2.253.72)  21.649 ms
 7  197.210.172.1 (197.210.172.1)  28.384 ms  27.296 ms  27.680 ms
 8  102.89.4.11 (102.89.4.11)  34.371 ms  33.050 ms  34.217 ms
 9  108.170.240.17 (108.170.240.17)  34.202 ms 108.170.240.33 (108.170.240.33)  32.536 ms 108.170.240.17 (108.170.240.17)  34.162 ms
10  172.253.76.219 (172.253.76.219)  35.950 ms 172.253.76.217 (172.253.76.217)  25.383 ms  33.663 ms
11  los02s04-in-f14.1e100.net (216.58.223.238)  33.092 ms  33.605 ms  29.428 ms
→  ~
```

Any questions about syntax can be answered using the man page for ping: `man traceroute`

Networking: Traceroute – Contd.

The basic syntax for traceroute on Windows is this: `tracert <destination>`

```
C:\Users\Zumaroc Tech>tracert google.com

Tracing route to google.com [216.58.223.206]
over a maximum of 30 hops:

  1     3 ms     2 ms     3 ms  CPE [192.168.0.1]
  2    27 ms    28 ms    29 ms  10.114.6.139
  3   503 ms    58 ms    19 ms  10.109.1.30
  4    42 ms    23 ms    22 ms  10.109.4.254
  5    23 ms    22 ms    26 ms  10.2.254.108
  6    48 ms    18 ms    28 ms  10.2.253.72
  7    65 ms    22 ms    24 ms  197.210.172.1
  8    20 ms    21 ms    24 ms  102.89.4.11
  9    29 ms    25 ms    24 ms  74.125.244.113
 10    36 ms    23 ms    23 ms  172.253.76.171
 11    32 ms    30 ms    20 ms  los02s03-in-f14.1e100.net [216.58.223.206]

Trace complete.

C:\Users\Zumaroc Tech>
```

Networking: WHOIS

Whois is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.

The basic syntax for traceroute on Linux is this: `whois <domain>`

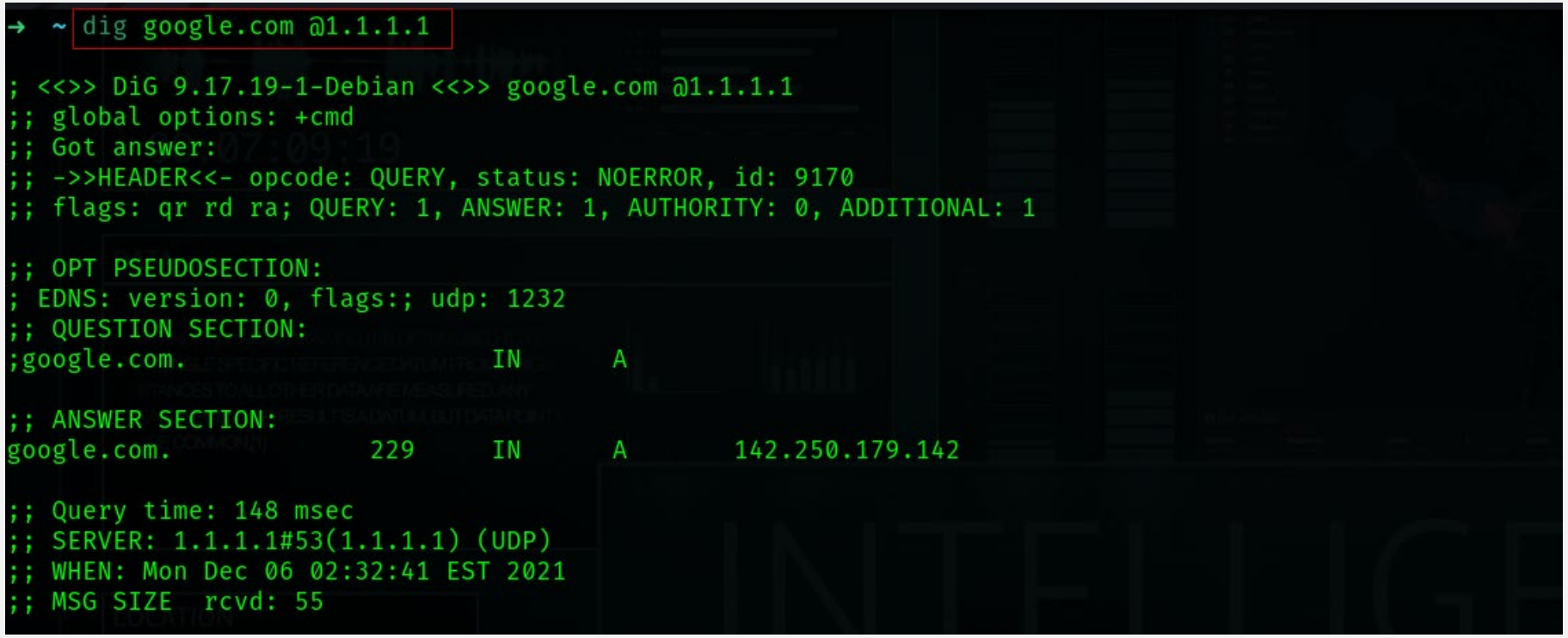
```
➜  ~ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
```

Any questions about syntax can be answered using the man page for ping: `man whois`

Networking: Dig

Dig is a network administration command-line tool for querying the Domain Name System (DNS). The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.

The basic syntax for traceroute on Linux is this: `dig <domain> <dns-server-IP>`



Any questions about syntax can be answered using the man page for dig: `man dig`

Networking: Dig - Contd.

DIG is a robust command-line tool developed by BIND for querying DNS nameservers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

Understanding the Dig Response

- QUESTION SECTION: The query made to the DNS. In this example, we asked for the first available A record for the hostname, google.com.
- ANSWER SECTION: The first available answer for the query made to the DNS. In this example, we received the A record for the IP address 142.250.179.142
- AUTHORITY SECTION: The authoritative nameservers from which the answer to the query was received. These nameservers house the zones for a domain.
- ADDITIONAL SECTION: Additional information the resolver may need but not the answer to the query.

Sources

- https://en.wikipedia.org/wiki/WHOIS
- https://help.dyn.com/how-to-use-binds-dig-tool/