Network Discovery Detection

Attackers perform certain actions to discover the target network.

Network Discovery

Attacker is trying to find an opening

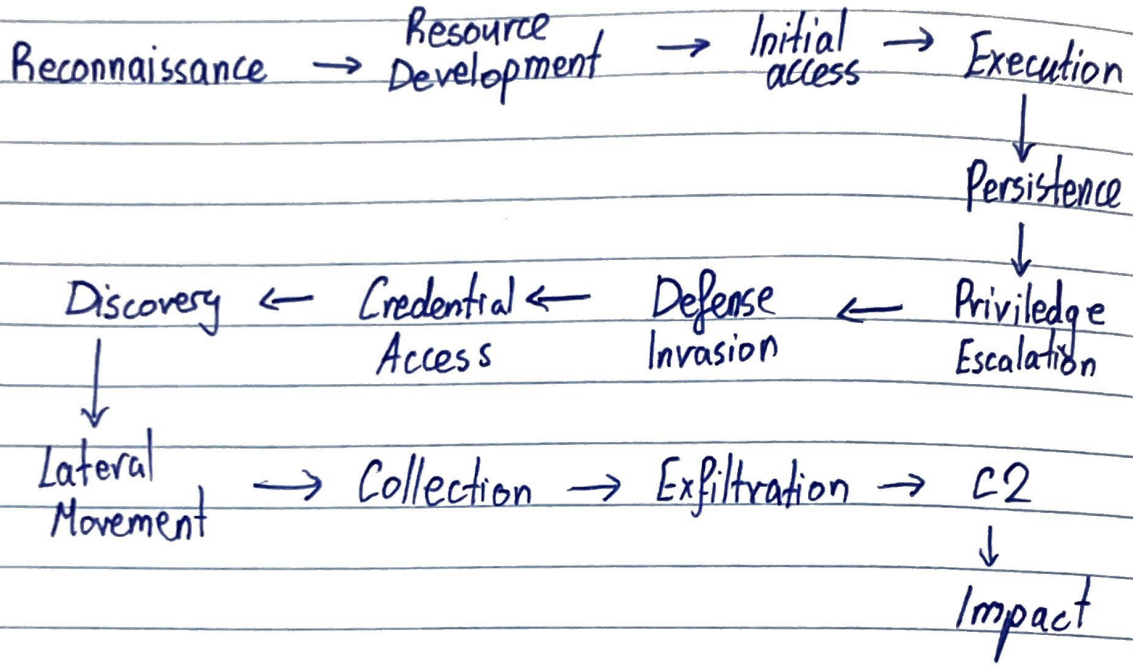
Both attackers and defenders perform discovery actions

Mitigating techniques:

- Allow list known internal and benign external scanners, ensuring no alerts triggered on those sources
-
- Integrate Threat Intelligence with detection use cases, and flag scanning activity only from known malicious or sus source
- Use the Threat Intelligence to raise severity of the alerts instead of only triggering alerts

External vs Internal Scanning

External



Internal Scanning Activity

→ this type of scan indicates that the attack has progressed to the Discovery

Question

- Which file contains logs that showcase internal scanning activity?

log-session-2.csv

Because all of the logs are from 192.168.230.xxx to 192.168.230.xxx

- How many log entries are present for the internal IP performing internal scanning activity?

2276 → 2276

- what is the external IP address that is performing external scanning activity?

Horizontal and Vertical Scanning

Once attacker get the host, they often go for open ports

Horizontal Scanning → performed to identify which hosts expose a particular port
→ same source IP, a single destination port but multiple destination IP addresses

Vertical Scanning → performed when attacker is focused on identifying a vulnerability on a single machine
(consider valuable target based on their objective)

Horizontal
→ Many ~~ports~~ hosts for the same or set of port
→ Goal is to which machines are running a specific service

Vertical
→ few host across many ports
→ Goal is to map which services are exposed on a particular machine

Question

1) One of the log files contains evidence of a horizontal scan. Which IP range was scanned?

203.0.113.0/24

- 203.0.113.~~5~~ is a one of the subnet of 203.0.113.0/24

2) In the same log file, there is one IP address on which a vertical scan is performed. Which IP address is this?

performing → 192.~~1~~68.230.127
performed → 192.168.230.145

3) On one of the IP addresses, only a few ports are scanned which host common services. Which are the ports that are scanned ~~of~~ on this IP address?

80, 445, 3389

The Mechanics of Scanning

Ping Sweep:

→ basic network scanning techniques
→ used to identify hosts present (online) on a network
→ run by sending (ICMP) packet to the host
- if the host is online: reply with ICMP

TCP SYN Scans

→ TCP initiated by 3-way-handshake

UDP Scans

→ Sending (empty) UDP packet
- closed: send back ICMP
- no response: marks down open

We are using Kibana to answer these questions

Questions

1) which source IP performs a ping sweep attack across the whole subnet?

network.protocol = icmp

192.168.230.127

2)

The zeek.conn.conn_state value shows the connection state. Using the information provided by this value, identify the type of scan being performed by 203.0.113.25 against 192.168.230.145

TCP SYN SCAN

3)

Is there any UDP scanning attemps in the logs?

N (Because it was not scanning, but there were 2 UDP connection)