Security Operations & Incident Management

Lab: Honeypot challenge

1. Setting up the Environment

The aim of this workshop is to build on skills from previous practicals and lectures and enable you to profile traffic and analyse a wide variety of attacks, captured by a honeypot. You can use Wireshark, tcpdump, and Snort for this practical. You will use the Ubuntu16045-base image to see how they detect attacking traffic. Each version of Snort uses different configuration and ruleset options, therefore, it will produce different alerts.

Ubuntu16045-base:
username: student
password: student

2. Analysing a dataset in VM Image

Before you run a new dataset, please open the BASE GUI on the web browser and delete any existing alerts. Please refer to section 9 for more details.

To analyse a dataset in the VM image, you need to read the pcap file with the –r parameter when you run snort.

```
sudo snort -v -g snort -u snort -c /etc/snort/snort.conf -r
<filename> -i ens33
```

Where: -c /etc/snort/snort.conf will run Snort in NIDS mode using configuration file /etc/snort/snort.conf

-r filename will read pcap file filename and will pass it as input to Snort

1. Now, open a web browser and type the URL:
   http://localhost/base/base_main.php

3. Dataset Files

Dataset Files (both files relate to the same incident)	
Image	**Location**
Ubuntu16045-base	`/root/Desktop/data/8-the-challenge/`**`challenge.pcap`**

4. Stage 1 – Discovering network architecture

1. What are the IP addresses of the hosts sitting on the honeynet's network segment? What can you tell about them by their MAC addresses?

   Description: Use tcpdump -r challenge.pcap to read the capture file, and use the appropriate filter to extract the appropriate traffic that will allow you to determine which hosts are sitting on the local segment. Analyze the MAC addresses and see if you can find a way to determine the hardware platform in which the systems are running out of that information.

Hint: ARP traffic is local to the network segment

2. What is the IP address of the honeypot?

   Description: Out of the addresses discovered in the previous question, identity which one corresponds to the honeypot by analyzing what traffic is generated/received by each of the IPs.

   Hint: Honeypot is a host that does not send any traffic (with the possible exception of "administrative" traffic such as syslog, dns or ntp)

3. What is the IP address of the local gateway(s)?

   Description: Identity the IP addressees) of the local gateway(s) by analyzing the traffic and looking for the characteristic that defines traffic going through a gateway. Find the MAC address(es) and map them to IP address(es) by analyzing the appropriate traffic (the ether src or ether dst bpf filters can prove useful). Verify if there is just one or more than one gateway in the network.

   Hint: Outgoing IP traffic will be directed at the link layer to the gateway; you will need to use the tcpdump flag that shows link layer information.

   Hint: To isolate outgoing traffic you will have to ignore traffic directed to the local network and broadcast traffic: not dst net 192.168.0.0/16 and not dst host 255.255.255.255

   Hint: Use ARP traffic to map the MAC address discovered to the IP of the gateway.

4. Can you identify any router(s) in addition to the local gateway? Can you estimate how many hops away it is?

   Description: Analyze the traffic in order to identify upstream routers near the looking for clear signs of router activity (typically some types of ICMP error messages).

   Hint: Signs of clear router activity are usually host unreachable, network unreachable or admin prohibited ICMP error messages.

   Hint: Hop information is derived from the TTL field, which is not shown by default in the standard tcpdump output. You will have to use the tcpdump flag that shows TTL information.

   Hint: TTL values are usually set by the sending host to 64, 128 or 255.

5. What are the IP addresses of the DNS servers used by the honeypot?

   Description: Use the appropriate filter to extract outgoing DNS traffic.

   Hint: DNS uses UDP port 53, except for zone transfers or big queries, in which case it falls back to tcp.

6. Can you identify NTP traffic? If so, identify the IP address(es) of the NTP server(s)?

   Hint: NTP uses TCP and UDP ports 123.

5. Stage 2 – Profiling traffic

1. Is there fragmentation activity in the capture?

   Description: Fragmented packets are often a sign of malicious activity (DoS, firewall or IDS evasion, etc.). Use tcpdump with the appropriate filter in order to be able to identify fragmentation activity in this particular dump.

   Hint: To look for fragmented packets, we will have to look for packets with either the MF flag set or a non-zero fragment offset (to catch the last fragments): ip[6] & 0x20 != 0 or ip[6:2] & Ox1fff!= 0

2. What protocols can you find in the traffic (layer 2 & 3 only)?

   Description: Analyze the traffic with tcpdump and try to determine what layer 2 and layer 3 protocols were in use (do not take into consideration higher level protocols such us http, ftp, smb, etc.).

3. What types of ICMP messages can you find in the traffic? Find a way to do it with tcpdump and with snort.

   Description: Extract all the ICMP messages from the dump file, and identify what kind of messages we have regarding their types and codes. Find the way to do this with tcpdump and find an easier way to do it with snort.

   Hint: Remember that snort, by default, dumps all the traffic into directories with the IP address of the offending systems. The names of the files are usually quite explanative regarding the type of traffic taking place: snort -r challenge.pcap -I snort _Iog_icmp icmp. Take a look at the files created.

4. Which ports were open in the honeypot? Which were closed? Can you recognize which well known services are supposedly running on the ones that were open?

   Description: Extract from the dump the packets issued by the honeypot that are clear sign of connection establishment.

   Hint: Open TCP ports will answer with a SYN/ ACK; Closed TCP ports will answer with a RST if unfiltered or will issue no response if filtered.

   Hint: The following filter checks for SYN/ACKs: "src host 192.168.1.3 and tcp[13] & 0x012 = 0x12"

5. Can you find evidence of possible backscatter activity (someone spoofing your IP address in TCP connections to third party hosts)? What other explanations could you give for this traffic? What is the most likely one?

   Description: You may receive backscatter activity in the form of unexpected SYN/ACKs coming into your network when someone borrows your IP address and sends spoofed SYNs to a third party. The intent may be to use your IP as a decoy (hiding the real IP in a forest of spoofed IP addresses, including yours), to use your host as a quiet host in an idle scan, etc. There are other possible explanations for this kind of traffic. Try to determine what is the most plausible in this case.

   Hint: Look for SYN/ACKs coming into your network that are not related to activity you have initiated: (tcp[13] & 0x12 = 0x12) and not src host 192.168.1.3

8. Stage 3 – Identifying attacks

1. Run the traffic through snort to identify attacks. How many different types of attacks did snort catch?

2. Can you identify worm activity? Which worms can you identify?

3. Can you identify any sessions that correspond to system compromises?

9. Cleaning up the VM image

Ubuntu16045-base

Please make sure that you delete all the alerts you created, to avoid interfering with other students' work.