**IOT & Cyber Security**

~Week 5-6~

Simulating Honeypot & Dos Attacks & Implementing Port Security

**Simulating Honeypot Cyber Attack:**

Honey pot is a computer system that is set up to trap cyber attackers who try to gain unauthorized access to information systems. Here are the simulated each step of attack.

* A hacker begins by scanning the internet for vulnerable systems to target.
* The hacker comes across a network that appears to have multiple servers and many open ports, indicating that it may be a valuable target.
* Upon further investigation, the hacker discovers that the network is a honeypot - a trap set up by cybersecurity professionals to attract and monitor potential attackers.
* The hacker attempts to gain access to the honeypot by entering various login credentials and attempting to exploit known vulnerabilities.
* As the hacker continues to try and gain access to the honeypot, they are being monitored by cybersecurity professionals. The professionals can track the hacker's IP address, the methods they are using to try and gain access, and any other information that may be useful in identifying and prosecuting the attacker.
* Eventually, the hacker realizes that they have been caught in a honeypot and ceases their attempts to gain access.
* The cybersecurity professionals use the information gathered from the honeypot to identify and track down the hacker, potentially leading to their arrest and prosecution.

Honeypots can be an effective tool in the fight against cybercrime, as they allow cybersecurity professionals to monitor and track potential attackers while they are in the process of trying to gain access to a system. This can provide valuable information that can be used to improve security measures and protect against future attacks.

**Demonstration of Honeypot attack:**

First do a Nmap scan on the host machine when the honeypot is not installed.

Text

Description automatically generatedShape, rectangle

Description automatically generated with medium confidence

Install the Honey BOT software and configure it, click on yes to proceed.

Graphical user interface, application, Word

Description automatically generated

Check all the parameters that you want in your honeypot and click on Apply to proceed.

Graphical user interface, text, application

Description automatically generated

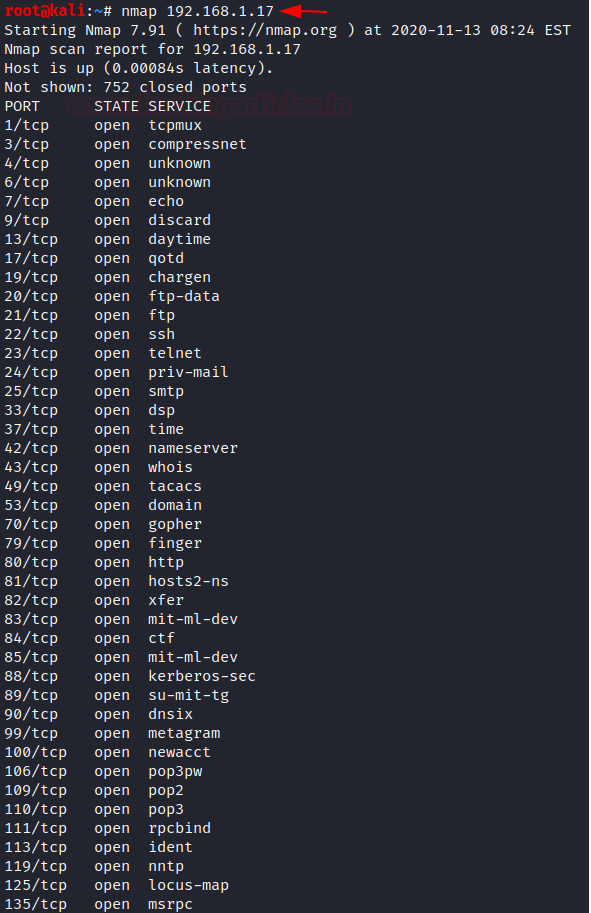
To get email reports on your honeypot, add the recipient email address and click on apply.

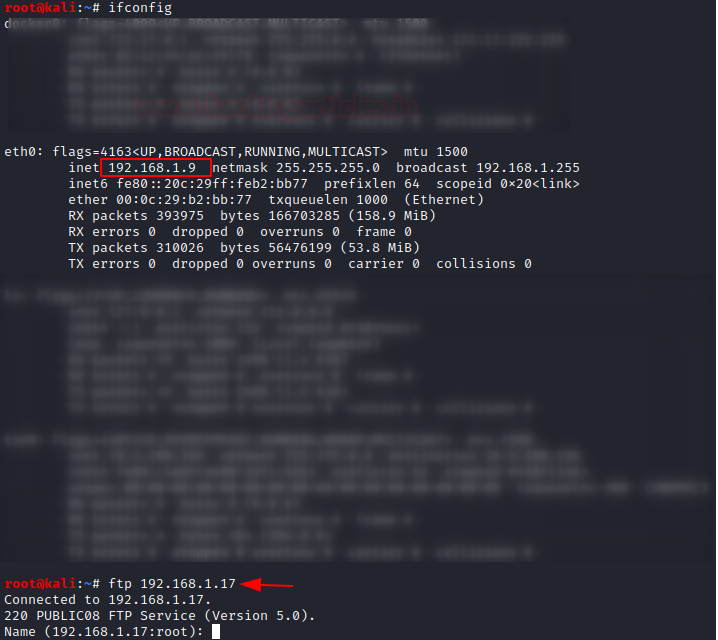
Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generatedIf you want to save the honeypot logs into CSV format, you can apply this setting.

On the attacker, machine performs a Nmap scan and there you will see so many fake services that are open due to the presence of honeypot in the system.

Let us try connecting to FTP from the attacker machine to the host machine.

Graphical user interface, text, application

Description automatically generatedWhere you see the log has been generated of the attacker’s IP and the port that he was connected on.

Graphical user interface, text, application

Description automatically generatedHere you can see a detailed report on the connection that is created by the attacker.

Graphical user interface

Description automatically generatedSimilarly, an SSH connection was initiated on port 22 from another operating system.

Now you can see that log for the same has been generated for the connection created on port 22.

Graphical user interface, text, application

Description automatically generated

**My Brief Reflection on Honeypot:** Honeypots are security resources that are specifically designed to attract and trap cybercriminals. These resources can be used to monitor and track the actions of attackers, gather intelligence on their tactics and techniques, and potentially divert them away from more valuable assets within an organization's network.

One of the main benefits of using honeypots is that they can help organizations to better understand the threats that they face. By studying the behavior of attackers who are interacting with a honeypot, security teams can learn more about the tactics, techniques, and procedures that are being used by attackers and use this information to improve their defenses.

However, there are also some potential drawbacks to using honeypots. One of the main concerns is that they can be resource-intensive to set up and maintain. Additionally, honeypots can potentially attract a lot of unwanted attention from attackers, which can put additional strain on an organization's security team.

Overall, honeypot attacks can be a useful tool in an organization's security arsenal, but they should be used carefully and with a clear understanding of the potential risks and benefits.

**Simulating Dos Attack**

A Denial of Service (DoS) attack is a type of cyber-attack in which a perpetrator seeks to make a particular computer or network resource unavailable to its intended users by overwhelming it with traffic or requests for data. This can be done in a variety of ways, such as sending a flood of messages to a server or website, or by exploiting vulnerabilities in a network to cause it to crash or become otherwise unavailable.

* Graphical user interface, text, application, email

  Description automatically generatedYou must set up a Wireshark program on our target system, which helps analyze the network traffic being sent and received from the instance.
* Text

  Description automatically generatedTo attack the target, you need to get its IP address, which acts as an identifier for the system. You can find the local IP address by using the command “ipconfig”.
* A screenshot of a computer

  Description automatically generated with low confidenceTo launch the attack, we will need a program called Hping3. It is a command-line tool that acts as a packet generator and analyzer for the TCP/IP protocol. You will use the IP address detected in the previous image to start the attack. The command to be given using hping3 is:
* Graphical user interface, application

  Description automatically generatedOnce this command is run, you can watch the Wireshark window on our target system and watch a flurry of requests being sent from a single IP address. After a few seconds, the system becomes completely unresponsive due to the lack of processing power in handling so many requests simultaneously.

**My Experience on DDOS Attack Using Node JS:** I demonstrated DDOS attack using Node JS. As you might have noticed, first I included a required node module which simulates DDOS attack with optional target website link.

Text

Description automatically generated

A picture containing text

Description automatically generatedWe can see the loop requests in the console. We sent 30 requests in a row and none of them returned with an error response.

**My Brief Reflection on DDOS Attack:**

DDOS attacks can have a significant impact on individuals, as well as on organizations. If you are a victim of a DDOS attack, you may find that you are unable to access certain websites or online services, which can be frustrating and inconvenient. In some cases, you may also be at risk of losing access to important personal data or sensitive information.

It is important for individuals to be aware of the risks associated with DDOS attacks and to take steps to protect themselves. This can include using strong and unique passwords, avoiding clicking on links or downloading attachments from unknown sources, and keeping your devices and software up to date with the latest security patches.

Additionally, it is a good idea to be cautious when accessing sensitive or personal information online, and to use trusted websites and services whenever possible. By taking these precautions, you can help to reduce your risk of being caught up in a DDOS attack or other cyber security incident.

**Implementing Port Security:**

Port security is a method of protecting network devices from unauthorized access or activity. It involves the use of various measures to prevent unauthorized devices from connecting to a network through physical port connections, such as Ethernet ports or USB ports.

There are several ways that port security can be implemented:

MAC address filtering: This involves configuring a network device to only allow connections from devices with specific MAC addresses. This can be effective in preventing unauthorized devices from connecting to the network but can be difficult to maintain if there are frequent changes to the list of authorized devices.

Port lockdown: This involves disabling unused ports on a network device or restricting access to certain ports to specific users or devices. This can help to reduce the risk of unauthorized devices being connected to the network.

Network access control (NAC): This involves implementing controls to verify the identity and security posture of devices that are attempting to connect to the network. NAC systems can use various methods to verify the identity of devices, such as requiring the use of a certificate or login credentials.

Overall, port security is an important aspect of network security, and implementing effective measures can help to reduce the risk of unauthorized access or activity on a network.

17330118 – Mustafa Guner