Home Network Honeypot

Joshua Brisson

UCCS

CS 4980

Home Network Honeypot

Abstract:

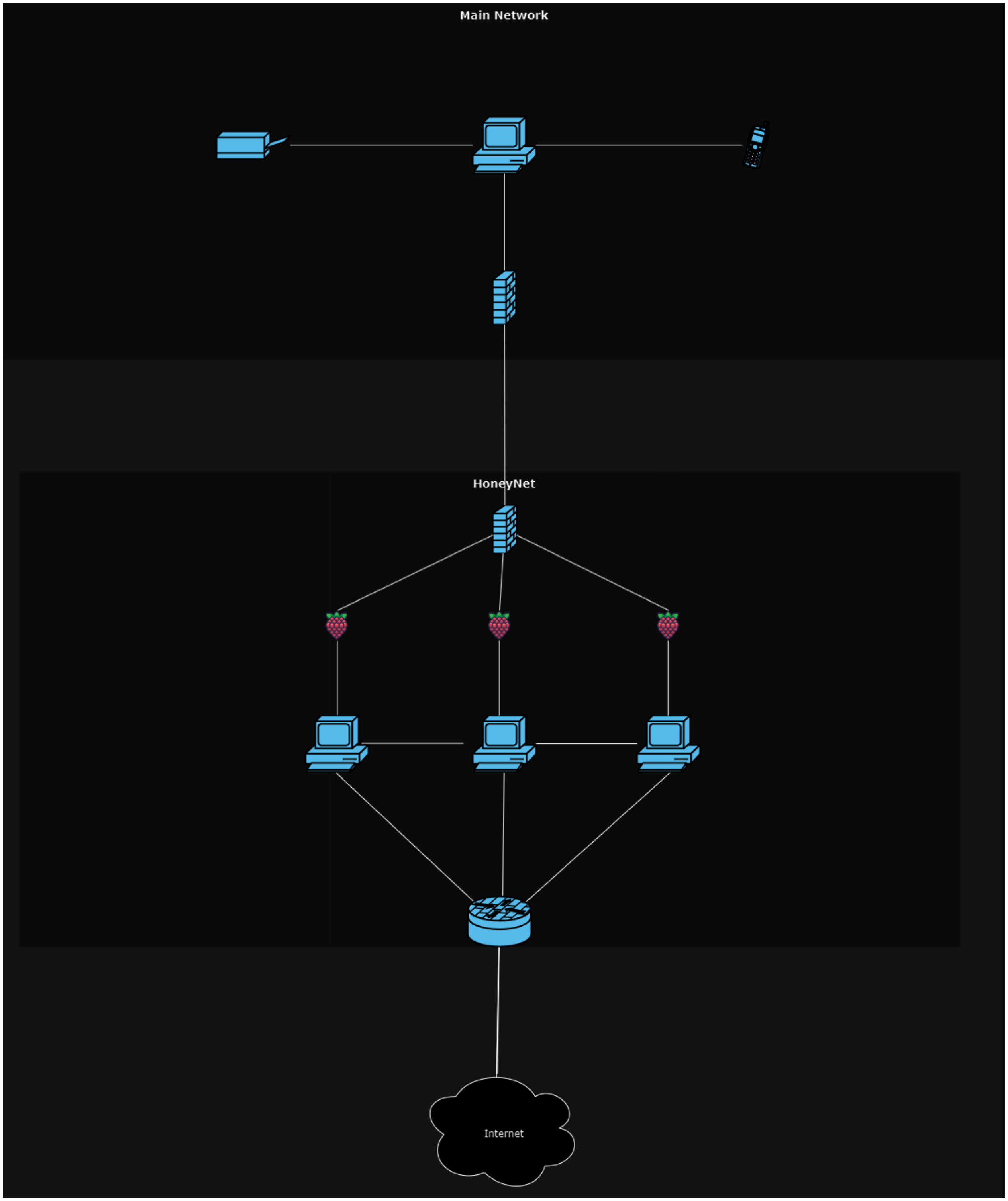
The project that I have decided on is to set up a honeypot/honeynet on my home network to monitor brute force attacks. The monitoring system will record where the attacks originated from, the usernames and passwords used to brute force into the honeynet, the commands used once inside the honeynet, and the time and date of the attacks themselves.

The driving mission statement behind this project does not necessarily come from a company perspective. Instead it comes from the perspective of a future cybersecurity professional trying to establish and develop the skills necessary to succeed. However this is not to say that the project has no applications when it comes to company implementation. A mission statement of a business implementing this system could be: As a software as a service based company we want to provide a useful and available service to our customers. As a smaller company we do not have the resources to have the newest and most expensive security measures. We need a method of identifying malicious actors using a system that prevents any harmful effects on our services while also allowing us to prevent future attacks.

Objectives:

- Monitor malicious activity, specifically over the ICMP and SSH ports.
- Identify malicious actors and keep track of malicious IPs and patterns
- Isolate malicious actors in a contained virtual system
- Prevent service disruptions on main network
- Log actions taken within the contained virtual system

System Map:



Vulnerabilities:

As shown above there is a separation as well as a number of firewalls between the established honeynet and the main network. While this is not a fully descriptive model of the entire network as not all traffic goes through the honeynet this diagram regards strictly the ICMP and SSH traffic directed through the honeynet.

While there are a number of safeguards to prevent any malicious actor from accessing the main network there are still vulnerabilities as the presence of a honeynet invites malicious actors to try and access the system. In order to prevent privilege escalation and lateral movement within the system there are a number of vulnerabilities to be addressed. The first of which is the access of the honeynet through means other than the monitored and established routes. In order to prevent this strict firewall rules are implemented within the router to prevent the transferring of inbound traffic to the honeypot machines unless it is the known and monitored connections that the honeynet is prepared for.

Another mitigation technique to prevent any kind of lateral movement or bypassing of the virtual environments is to limit the connectivity that the raspberry pies have with the main network. The first technique is to simply limit any kind of communication between the raspberry pies and the main network unless necessary as well as limiting packet transfer outside of the ssh packets necessary to manage the virtual environments and honeypot systems. This is done through a firewall which has the default of dropping all packets unless they are preapproved packets sent by the raspberry pies after a connection is established from the main network.

However this potentially leaves the vulnerability of the ssh connection with the raspberry pies themselves. This can be mitigated through the establishment and use of SSH keys and disabling any other kind of access (for example an admin account). So without the presence and use of the pre established SSH keys during setup it will be very difficult to access the raspberry pies themselves.

Another layer to prevent any kind of access to the administrative portion of the honeynet is the redirection of the incoming traffic to a different port. By running the honeypot on a separate port from the standard SSH port (22) and redirecting any traffic with a destination port of 22 to the new port prevents any kind of confusion or access to the administrative portion of the honeynet. You can even go a step further and redirect any actual SSH communication with the raspberry pies to a different port.

System Security:

There were a number of security methods applied to the system outlined above. The first of which were the multiple firewall protocols put in place to separate both the systems and to limit any kind of communication between the networks that was not absolutely necessary. These security measures were implemented in order to prevent any kind of privilege escalation or lateral movement within the networks if a malicious actor realized they were in a honeypot and was able to escape it.

A second security method was the "disconnect" of the virtual environment hosting raspberry pies from the main network. The only connection that the devices have with the main network is through the use of the pre established SSH keys used to administer the honeynet. Without the SSH there should be no access directly to the raspberry pies outside of the virtual environments.

Policies:

- No communication between the raspberry pies and main network is allowed outside of administration of the honeynet
- No access to the administration of the honeynet is allowed outside of the SSH keys generated during setup
- Each raspberry pi is isolated with the exception of the virtual environments which are permitted to communicate with one another
- No execution of commands on the raspberry pi is permitted from outside users. Only the emulation of command execution through the feedback of text by the virtual machine.
- No communication with outside networks by the virtual environments is allowed outside of the preapproved ssh and ICMP packets and sockets.