HONEYPOT DETECTION SYSTEM

[1] Pinak Pathak, [2] Dr. Poonam Gera

[1] Student, [2] Professor of the department
LNM Institute of Information Technology, Jaipur

Abstract: Honeypots are important in terms of research purposes as well as to protect individual organizations. They can help researchers keep themselves up-to-date regarding the new techniques used by hackers to gain access. They act as an Intrusion detection system in private organizations that alert the administrators regarding the unauthorized accesses made from outside the network. It sometimes outshines the real intrusion detection system(IDS) as these technologies can have difficulty identifying unknown attacks or behavior, whereas to honeypots, all the activities are anomalous making new and previously unknown attacks stand out.
Honeypots help us to log the information as to what the malicious user is trying to do with the system and can analyze the intent of the attacker.

Index Terms : Nmap, honeypots, s7comm, modbus, ports

I Introduction :

Honeypots are computers set up on a network primarily to detect unauthorized attempts made to access the network or computers within the network. They usually contain intentional security flaws, weak protocols, and other such issues that lure attackers to exploiting them. Once accessed these honeypots log every bit of data, protocol opcodes, and other such information sent to it. This helps identify and study the methods used by attackers to gain unauthorized access.
HoneyPot is basically a trap for malicious users as it is a weak system with unimportant data just to make it easy for hackers to attack and then we can note the activities of hackers thus the name given Honeypot.

Is this research helping the hackers?

NO - Honeypot Detection is done so as to help avoid default settings and flows that let attackers know that the systems they have access to/ trying to gain access to the honeypot.
The eradication of these flaws will prevent the attackers from gaining access to the real Operating System interface/shell and let them interact only with the virtual honeypot environment we have created for them.

II Existing System :

The existing tools to scan the machines perform only common tests. By common tests, we refer to tests like OS combination or SSL validation or check executed on its websites. Therefore the given system does not help in increasing the efficiency of a honeypot.

III How is the Honeypot detection process being done :

The basic component of Honeypot Detection is port scanning. By default, the script scans all the ports from 0-65535. The user however can pass his preferred ports to be scanned changing this value. Various tests will be performed on the target machine each of which returns a value related to the probability of the target machine being a honeypot based on their relevance. The script also returns a report post the completion of all tests as well as real-time logs regarding each test.

In this project, I am implementing checks on specific protocols. Protocols that are usually seen as a part of common honeypots. Such tests include the S7comm test, Modbus test, and furthermore. Tests will be performed on the target machine each of which returns a value related to the probability of the target machine being a honeypot based on their relevance.

The tests that are currently implemented are:

1. An O.S combination test.
2. Port Service Combination test
3. S7comm protocol test
4. SSL validation test.

1. OS COMBINATION TEST :

This test is run on the basis of the port scanning data returned by Nmap. This test searches all the possible target OS family's returned by the Nmap for anomalies.

For example, if Nmap predicts with 90% possibility that the Target O.S could be a Windows machine and with a 50% possibility that it is a Linux machine, then this an anomaly and could be due to the possibility that the target machine contains a virtual O.S running on it.

2. PORT SERVICE COMBINATION TEST :

This test is also run on the basis of the port scanning data returned by Nmap. Nmap returns a large set of services running on all of the open ports on the target machine. This tests for the Odd combination of such services running on the target machine.

For eg: A machine running a Microsoft SMB service and a Linux based Openssh service can be considered as an anomaly.

3. S7COMM PROTOCOL TEST:

S7comm protocol is a network protocol primarily used by Siemens's S7 PLCs. This protocol is often being run on many honeypots as it contains many weak links. The primary objective of this test is to connect to this service if running on the target machine and get a list and details of the PLC controlled by it. Honeypots are usually left with default settings and therefore the complete data regarding these PLCs are not entered.

4. SSL CERTIFICATE VALIDATION TEST:

The objective of this test is to attempt to connect to the HTTPS service running on the target machine and attempt to verify the validity of its SSL certificate. Honeypots usually don't have a valid SSL certificate and thereby FAILS this test. The Primary reason to use SSL is to secure the information sent across the internet by encrypting it so that only the intended recipient can access it.

Assumptions and Constraints :

- Here we have made probabilistic assumptions using importance or priority factors. We have assigned **12.5%** weightage to both Port Service and OsCombination Test, **5%** to SSL Validation Test, and **70%** to S7comm Test.
- On the basis of the above assumptions, the final report generated after performing tests will pass through the above parameters, and according to weightage the final probability of whether a system is a HoneyPot or not will be evaluated.

These Assumptions are done on the basis of the importance of each test(S7comm test being the most important and best way to detect a honeypot in comparison to the other three mentioned above) and also the total number of tests performed. I I had included the Modbus test also then the probability percentage would decrease for each of the other four tests and the highest would be awarded to the modbus test.

IV Results :

CASE 1:

When the OS Combination and Port Service test fails and SSL and S7comm tests are passed then we can say that with the certainty of 12.5+12.5=25% that our target system is Honeypot.

CASE 2:

When all tests except the S7comm test are passed then we can say with a 75% probability that the target system is a honeypot.

The target computer I used was my laptop and the final result was that the OS Combination test passed as there was only one operating system installed in it. Port scanning test failed, S7comm test passed and SSL validation test also failed. So overall my laptop was a honeypot with a 12.5 probability only.

V : Language used to write the script - Python 3.5

VI Applications and Uses:

- The system can be used by big companies to protect their servers or honeypots from various malicious attacks and thus saving the data from being used or corrupted by attackers.
- The system can be used by researchers for research purposes to further improve the current existing Honeypot detector.
- This system is used to increase honeypot efficiency so that it is made better and close to the ideal honeypot where attackers can attack it easily and can get traced by the organization in which the malicious user tried to hack.

VII Conclusion :

1. We have finally found a chance or a probability of whether a target system is a HoneyPot or not.
2. We can further make it more efficient and close to the best model which can detect the best honeypot already present in today's world by including some high level more reliable tests like Modbus, BACnet.
3. This system can be used by organizations to check their existing honeypots to improve their efficiency by analysing the information provided by this system after the tests performed on the honeypot.

VIII Future Work :

- Adding More tests like Modbus and BACnet are two more such tests that can be added to our system for improving its capability to detect a well-developed honeypot. Modbus is a communication protocol for industrial devices developed in 1979 used for communicating with PLCs. BACnet is also a communication protocol for building automation and control (BAC) networks. It provides a mechanism for computerized building automation devices to exchange information.
- Adding UDP functionality is also one of the improvements in our system.

IX References :

[1] Honeypot-based intrusion detection system: A performance analysis
Authors - Janardhan Reddy, Santosh Kumar Bharti, Sambit Kumar Mishra.

[2] T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments", *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop 2005. IAW '05.*, pp. 29-36, 2005.

[3] Identifying S7comm Protocol Data Injection Attacks in Cyber-Physical Systems
Authors - Oliver Eigner, Philipp Kreimel, Paul Tavolato

[4] Honeypot based Secure Network System
Authors - Yogendra Kumar Jain, Saurabhi Singh