Lab 7 - Intrusion Protection

EECS 4481 4.0 Computer Security Lab, Winter 2015

Format: Individual

Learning Objective: To study intrusion protection strategies, and gain hands-on experience with different types of protection methods, such as intrusion detection and prevention software (IDPS), auditing, and honeypots.

1 Snort

Snort is an open source network intrusion prevention and detection system that has been deployed on the Toolbox computer.

Develop *snort* rules for the following hacks:

- Any packet of size > 100 bytes from network 192.168.102.0/24 designated to port 80
- Any packet that contains the string "Hello World!"
- Any packet that is designated to a non-running service in the domain controller
- Any port scanning activity (assume that the intrusion uses *nmap* and/or *hping3* for port scanning).

Report: Present and explain the snort rules you developed.

2 Honeypots

A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers.

Your task is to create a honeypot on a computer of your choice (the Toolbox computer has the *honeyd* and *labrea* software for Linux). You must also configure snort to detect attacks on the honeypot.

Report: Explain how your honeypot is configured, and discuss how to identify malicious or unauthorized access attempts by using honeypots.

3 System Auditing

The management team has decided to store all the company's sensitive documentation in a shared folder. Your task is to create a shared folder on the domain controller (similarly to the one in Lab 1) and allow users read/write/update/delete access to the shared folder. The new shared folder will be auto-mounted for all company users. You should document all changes to the domain controller and any other configuration modifications.

What is the most critical auditing policy for the shared folder? Design and implement it.

Report: Justify the choice of your auditing policy, and explain how to configure it.

4 Infrastructure Protection

- Create a back door using *netcat*
- Using any of the tools above, prevent an intruder from using the back door

Report: Describe the steps you followed to install the back door, and the approach you used to prevent intrusion.