SEC520

Intrusion Detection

Today's Objectives

Intrusion Detection:

- Purpose
- Intrusion Detection Basics:
    - Monitoring (Logging):
        - Unusual Processes (network usage, tasks)
        - Unusual User Accounts
        - Unusual Files
        - IP Tables (Logging)
- Intrusion Detection Systems
    - Purpose
    - Software Example: Tripwire

Intrusion Detection

- In many information systems (eg. accounting, management, content management), there are levels of **controls** in order to help maintain the accurate, safe, and smooth operation of an organization.
- The levels of controls have costs (in terms of consequences of failure or exploitation) associated with them.
- The basic levels of controls are:
  - **Prevention** (least expensive)
  - **Detection** (more expensive)
  - **Correction** (most expensive)

Intrusion Detection

- For example, performing an audit to help detect fraud is more expensive than having a system in place to prevent fraud from happenning in the first place. Another example would be going to court to sue an indivual for money stolen from the company (possibly not all money would be recovered, less lawyers' fees) – this would be very costly.

- So far, we have studied ways to help harden our systems. This not only involves applications and settings, but setting up and maintaining a security system based on the **8 Rules of Internet Security**.

- In this lesson, we will study the second level of control: namely instruction Detection practices, as well as learning about **Intrusion Detections Systems**, mentioning a commonly-used Intruction Detection System (called **tripwire**) to monitor any weaknesses in our security perimeter in order to make corrections and improvements to our security system.

Intrusion Detection

Monitoring:

In order to detect penetration (or attempts of penetration) of computer system, it is important to view logs and note any unusual activity that occurs on the computer system.

Monitoring Activity:

- Reduced System Performance
- Usual Activity (Processes)
- Network Usage
- User Accounts
- Unusual Files
- Unusual Log Entries

Intrusion Detection

Reduced System Performance:

Learn to become familiar with command processes

List running processes:

In Linux:

- **uptime** (look at “load average”)
- **df** (look at available disk space)

In Windows:

- **Task Manager** > **Processes and Performance**
- Run benchmark programs
- Look for unusual system crashes

Intrusion Detection

Unusual Activity (Processes):

Learn to become familiar with command processes

List running processes:

In Linux:

- **ps -aux** , **lsof -p [pid]**
- **chkconfig --list** (or **systemctl list-units --all**)

In Windows:

- **taskmgr.exe** , **wmic process list full**
- **services.msc**
- **net start** , **sc query**
- **tasklist /svc**

Intrusion Detection

Unusual Network Usage:

Detect if hackers are using “sniffer applications”

Run Network Utiltities:

In Linux:

- **netstat -nap** , **lsof -i**
- **arp -a**

In Windows:

- **netstat (-na) (-nao 5) (naob 5)**
- **net view \\\127.0.0.1** , **net session** , **net use**
- **nbstat -S**
- **Netsh firewall show config**

Intrusion Detection

Unusual User Accounts:

Detect if hackers have created irregular accounts

Run Network Utilities:

In Linux:

- **sort -nk3 -t: /etc/passwd | more** (look for UID < 500)
- **egrep ':0+:” /etc/passwd** (UID 0 accounts)

In Windows:

- **lusrmgr.msc (groups, Administrators,** look for same group members**)**
- **net user**
- **net localgroup administrators**

Intrusion Detection

Unusual Files:

Look for large files, and unusual SUID root files:

Run Utiltities:

In Linux:

- `find / -size +10000K -print`
- Look for hidden files
- `lsof +L1`
- `rpm -Va | sort`

In Windows:

- **Start > Search > For Files or Folders**
  Search Options > Size > At Least 10000 KB
- **regedit** (search for unusual entries)
- `reg query <reg key>`

Intrusion Detection

Unusual Log Entries:

View log-files to note any irregular / suspicious activity:

Run Utilities:

In Linux:

- **System log Files** (in /var)
- Logins (remote, local), **rpc** programs
- **Apache** logs (stating "error")
- Reboots, application starts

In Windows:

- **eventvwr.msc** (Graphic tool)
- **eventquery.vbs | more**
- **eventquery.vbs /L security**

Intrusion Detection

IPtables:

Iptables is the built-in firewall for LINUX. While this program can be controlled by different GUI's, we are going to investigate the powerful command line interface for this program to choose what data is allowed into, out of and through our computer.

Essentially, Iptables is a list of rules. Each rule is placed into a particular chain and when data is sent into, out of or through a PC the data is checked against these rules. If the data matches a particular rule, it then must “jump” to a condition.

Intrusion Detection

Iptables:

In OPS235, you learned how to use Iptables to redirect the port for SSH.

In addition, Iptables rules can be set-up to LOG entries to report on unusual activity that would be associated with system intrusion.

Intrusion Detection

Intrusion Detection Systems (IDS's) / Honey Traps:

Intrusion Detections Systems (IDS) are applications that allow for the automatic configuration, monitoring, flagging and reporting of unauthorized access to an existing computer system.

There are many, many products that are available (both open-source and proprietary).

Intentional vulnerable systems (**Honey-traps**) can be employed to monitor intrusion attempts to silently harden your server(s).

Intrusion Detection

IDS Example: Tripwire

Tripwire is an open-source (multiple platform) network security tool.

After installation, and configuration, Tripwire scans the system (on demand, or via a scheduling program) to report changes of the current system (files, processes, etc), against a database containing the standard (i.e. the normal “clean” system).

Lab Time

Perform:

Lab 7: Intrusion Detection (Linux)