



Security Guidelines For Detecting Signs of Intrusion

Document ID: GUI-0002

Information Technology Protective Security Services Pte. Ltd.

Block K, Information Technology And State Store Building,

Jalan Gadong BE1110,

Negara Brunei Darussalam

Tel: +(673) 245 8001

Fax: +(673) 245 8002

Email: cert@brucert.org.bn

Website: <http://www.brucert.org.bn>

DISCLAIMER

Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.

This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore, this guide does not address site-specific configuration issues. Care must be taken when implementing this guide while using mission specific and mission critical products.

The security changes described in this document only apply to the intended operating system, service or product and should not be applied to any other software.

SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED, WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Document Version History

Version	Reason for Issue	Date of Issue
1.00	Draft	20 th January 2005
1.02	First Release	4 th February 2005
1.03	Second Release	14 th February 2005

Related Documents

Document ID	Document Name
GUI-0003	Intrusion Detection System Security Guidelines

Table of content

LIST OF FIGURES	5
EXECUTIVE SUMMARY	6
1. INTRODUCTION	7
1.1 PURPOSE AND SCOPE	7
1.2 ASSUMPTIONS	7
1.3 COMMONLY USED TERMS.....	7
2. DOCUMENT ORGANIZATION.....	9
3. WHAT IS INTRUSION.....	10
3.1. WHO ARE THE POTENTIAL INTRUDERS	11
3.2. SOURCES OF INTRUSIONS.....	12
4. DETECTING SIGNS OF INTRUSION.....	13
4.1. DETECTING UNKNOWN USER ACCOUNTS.....	13
4.2. REVIEW UNKNOWN APPLICATION & PROCESSES RUNNING.....	13
4.3. DETECTING UNKNOWN SERVICES	15
4.4. MONITOR AND REVIEW SYSTEM RESOURCES	15
4.5. MONITOR CURRENT LOGGED ON USERS OR COMPUTERS	17
4.6. NETWORK UTILIZATION	17
4.7. CHECK NETWORK STATISTICS FOR LISTENING, AND ESTABLISHED CONNECTION	18
4.8. CHECK FOR UNKNOWN INSTALLED SOFTWARE OR PROGRAMS.....	18
4.9. CHECK FOR SUSPICIOUS FILES OR FOLDERS IN THE SYSTEM.....	18
4.10. SETUID SETGUID FILES (LINUX/UNIX)	19
4.11. CHECK THE SYSTEM BINARIES TO MAKE SURE THEY ARE NOT TAMPERED	19
4.12. REVIEW FILES OR FOLDERS ATTRIBUTES.....	19
4.13. CHECK FOR HISTORY OF COMMANDS EXECUTED (LINUX/UNIX)	19
4.14. CHECK FOR ALL LOGS.....	19
4.15. CHECK FOR EXISTING NETWORK DEVICES LOGS	20
4.16. CHECK FOR SERVER LOGS (WEB, FTP SERVERS)	21
4.17. CHECK INVALID NETWORK CONFIGURATION.....	21
4.18. CHECK FOR VIRUSES USING LATEST VIRUS DEFINITION	21
4.19. CHECK FOR UNKNOWN REGISTRY ENTRIES (WINDOWS)	22
4.20. CHECK FOR SCHEDULED TASK.....	22
5. RECOMMENDED TOOLS	23

5.1. MONITORING TOOLS 23

5.2. INTEGRITY CHECKSUM 23

5.3. INTRUSION DETECTION SYSTEM..... 24

5.4. NETWORK MONITORING TOOLS 24

5.5. ROOTKIT CHECKER..... 24

5.6. REGISTRY MONITORING TOOL 25

5.7. WEB SERVER LOG ANALYZERS..... 25

5.8. FIREWALL LOG ANALYZERS 25

6. CONCLUSION 26

REFERENCES..... 27

List of Figures

FIGURE 1: WINDOWS TASK MANAGER..... 14

FIGURE 2: WINDOWS TASK MANAGER..... 16

FIGURE 3: EXAMPLE OF CHECKPOINT FIREWALL-1 LOG 20

FIGURE 4: EXAMPLE OF MICROSOFT INTERNET INFORMATION SERVICE LOG..... 21

Summary

This guide shows how to analyze and detect sign of intrusion using built-in tools, utilities, third party freeware tools, and determine whether a computer system has been compromised. Verify what data, system and network are being attacks and what breached confidentiality, integrity and availability. Furthermore, this guideline could help increase the knowledge and ability of security professionals, system or network administrators, or even home users to detect signs of intrusions, and minimize the risk of exposure to intrusions and possible damage to their system.

1. Introduction

1.1 Purpose and Scope

The purpose of this document is to provide guidelines and best practices for users, administrators and security professionals of networked computer systems on detecting signs of intrusion. This guideline is appropriate for Windows NT 4.0, 2000, XP or later and Linux/UNIX operating systems in a networking environment.

This document will not mention on how to secure workstation, network server, web server and prevention against an intrusion. The guidelines recommended below are designed to help you prepare and detect intrusions by searching or reviewing unexpected or suspicious behavior and "fingerprints" of common intrusion methods.

1.2 Assumptions

This practice is appropriate for security professional, network and system administrator, security personnel and also home users who has basic knowledge on:

- Information security
- Networking TCP/IP
- Windows NT, XP, 2000 or later
- Linux/Unix Operating System

1.3 Commonly Used Terms

BIOS – Basic Input/Output System

Backdoor – Backdoor is a program/software used by intruders to maintain their unauthorized access, once they have compromised the system.

IDS – Intrusion Detection System is defined as an alerting tool which has the capability to notify the user or administrator when intrusion occurs based on known signatures.

CGI – Common Gateway Interface is an interface program that enables an Internet server to run external programs to perform a specific function.

SMB – Server Message Block is a network file sharing protocol. Communication over SMB occurs mainly through a series of client requests and server responses.

Rootkit –Rootkit is a set of tools and utilities that an intruder can use to allow hackers to seek out usernames and passwords, launch attacks against remote systems, and conceal their actions by hiding their files and processes and erasing their activity from system logs and other malicious stealth tools.

DoS – Denial of Service is one of the most common types of attacks used by attackers/intruders to make an online service or computer unavailable to its legitimate users.

NetBIOS - Network Basic Input Output System is a protocol in Windows.

Firewall – A network security device used to block or allow incoming or outgoing network traffic depends upon security policy.

Scanning – One of the most common methods for network reconnaissance which involve probing a computer system for open ports or closed ports.

TCP/IP - Transmission Control Protocol/Internet Protocol is a suite of protocols containing set of rules that tells computers how to exchange information over the Internet.

Port - One of the network input/output channels of a computer running TCP/IP. In the World Wide Web, port usually refers to the port number a server is running on. The default port for WWW servers (Web Server) is 80.

Exploit - A program or technique that takes advantage of vulnerability in software and that can be used for breaking security, or otherwise attacking a host over the network.

2. Document Organization

An overview of all the topics to be covered in the guidelines is given below:

- **What is Intrusion** – Description of the term intrusion and three main concern areas in information security (Confidentiality, Integrity and Availability).
- **Who are the potential Intruders** – Provides examples and types of intruders, their motives and targets.
- **Sources of intrusions** – Brief description of possible ways, intruders can use to penetrate into a computer system.
- **Detecting Signs of intrusion** – Provides guidelines and best practice on how to identify or detect signs of intrusion using built-in commands in Windows and Linux/Unix operating systems.
- **Recommended tools** – Provides third party tools to aid in detecting signs of intrusion.

3. What is intrusion

The term intrusion in information security is used to describe an unauthorized access to computer systems. As information technology becoming more advance, intruders will also never stop looking for new techniques to break into a computer systems.

They may attempt to breach your network's perimeter defenses from remote locations, or try to physically infiltrate your organization to access information resources. Intruders seek old, un-patched vulnerabilities as well as newly discovered vulnerabilities in operating systems, network services, and protocols and take advantage of both. They develop and use sophisticated programs to rapidly penetrate your systems.

Even if your organization has implemented comprehensive information security protection measures (such as firewalls), it is essential that you closely monitor your information assets and transactions involving these assets for signs of intrusion. Monitoring may be complicated because intruders often hide their activities by changing the system once they break into it. An intrusion may have already happened without being noticed because everything seemed to be operating normally.

Information security is concerned with three main areas :

- Confidentiality - information should not be accessed by unauthorized users.
- Integrity - information should only be modified by authorized users.
- Availability - information should always be accessible to legitimate users who need it.

Once intrusion happen it will affect those three main areas mentioned above. For example, if a system is being compromised and the intruder manage to grab administrator's password, it affects the confidentiality

A general security goal is to prevent intrusions. However, because no prevention measures are perfect, a strategy for handling intrusions that includes preparation, detection, and response. This document focuses on detection and will cover a few on preparations.

3.1. Who are the potential intruders

The term intruder used in this document means an individual who penetrates and gain unauthorized access to information, data, computer programs, computer systems.

Following are the most common intruders for a network:

- **Internal Employees**

Various studies indicate that internal employees are responsible for more than half the attacks. These types of people cause more damage than the actual hackers. Disgruntled employees, contract employees and sacked employees fall in this category.

- **Hackers**

Hackers are a real danger to most organizational computer systems linked by networks. From outside the organization, sometimes from another continent, hackers break into computer systems and compromise the privacy and integrity of data before the unauthorized access is even detected. The hacking activity is not limited to fraud but also includes the ability to break into systems resulting in the degradation or disruption of system availability.

- **Black-Hat Hackers**

Black-hat hacker is a hacker who breaks into a computer system or network with malicious intent of destroying files or stealing data for some future purpose. He may also make the exploit known to other hackers and/or the public without notifying the victim.

- **Gray-Hat Hackers**

Gray-hat hackers are those who spend their time in finding out vulnerabilities in software and publishing them for both black-hat hackers and software developers. But this information also goes into wrong hands who exploit these vulnerabilities to their benefit.

- **Hactivists**

Hactivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of Hactivism is said to be a Hactivist. A Hactivist uses the same tools and techniques as a hacker but does so in order to disrupt services and draw attention to a political or social cause.

- **Script Kiddies**

Script Kiddies is a term used to describe a novice who aspires to be a hacker, but does not have the knowledge and technical skills. They use existing and freely available techniques, programs or scripts and exploit weaknesses in other computers on the Internet. They often do it randomly and with little understanding of the potential harmful consequences that may occur.

- **Competitors**

Competing organizations can try to hack into your network or system to gain that extra edge in their business. The types of information they usually look for are related to manufacturing and product development, sales and cost data, client lists, technology, research and planning.

- **Industrial Espionage**

Industrial espionage involves commercial spying on competitors for the purpose of gaining proprietary information or data which are not easily obtainable or legitimately for the benefit of another company or organization.

3.2. Sources of intrusions

The primary ways intruders can get into a system:

- **Physical Intrusion**

If intruders have physical access to a machine they can just remove the disk drive (and read/write it on another machine). Even BIOS protection is implemented, it can still be bypassed. Virtually almost all BIOS have backdoor passwords.

Physical security must be taken into account, for example a CCTV to monitor activity in a server room, or Security Guard to prevent unauthorized personnel to enter.

- **System Intrusion**

This type of attack assumes the intruder is an authorized user who already has a low-privilege user account on the system. If the system is not updated with the latest security patches, there is a possibility that the intruder will be able to use a known exploit in order to gain additional administrative or higher privileges on the system.

- **Remote Intrusion**

This type of hacking involves an intruder who attempts to penetrate a system remotely across the network. The intruder begins with no special privileges. There are several forms of this hacking. Normally the intruder will start by gathering information, probing for active hosts, scanning for open port or services and gather the target's vulnerabilities. The intruder will run known exploits to gain access to the target system.

If logical security is in place, such as firewall, it would help to deter the intruder from penetrating into the system.

4. Detecting signs of Intrusion

The best approach before detecting sign of intrusion is to prepare documentation of all the current and latest system state, for example legitimate user or group accounts, installed programs or software. Continuous monitoring of systems for anything unexpected or suspicious is crucial.

4.1. Detecting unknown user accounts

Creating user accounts are one of the basic ways used by intruders to gain access to a computer system thus creating a backdoor for them to re-enter the system.

Reviewing and documenting list of user accounts and groups is very important. Users or System Administrators should know which user accounts are disabled and which are legitimate.

In Windows users or administrators can use the Local Users and Groups snap-in under the Computer Management or the NT User Manager utility to review user and group accounts. You can also use the net user, net group and net local group commands to list users and groups in command prompt.

In Linux environment, user accounts are stored in `/etc/passwd` file. Review all user account names, User IDs and Group IDs, especially with the User ID of 0. The root accounts in Linux/Unix are assigned to User ID 0 which is unique. If there exist another unknown username with User ID 0, indicates someone has manually edited and add the `/etc/passwd` file.

4.2. Review unknown application & processes running

Abnormal system processes are normally causes by Backdoors, Malicious code (virus, worms and Trojan) and Spyware. Use the task manager in Windows NT 4.0, Windows 2000 and Windows XP to view the current running processes and application.

To view Windows Task Manager: Right Click **Task Bar** → Click **Task Manager**

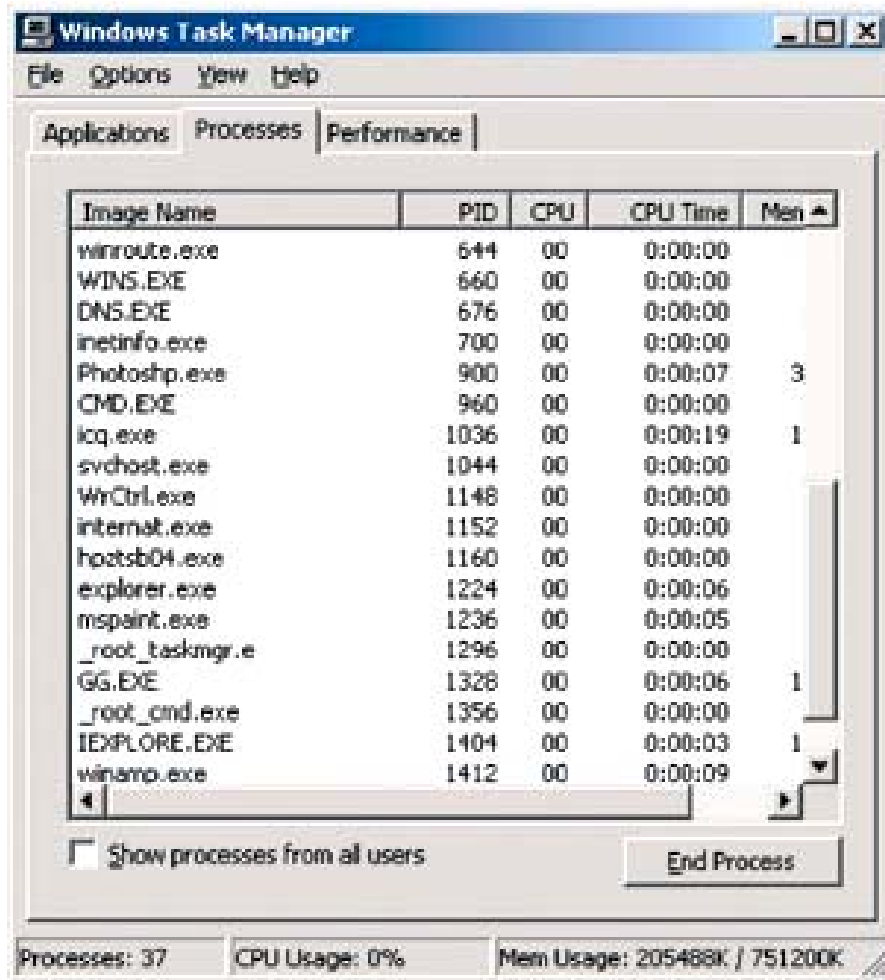


Figure 1: Windows Task Manager

Most Linux/UNIX operating systems are built with a command line tool called “ps”. The “ps” command report the process status. To view all the full listing of process running Administrators or Users, the “ps -ef” command can be executed.

```
$ ps -ef
```

```

    UID    PID    PPID    C  STIME  TTY          TIME CMD
  root      0      0      0 16:02:01 ?        0:00 sched
  root      1      0      0 16:02:01 ?        0:30 /sbin/init
  root      2      0      0 16:02:01 ?        0:14 pageout
  root      3      0      0 16:02:01 ?        2:11 fsflush
  root      4      0      0 16:02:01 ?        0:00 kmdaemon
  root    444    436      0 16:04:53 ?        0:07 /usr/lib/saf/ttymon
  root    364      1      0 16:04:14 ?        0:01 /usr/X/bin/xdm
  root    388      1      0 16:04:20 ?        0:01 /usr/lib/nfs/mountd
  root    390      1      0 16:04:21 ?        0:01 /usr/lib/nfs/statd
  root    392      1      0 16:04:21 ?        0:03 /usr/lib/nfs/lockd
  root    396      1      0 16:04:22 ?        0:02 /usr/sbin/rpcbind
  root    397      1      0 16:04:25 ?        0:00 /usr/lib/nfs/pcnfsd
  root    399    383      0 16:04:25 ?        0:00 /usr/lib/nfs/nfsd -
  root    445    436      0 16:04:53 ?        0:04 /usr/lib/saf/ttymon
    
```

```
root    463      1      0 16:05:16 ?          2:28 /usr/sbin/cron
root    8874     1585    0 11:43:36 console  0:01 ksh
user    9151     7642   80 12:24:50 pts/2    0:02 ps -ef
```

From the output result above, the list can help to determine and detect any unknown process running especially processes with UID named “root”. This could indicate the system is having backdoor. This detection method requires knowledge on the Linux/UNIX system, to be able to differentiate between legitimate processes and unauthorized processes.

4.3. Detecting unknown services

Attackers often install backdoors so that they can easily reenter the system. Some backdoor install themselves as legitimate services that start automatically when windows startup.

To view the status of services running In Windows NT 4.0

Click **Start Menu → Control Panel → Services**

In Windows XP, 2000 or later operating system

Click **Start menu → Programs → Administrative tools → Services.**

Inspect odd or unknown services which are running automatically.

4.4. Monitor and Review System Resources

DoS (denial of services) attack is one method of intrusion where the attacker will try to compromise system availability by crashing a services, fills and corrupt the hard disk space, memory segment manipulation and overload the CPU. View the current CPU usage, physical memory usage, page file or swap file for any unusual activity. This can be viewed by using the Task Manager. Check for any abnormal activity in particular, the presence of high CPU usage.

To view system resources usage In Window XP, 2000 or later,

Press Ctrl + Alt + Del → Click **Performance** tab

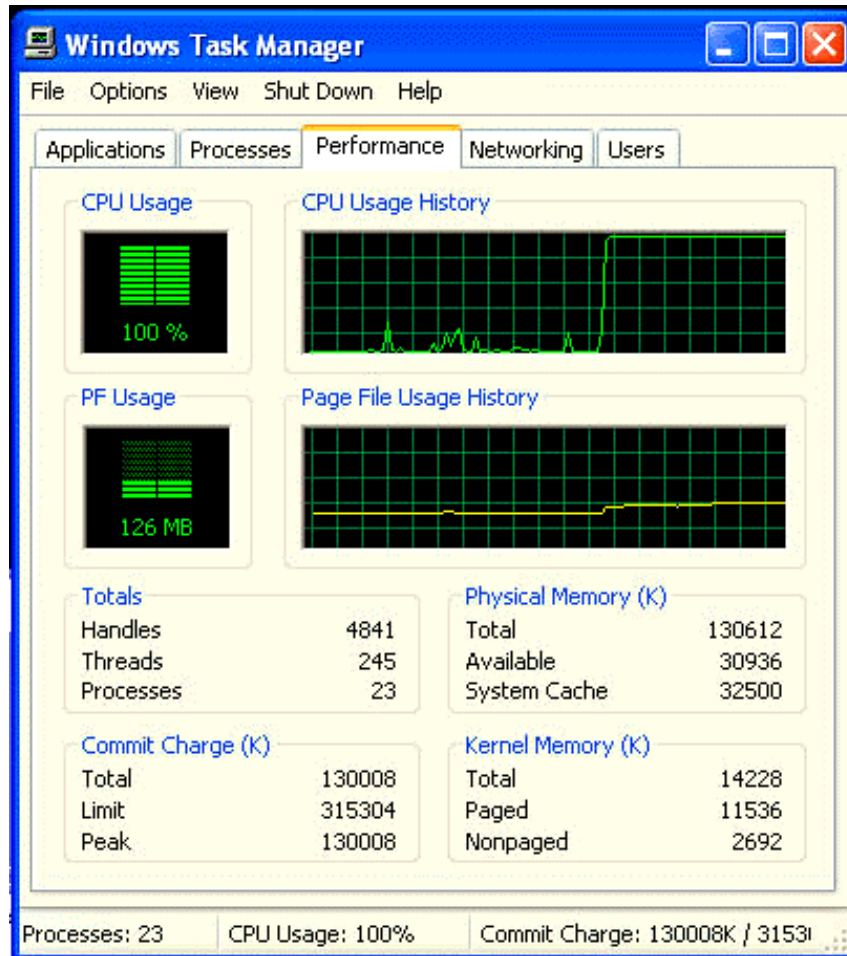


Figure 2: Windows Task Manager

As mentioned earlier, Linux/UNIX operating systems are built with the “ps” command. With “ps - aux” command users are able to view the report process status, CPU usage, and memory usage.

```
$ ps -aux
```

```

USER      PID  %CPU %MEM    VSZ   RSS  TTY  STAT  START   TIME COMMAND
root         1   0.0  0.1  1096   472 ?        S    Jun26   0:03 init [3]
root         2   0.0  0.0     0     0 ?        SW   Jun26   0:00 [kflushd]
root         3   0.0  0.0     0     0 ?        SW   Jun26   0:00 [kpiod]
root         4   0.0  0.0     0     0 ?        SW   Jun26   0:00 [kswapd]
root         5   0.0  0.0     0     0 ?        SW   Jun26   0:00 [mdrecoveryd]
bin        316   0.0  0.0  1088   368 ?        S    Jun26   0:00 portmap
root       351   0.0  0.1  1132   412 ?        S    Jun26   0:00 /sbin/apcupsd
root       412   0.0  0.1  1284   532 ?        S    Jun26   0:00 crond
root       430   0.0  0.1  1240   516 ?        S    Jun26   0:01 inetd
root       444   0.0  0.5  3084  2008 ?        S    Jun26   0:11 named
root       458   0.0  0.3  1324  1324 ?        SL   Jun26   0:00 xntpd
root       473   0.0  0.1  1288   516 ?        S    Jun26   0:00 lpd
root       491   0.0  0.1  1580   640 ?        S    Jun26   0:01 /usr/sbin/dhcpd
root       512   0.0  0.1  1884   716 ?        S    Jun26   0:01 sendmail
root       520   0.0  0.1  1856   752 ?        S    Jun26   0:00 /usr/sbin/httpd
root       557   0.0  0.1  3212   424 ?        S    Jun26   0:00 squid -D

```

Note: High CPU or Memory usage does not directly indicate that an attack or intrusion has taken place, but it could help in detecting signs of intrusion.

4.5. Monitor current logged on users or computers

For windows environment, type “net session” at the Command Prompt to get the list of all NetBIOS session connected to the machine.

Linux/UNIX operating system has a built-in command for checking user who are currently logged on to the system. This is done by using “who” command.

4.6. Network utilization

Most attacks or intrusion are done through network. By monitoring network utilization, an administrator can detect unusual usage of network resources and can react accordingly.

To view network utilization in Windows NT, XP, 2000 or later

Press Ctrl + Alt + Del → **Networking** or

Right Click Task bar → **Task Manager** → **Networking**

4.7. Check network statistics for Listening Ports, and Established connections

Document and review all Protocol statistics and the current TCP/IP connection. Use the “netstat -a” and to show active TCP ports. On Windows XP and 2003 systems, Administrators can use “netstat -an”.

For Linux/UNIX, user can use “netstat -taun”, to view all network connection, routing table interface statistic and masquerade connection.

4.8. Check for unknown installed software or programs.

Check for any unknown software, application, patches and hot fixes that are installed in the operating system. This can be done by periodically checking the “Add or Remove Program”. Administrator and user should document and review all software and application installed.

To view Add and Remove Programs:

Click **Start** → **Control Panel** → **Add or Remove Programs**

4.9. Check for suspicious Files or folders in the system

It is important to search periodically for suspicious file or hidden files. Intruder can conceal tools, malicious code and information (password cracking tools). Review all files or folders that are stored in the system including hidden file.

In windows, to view hidden files open **Windows Explorer** → **Tools** → **Folder Options** → **View** → check “**Show hidden files and folders**” and click **apply**.

For Linux/UNIX check presence of suspicious files in folder such as:-

```
/tmp  
/var/tmp  
/usr/spool
```

User can view all files including hidden files by using the “ls -al” command.

Note: Some intruders hide executable files (backdoor or Trojans) by changing the files extension, other than the normal “.exe”. This type of attack is not easy to detect, but there are few recommended tools that can help to detect such attacks.

4.10. SETUID, SETGUID files (Linux/UNIX)

Inspect if any program or files having SETUID bit turned on. This means, that when any user executes this file he or she will inherit all their file access permissions.

And check the SETGUID setting. Any program or files with the `setguid` bit turned on; anyone who has access to this program will be treated as if they belong to the program group.

4.11. Check the system binaries to make sure they are not tampered

Intruders tend to change program on Linux/UNIX system binaries such as `ls`, `ps`, `cd`, `su`, `netstat`, `ifconfig`, `find`, `du`, `df` etc. Compare the genuinity of these binaries on your system with the last known good backup. A number of file system integrity check tools are currently available. The commonly used tools are **Tripwire** and **MD5sum**.

NOTE: This detection method requires preparation and documentation of the data or information of the system. Records and checksums of last known good backup should be in place.

4.12. Review Files or Folders attributes

In Windows family, user will be able to determine when the file or folder was last modified, created and accessed. Check the time, and date of the file or folder.

Right Click the File or Folder → **Properties**.

For Linux/UNIX, user will be able to view when the files of folder was last modified by typing "`ls -al`" command.

4.13. Check for the history of commands executed (Linux/UNIX)

Display the command history list with line numbers that are being executed, use "`history`" command to get all the list of command being executed from Bash shell. From "`.bash_history`"; Administrator or user will be able to review the last commands used with the bash shell.

4.14. Check for all logs

Windows NT, Windows 2000, Windows XP and 2003 systems have three common event logs - System, Application and Security logs. These are useful logs to help tracking intrusion activity on or against a particular system. User should review logs for unexpected events and investigate suspicious activity.

To access Event Viewer, Click **Start Menu** → **Programs** → **Administrative Tools** → **Event Viewer**

Log files for Linux/UNIX vary from flavour to flavour, but System and Accounting logs are stored in “/var/log” or “/var/adm”. Common log files include 'messages', “syslog”, and on some systems “suLog”. Also “wtmp”, “utmp”, and “lastlog” contain information on logins.

4.15. Check for existing network devices logs

Before attempting to penetrate a system, intruders tend to scan their target (network reconnaissance) for open ports and vulnerabilities. This often created signature or log on network devices such as Routers, Firewalls, etc which have logging enabled.

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
23:57:24	Firewall-1	accept		192.168.3.101	192.168.1.1	icmp	
23:57:25	Firewall-1	accept		192.168.3.101	192.168.1.2	icmp	
23:57:26	Firewall-1	accept		192.168.3.101	192.168.1.3	icmp	
23:57:36	Firewall-1	accept		192.168.3.101	192.168.1.4	icmp	
23:57:36	Firewall-1	accept		192.168.3.101	192.168.1.5	icmp	
23:57:37	Firewall-1	accept		192.168.3.101	192.168.1.6	icmp	
23:58:19	Firewall-1	accept		192.168.3.101	192.168.1.7	icmp	
23:58:19	Firewall-1	accept		192.168.3.101	192.168.1.8	icmp	
23:58:19	Firewall-1	accept		192.168.3.101	192.168.1.9	icmp	
23:58:21	Firewall-1	accept		192.168.3.101	192.168.1.10	icmp	
0:30:26	Firewall-1	accept		192.168.3.101	192.168.1.11	icmp	
0:30:28	Firewall-1	accept		192.168.3.101	192.168.1.12	icmp	
0:30:29	Firewall-1	accept		192.168.3.101	192.168.1.13	icmp	
0:30:39	Firewall-1	accept		192.168.3.101	192.168.1.14	icmp	
0:30:39	Firewall-1	accept		192.168.3.101	192.168.1.15	icmp	
0:30:40	Firewall-1	accept		192.168.3.101	192.168.1.16	icmp	
0:31:22	Firewall-1	accept		192.168.3.101	192.168.1.17	icmp	
0:31:22	Firewall-1	accept		192.168.3.101	192.168.1.18	icmp	
0:31:22	Firewall-1	accept		192.168.3.101	192.168.1.19	icmp	
0:31:24	Firewall-1	accept		192.168.3.101	192.168.1.20	icmp	

Figure 3: Example of Checkpoint Firewall-1 log.

From the example above, it can be seen that IP address (192.168.3.101) is probing network IP addresses (192.168.1.1 to 192.168.1.20) using ICMP protocol to scan for active host in the network. This is one of the most common techniques used by attacker. This technique is known as “Ping Sweep” and it can be done by using network scanning tools easily available on the Internet.

This clearly indicates that an intrusion attempt has occurred. If such an incident happens, the best practice is, to configure the firewall to block the source IP address (e.g. 192.168.3.101) to prevent future attacks from the same IP address, and monitor any other suspicious activity. And if possible, block any ICMP requests from all IP addresses unless required.

4.16. Check for server logs (Web, FTP servers)

By reviewing server logs such as web server logs will help identify intrusion attempt or a successful intrusion. Web server logs normally contain requests from clients or visitors as well as timestamp and IP addresses.

To view log file for Microsoft IIS (Web Server), go to `c:\WINNT\System32\LogFiles\W3SVC1\`

```
Log format: <date> <Time> <source IP> - <Dest IP> <Dest Port> <Action>

2001-06-18 06:34:49 10.1.7.112 - 192.168.1.103 80 GET
/scripts/../../../../winnt/system32/cmd.exe /c+dir 200 -
2001-06-18 06:34:49 10.1.7.112 - 192.168.1.103 80 GET
/scripts/../../../../winnt/system32/cmd.exe /c+dir+..\ 200 -
```

Figure 4: Example of Microsoft Internet Information Service Log.

From the log file example given above, it can be seen that on **2002-11-12** (Date) at 13:00:37 HRS (Time) **202.101.230.112** (Source IP address) is trying to execute the dir command (**/scripts/../../../../winnt/system32/cmd.exe /c+dir**) remotely on the Web Server **192.168.1.103** (Destination IP address).

This technique is known as Directory Traversal attack, used by intruders to run commands on Microsoft IIS Web Servers remotely. This could result in high severity if the IIS server is not updated and secured. The best action is to configure firewall (if available) to block intruder's IP address (example **10.1.7.112**) to prevent future attacks, and apply all vulnerability updates or patches on the Web Server Application and its Operating System.

4.17. Check invalid network configuration

Inspect for any invalid entry for network setting such as Gateway, DNS, WINS and IP forwarding.

In Windows, these could be done by typing "`ipconfig /all`" in **Command Prompt**.

For Linux, to check for any invalid network configuration type "`ifconfig`".

4.18. Check for viruses using the latest virus definition

It is recommended that Administrators or Users should install antivirus software on their system. Frequently scheduled for automatic scanning, to detect any suspicious files, folders or email attachments. Before scanning your system, remember to update the latest virus definitions.

Typical symptoms that a virus may be present in your system or computer:-

- Decrease performance of the computer
- Missing files or folders
- A sudden lack of disk space
- Unusual popup message

4.19. Check for unknown registry entries (Windows)

Windows families come with a built-in registry editor. This registry can be access by clicking **Start → Run → type regedit** and click **ok**.

In Windows, a typical backdoor normally resides in registry key as shown below :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

This key enables the backdoor server to run automatically when Windows starts. By inspecting the registry key above helps Administrators or Users to detect unknown services which can be a potential backdoor.

NOTE: It is recommended that Administrators or Users has technical knowledge on Windows registry and backup the system's registry before manipulating the registry keys.

4.20. Check for Scheduled task

Examine if there is any task schedule being set such as "crontab" or "at". Intruder created a backdoor in files run at "crontab" and "at". This technique will allow them to reenter into the system.

Windows is built with Task Scheduler, a graphical tool that Administrators or Users can use to run scripts or programs according to a schedule. To view the Scheduled Tasks applet, click **Start → Programs → Accessories → System Tools → Scheduled Tasks →** and Double-click the Scheduled Tasks icon.

Another command-line tool used to schedule tasks is "at" command. To view the current scheduled tasks, open Command Prompt → type `at`

In Linux/UNIX the command used to schedule a program to run automatically is called "crontab". Any entries made by the "crontab" command will be stored in "/var/spool/crontab/Username". For example if the scheduled cron is created by the "root" account, the entry will be stored in "/var/spool/crontab/root".

5. Recommended tools

5.1. Monitoring tools

Below are few examples of monitoring tools that can be used to inspect system resources, running applications, processes and services:

For Windows:

- **PsInfo** obtains information about a system.
- **PsServices** view and control services
- **PsList** shows information about process and threads
- **ProcessExplorer** Combines the functionality of Handle and List DLLs into a graphical interface.

The tools listed above can be obtain from <http://www.sysinternals.com>

5.2. Integrity Checksum

Tripwire software is an example of an integrity checking tool that check for any changes in data integrity.

The latest version of tripwire can be obtained from the following URL: <http://www.tripwire.org>

AIDE (Advance Intrusion Detection Environment) creates a database from the `config` files. The database consists of various attributes:

Permissions, time, files size, user, group, time and number link.

Further details can be obtain from the following URL: <http://sourceforge.net/projects/aide/>

MD5sum command utilities are available for both Linux or MS-DOS/Windows base, which generates and verifies message digests using the MD5 algorithm. This program can be useful for file comparison, and detection of corrupted file and tampering attempts.

For more information on this program visit the site at <http://www.fourmilab.ch/md5/>

5.3. Intrusion Detection System (IDS)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network.

Further information about IDS can be obtained from <http://www.itpss.com>

Snort is a freeware network intrusion detection system, capable of performing a real-time traffic analysis and packet logging on IP network. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and more.

The main distribution site for Snort is <http://www.snort.org>

5.4. Network Monitoring Tools

Smartline Active Ports is a network tool capable of listing active ports, services or application running, with details of source and destination IP addresses on the system.

This tool can be downloaded at <http://www.protect-me.com/freeware.html>

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows NT, 2000 and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that shipped with Windows.

This tool can be obtain from <http://www.sysinternals.com>

5.5. Rootkit checker

Chkrootkit is a UNIX/Linux based tool that checks system binaries for any rootkit modification. The tools provides:

- check for a network interface set in promiscuous mode.
- check the `lastlog` for deletions.
- Check the `wtmp` for deletions.

This tool can be downloaded from: <http://www.chkrootkit.org>

Carbonite is a tool equivalent to an `lsOf` and `ps` but at the kernel level used to detect kernel level rootkits. Carbonite "freezes" the status of every process in Linux's `task_struct`, which is the kernel structure that maintains information on every running process in Linux.

For further information visit <https://www.foundstone.com>.

5.6. Registry Monitoring Tool

Smartline Active Registry Monitor is a utility designed for analyzing the changes made to Windows Registry - by recording "registry snapshots" and keeping them in a browsable database.

This tool can be downloaded from <http://www.protect-me.com>

5.7. Web Server Log Analyzers

WebLog Expert is a powerful access log analyzer. It will give you information about your site's visitors : activity statistics, accessed files, paths through the site, information about referring pages, search engines, browsers, operating systems, and more. The program produces easy-to-read HTML reports that include both text information (tables) and charts. It supports Apache and Microsoft IIS Web servers.

This tool can be downloaded from <http://www.weblogexpert.com>

5.8. Firewall Log Analyzers

DShield provides a platform for users of firewalls to share intrusion information. DShield is a free and open service. If you use a firewall, please submit your logs to the DShield database. You may either download one of the ready-to-go client programs, write your own, or use the Web Interface to manually submit your firewall logs. Registration is encouraged, but is not required. Everybody is welcome to use the information in the DShield reports and database summaries to protect their network from intrusion attempts.

For more information visit <http://www.dshield.org>

FireLogXP is a simple program for people using the Internet Connection Firewall (ICF) in Windows XP. It will read the log file and show you who is trying to get into your computer, and from which ports.

For more information, visit <http://www.mjleaver.com/Software/software.htm>

6. Conclusion

As mentioned in the preceding topics, there is no such hardware or software tools that could guarantee to eliminate intrusions completely. These tools will only help reduce the chances of intrusion.

As computer technology becoming more advanced, intruders will also continuously looking for new techniques to find vulnerabilities in a computer systems, some are still not known by security professionals and practitioners.

Vulnerabilities are discovered almost everyday. Security is a continuous effort and it is not a one time job. With the growth of the Internet, more computers are connected globally, hence more potential computers are exposed to intruders.

It is also important for the security professionals and administrators to prepare and able to detect the variety of signs of intrusions apart from just relying on the use of security devices in their network and taking necessary steps for preventing the network and systems against them.

References

CERT Coordination Center

<http://www.cert.org>

Global Information Assurance Certification

<http://www.giac.org>

FoundStone Inc. ® Strategic Security

<https://www.foundstone.com>

Chkrootkit

<http://www.chkrootkit.org>

Computer Security Resource Center, National Institute of Standard and Technology (NIST)

<http://csrc.nist.gov>

Microsoft Technet. "Fast Path to Intrusion Detection and Event Logging". Microsoft.

<http://www.microsoft.com/technet/security/tips/deteclog.msp>

Robert Graham Homepage. Network Intrusion Detection.

<http://www.robertgraham.com/pubs/network-intrusion-detection.html>

Tripwire, Sourceforge.

<http://sourceforge.net/projects/tripwire/>

Fourmilab Homepage. MD5sum utility.

<http://www.fourmilab.ch/md5/>

SecuriTeam Homepage. Chkrootkit, a root kit detection tool.

<http://www.securiteam.com/tools/5VP011536O.html>