ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

SCAN DETECT: An Intrusion Detection and Prevention System

Harsha P. Chari
Computer Engineering Department
Shree Rayeshwar Institute of Engineering And Information Technology
Shiroda, Goa -India

Abstract: ***The Internet is practically entwined in our everyday lives. Reports of security benches are heard almost every day. Simple steps to keep intruders at bay can go a long way in protecting business, resources and even lives. Network security in the current scenario starts at a single system level and rolls to the internet.***

The purpose of ScanDetect is to monitor the incoming network traffic to your system and to find any malicious activities and reporting those activities to network administrator. Administrative configuration ranges from shutting down the computer to sending port scan packet capture and analysis report.

Keywords: IDS, intrusion, packet, NMAP, log file, network security.

I. INTRODUCTION

An **intrusion detection system** (**IDS**) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies.

An intrusion detection system on the network proves to be very effective in keeping attackers at bay. Common network entry points like gateways can be equipped with Scandetect to detect, thwart and warn about threats early in the attack stage so that mitigation strategies can be devised and implemented effectively. ScanDetect detects any port scanning attempts and takes actions based on Administrative configuration which range from shutting down the computer, disconnecting it from the network, sending port scan packet capture and analysis report to the administrator and playing an audio media to attract the attention of the administrator.

The proposed Intrusion Detection system will be running on the client system as shown in Fig 1.

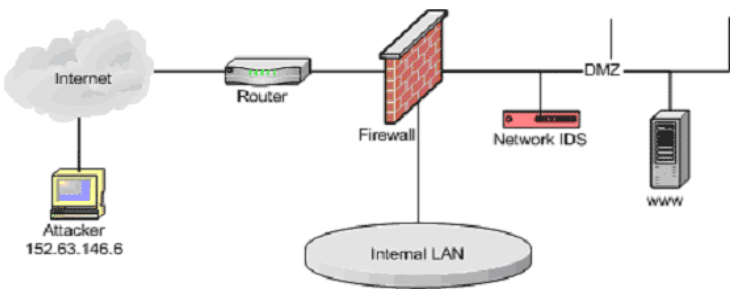

Fig.1 Intrusion detection system

II. System Architecture

The paper deals with the development of NIDS [9] .

ScanDetect is the Intrusion Detection Module that detects and prevents several types of port scans, including the SYN/Connect and Window scans of NMap.

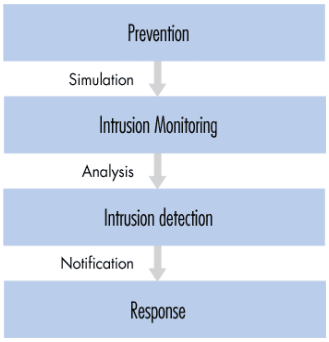

Fig. 2 flow of Intrusion detection

The ScanDetect Window provides system information and ways to configure its internal engine. When minimized or closed, ScanDetect collapses to the Notification Area and can be accessed again by a double-click on the icon or the right-click Show Window option.

ScanDetect

ScanDetect has to be configured before running it to detect scans.

ScanDetect - Configuration:

The System Information Pane provides additional information about the system like memory and Product ID etc.

The IP Behavior Configuration Pane allows configuration of IPs that are allowed or blocked by default.

The Total Denied Hosts gives the *count* of the number of IP Addresses that have been added to the *ip.deny* file. The ip.deny file contains a list of IP addresses that are not allowed to scan or communicate with your computer. ScanDetect reads the file at run-time and creates firewall rules for these specific IP addresses to block communication from and to those IPs. To manually add entries to this file or edit previous entries, click on the Edit infront of the count for Total Denied Hosts. In the text file that opens in notepad, add entries one below the other without anynewline at the end of the list.

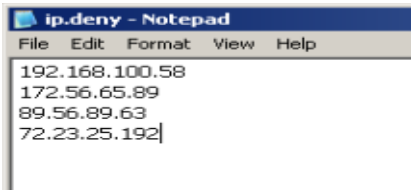

Fig 3. Sample ip.deny file.

The Network Information pane provides a drop down menu to select the network interface to monitor for port scans. The IP Address is displayed as the Network Interface is chosen from the drop down menu so that the user can chose what IP address to monitor, if recollecting the device name presents as a challenge.

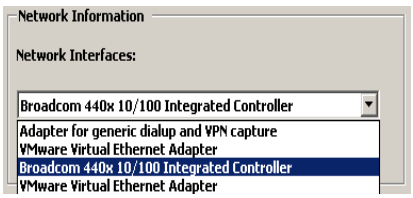

Fig 4.List of Network Interfaces on the System

Only a single instance of ScanDetect can be run, hence only a single interface can be monitored at any given time.

III. IMPLEMENTATION RESULTS AND TESTING

The following are the Snapshots of the System upon implementation

A. Application User Interface on start up

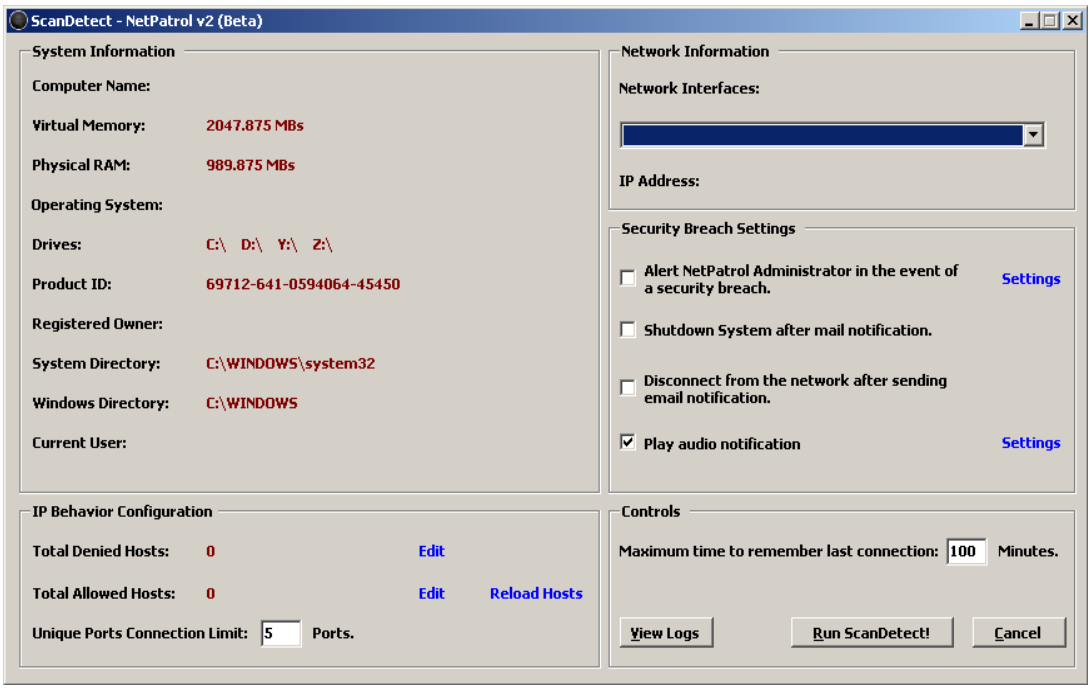

Fig 5 Snapshot of user interface of ScanDetect

Currently ScanDetect is capable of informing the Administrator by sending him a mail with the entire packet analysis of the Port Scan, Shutdown the computer after the mail notification has been sent, Disconnect from the network after the email notification and Play an Audio Notification. The email address and the smtp server settings can be configured by clicking on settings in front of the first checkbox. The audio file can be chosen by the Setting page for the audio notification. By default ScanDetect adds the IP address of the Port Scanning machine to it ip.deny list, thus effectively preventing any further communication from the remote machine. ScanDetect also displays Notification messages in the Notification Area informing about the Port Scan with the IP and about the IP being logged and the addition of the IP to the IP.deny file.

B. Scan Detect notification

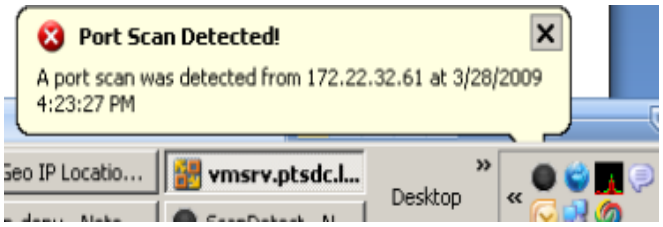

Fig 6. Port Scan Detected Notification Message

C. IP block notification

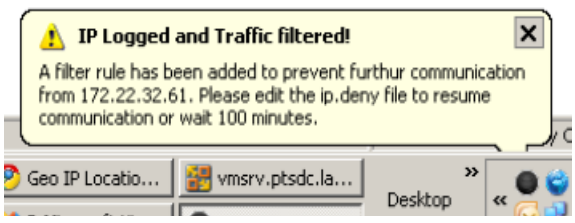

Fig 7 IP Blocked Notification Message

D. Administrator Notification

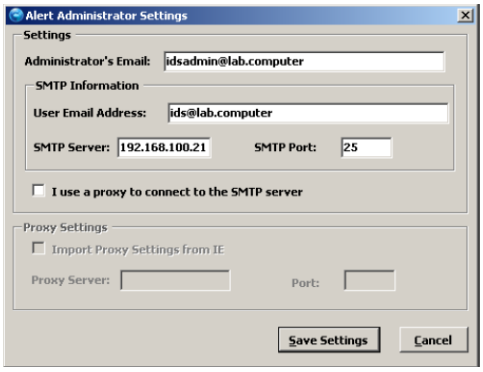

Fig 8. Alert Administrator Settings

E. Shutdown Notification

Fig 9. System Shutdown Notification

F. Log File

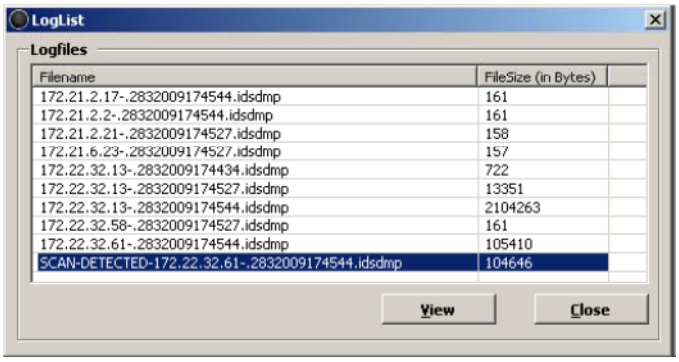

Fig 10 Snapshot of stored log file

The LogFiles created are of the form

<RemoteIP>-.DDMMYYYYHHMMSS.idsdmp

ScanDetect - Running:

ScanDetect uses multiple threads to analyze packets thus keeping the UI responsive. Running ScanDetect after proper configuration ensures the complete protection of your network. ScanDetect will log information about every packet that enters the network unless exclusively excluded via the ip.allow list.

ScanDetect - In the Event of an Attack:

In the event of ScanDetect detecting an attack, let the application block the IP first. As your network is now safe from the threat, you can use the IP address that ScanDetect provides you and then stop ScanDetect to analyze the logs. The logs are stored in a simple human readable format.

The following is an example of a log collected by ScanDetect:

10:23:43,760 Len=60 SYN 172.22.32.61:33605 ----> 172.22.32.60:554 window size 1024 src hdw addr: 00:0c:29:ec:d2:48 seq num1586966346 TCP TTL: 56

The fields from the log are explained below:

10:23:43,760	provides the time from the packet
Len=60	length of the packet in bytes
SYN	flag that was set on the packet
172.22.32.61:33605	Source IP address and the source port separated by a colon
172.22.32.60:554	destination IP address and port separated by a colon
window size 1024	window size of the packet
src hdw addr: 00:0c:29:ec:d2:48	source hardware address read from the packet
seq num1586966346	seq number of the packet
TTL: 56	TTL of the packet

Table 1. EXPLANATION Of LOG FIELDS

IV. CONCLUSION

ScanDetect has an IP blocking mechanism that will drop all packets from a malicious IP address thwarting any future attempts of system or network exploitation when a threat is detected. To resume communication to or from the remote computer, the IP address entry will have to be removed from IP.Deny file. ScanDetect is fully customized and have options to send an email detailing the nature of the probable attack with other relevant information or log all information to log files.

References

1. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
2. http://nms.lcs.mit.edu/papers/portscan-oakland04.pdf
3. http://www.cs.ucsd.edu/~clbailey/PortScans.pdf
4. http://www.codeproject.com/KB/IP/dotnetwinpcap.aspx
5. http://www.securityfocus.com/infocus/1580
6. http://www.openwall.com/scanlogd
7. http://en.wikipedia.org/wiki/Network_intrusion_detection_system
8. http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html
9. Mastering Network Security by Chris Brenton
10. Hack Notes-Mike Horton

AUTHOR(S) PROFILE

Harsha P. Chari is working as Assistant Professor in the department of Computer Engineering, Shree Rayeshwar Institute of Engineering and IT, Goa University, Goa. She did M.E. in Internet Technology from Padre Conceicao college of engineering, Verna, Goa University and B.E. in Computer Engineering from Shree Rayeshwar Institute of Engineering and IT, Goa University, Goa. India

