Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 3, March 2013, pg.52 – 56

RESEARCH ARTICLE

Federated Network Security Administration Framework

Bhadreshsinh G. Gohil[1], Rishi K. Pathak[2], Axaykumar A. Patel[3]

[1]PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University, Gujarat, India

bhadu.gohil@gmail.com

[2]Senior Technical Officer, C-DAC, Pune, India

riship@cdac.in

[3]PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University, Gujarat, India

axay.a.patel@gmail.com

Abstract— In today's world, Internet is now ubiquitous. Most of Applications are based on Internet. Web and Internet technologies are becoming critical to many enterprises, and their huge potential in facilitating communication, decision making, and better business processes makes security a major concern. The factor that most affects network security solutions is the change of computing model. Since a Web-based application typically spans multiple host machines, a solution must be user-centric instead of system-centric. System-centric solutions such as login and password become extremely cumbersome to manage in the Web model. To resolve these issues it is proposed to build a framework which will streamline the process and also delegate most of the activities to several of designated stakeholders from each group. The framework enable the users/groups to do most of the work related to public release of the Websites/web portals and other network based services on their own with the intervention from the systems administrators or network security experts coming in only towards the final steps. The framework will also support different roles. The framework requires extensive scripting in either bash or python on Linux platform to handle several of the backend tasks like implementing policy changes on the security device.

Key Terms: - Vulnerability scan, security framework, web hosting.

I. INTRODUCTION

In organization scanning is critical and important process. Vulnerability scanning can help to secure network or it can be used by bad guys to Identify weakness in your system to mount an attack against. A vulnerability scanner is a computer program designed to access computers, network, or application for weaknesses [1].

There are number of vulnerability scanner available today. Every vulnerability tool come with their own monitoring interface it is so idea to create solution which will use for distributed scanning, report generation, scheduling and implementing the policies in large organization. Management interface will used by user and the administrator. Single point of management interface [2] for users so it can easily view report and statistics, do scanning, implement policies, etc. And take action on the basis of statistics.

II. VULNERABILITY SCANNING TOOL

There are lots of tools available in market for vulnerability scanning.

A. NESSUS

In computer security, Nessus is a proprietary comprehensive vulnerability scanning program. It is free of charge for personal use in a non-enterprise environment. [3] Its goal is to detect potential vulnerabilities on the tested systems. According to surveys done by sectools.org, Nessus is the world's most popular vulnerability scanner, taking first place in the 2000, 2003, and 2006 security tools survey. Tenable estimates that it is used by over 75,000 organizations worldwide. Nessus allows scans for the following types of vulnerabilities: [4]

-Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.

-Mis-configuration (e.g. open mail relay, missing patches, etc.).

-Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.

-Denials of service against the TCP/IP stack by using mangled packets

-Preparation for PCI DSS audits

On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user.

B. Nikto

Nikto Web Scanner is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems [5]. It performs generic and server type specific checks. It also captures and prints any cookies received. The Nikto code itself is Open Source (GPL), however the data files used to drive it are not. [6]

C. NMAP

NMAP (Network Mapper) is a security Scanner. Remote OS detection is an important technique in the network system security and becomes more and more popular these days, because it has close connection with the vulnerability just for an open port [7]. TCP/IP stack fingerprinting in the remote OS scanning, presents how to simulate the fingerprints of OS which will react to OS detection uses NMAP. In the network system security, especially in the network attack or security assessment system, it is very important to collect and analysis information of network. Learning which OS is running on a remote system in the network can be very valuable, because every different hole must cling to different OS, and it is more purposively to discover the vulnerability and more exactly to assess the security of the system or more easily to attack it only after recognizing the kind of the remote OS. [8]

III. SECURITY MANAGEMENT PORTAL (SMP)

SMP introduce a central management for scanning and service provisioning of gateways, firewall, and router. It features is intuitive, web-based user interface. [9]Management interface incorporate different scan policies. This web interface integrates with other backend module. This is single point of interface so user can easily access different scanning tools in one roof. For example: Scanning, Reporting, Service provisioning (Gateways, Router, DNS, DHCP), Schedule scanning etc.

A. User

User can do hosting of server, scan server, scan hosted server, open port request. When user want to host server in public domain he has to provide new IP address and domain name which is require for DNS, Gateways, router and firewall service provisioning.[10] Before hosting server it has to scan for vulnerability and remove vulnerability until all fix. Sometimes user have to open ports on gateway, router or firewall as per there requirement.

B. Administrator

Administrator can do hosting a server, scan already hosted server, policies, and open port request etc. type of work. When user request for hosting of server, administrator check the scanning report if any vulnerability present, admin user to remove all vulnerability. Until all vulnerability removed system not hosted. [11] Admin takes final call of hosting system. Admin can scan already hosted machine. And he can do schedule scanning. Admin can add or remove policies which are applied to server. Mail is send to respective user whenever server

policies are changed. And whenever port request come it take appropriate action apply rules in gateways, router and firewall. Prohibited service scan may only be performed by administrator. Access to machine is prohibited during scanning period.

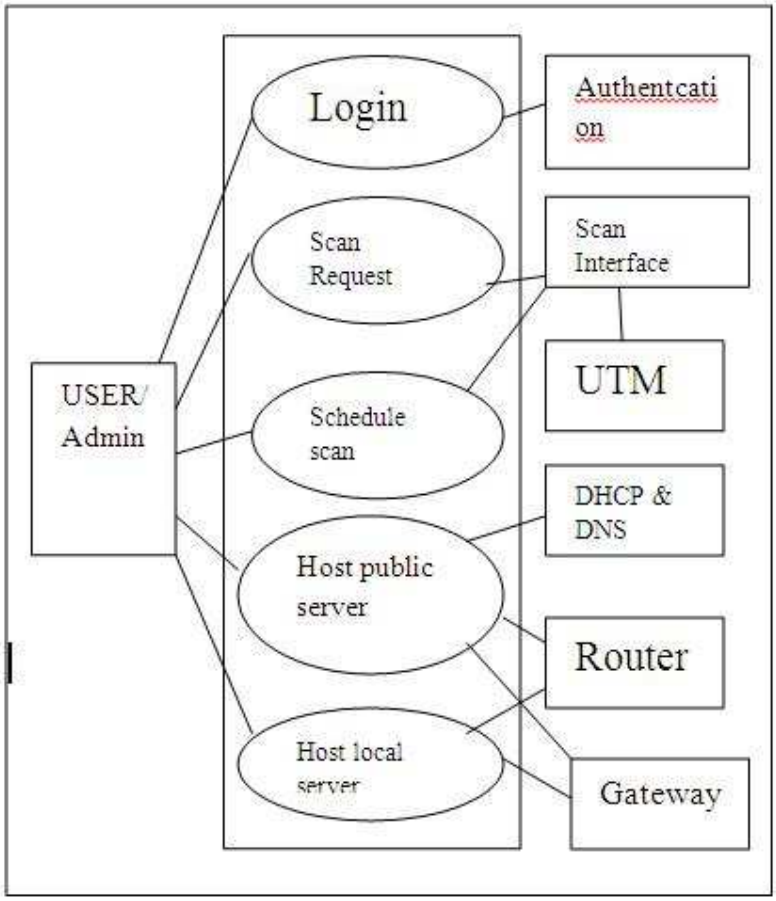

Figure 1 Security Framework

Figure 1 shows that user and administrator can log in to the framework and do scanning and hosting there server. They can do schedule scan. For hosting there server they can update DNS, DHCP or firewall or router as per there requirements.

IV. SURVEY FOR SECURITY FRAMEWORK

There is lots of security framework which can provide this type of interface to do vulnerability scanning and fix it to avoid attack from bad guys.

A. IBM Unified Threat Management (UTM)

Keeping network operations safe and efficient is more challenging than ever before, and network security has become one of the most critical issues facing today's internet. Because of the increased sophistication of security threats, standalone security threats, standalone security products are not affective. To build a good protection against complex and blend threats, multiple security features need to be integrated into UTM [12]. UTM refers to a security appliance as a combination of hardware, software, and networking technologies whose primary function is to perform multiple security functions.

According to IDC [13]The official definition of UTM is " Products that include multiple security features integrated into one box. To be included in this category, an appliance must be able to perform network firewalling, network intrusion detection and prevention, and gateway antivirus. Some of the key benefits of UTM is Cost effectiveness, easy to use, and application level gateway. The practical performance of a UTM

appliance is typically just the performance of the firewall with the other security applications disabled or providing minimal functionality.

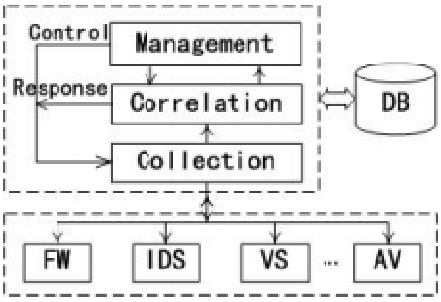

Figure 2 UTM

Figure shows one [14] UTM for a system. Some security devices are there like Firewalls(FWs), Intrusion Detection Systems(IDSs), Antivirus Software(AV), Vulnerability Scanners(VSs), etc. As you can see in figure there are four modules, the data collection module, the correlation and analysis module, the management module, and the database module.[15]

Protect your network from a wide variety of Internet threats with unified threat management (UTM) systems from IBM Internet Security Systems (ISS). These systems are designed to stop all types of Internet threats before they penetrate your network and impact your business. The UTM Service is separated into two main packages-Protection and Content-which correspond to the protection capabilities available from most UTM appliances. [16] The Protection package supports and manages intrusion prevention systems (IPS) and firewalls designed to block traditional attacks like worms, Trojans and intruders. The Content package provides management and support for Web filtering, anti-spam and anti-virus technology (where available). The Content package helps organizations filter unsolicited e-mail and objectionable Web content, and protects against phishing scams, spyware and viruses. [17]

B. OSSIM (Open Source Security Information Management)

OSSIM [18](Open Source Security Information Management) by AlienVault is an open source Security Information and Event Management (SIEM), comprising a collection of tools designed to aid network administrators in computer security, intrusion detection and prevention. Some components of OSSIM is

- Arpwatch (used for MAC address anomaly detection),
- P0f (used for passive OS detection and OS change analysis),
- Nessus (used for vulnerability assessment and for cross correlation (Intrusion detection system (IDS) vs Vulnerability Scanner)),
- Snort, used as an Intrusion detection system (IDS), and also used for cross correlation with Nessus.
- Ntop, which builds an impressive network information database for aberrant behavior anomaly detection.
- Nagios, used to monitor host and service availability information based on a host asset database.
- Snare, a log collector for windows systems. [19]
- OSSEC, a Host-based intrusion detection system (HIDS). Etc.

C. IBM App scan

This is one another tool for vulnerability scanning. It is a leading suite of automated Web application security and compliance assessment tools that scan for common application vulnerabilities, generate actionable reports, and help manage regulatory and standards compliance in online environments. These products are designed for the broadest range of users-from non-security professionals to advanced power users who can utilize the added tools and extensions to create a customized scanning environment. IBM Security AppScan automates vulnerability assessments and scans and tests for all common Web application vulnerabilities including SQL-injection, cross-site scripting, buffer overflow, and new flash/flex application and Web 2.0 exposure scans. [20]

IBM Security AppScan Standard is an industry-leading Web application security testing solution that includes: 1) Dynamic application security testing (DAST) to test for all common web application vulnerabilities, 2) Glass box testing for run-time analysis - a form of integrated application security testing (IAST), and 3) Static application security testing (SAST) [21] of JavaScript to identify client-side vulnerabilities.

V. CONCLUSION

By using this framework we can do distributed scanning and vulnerability assessment with single point of management interface. An advantage of this framework is distributed scanning, single point of interface, schedule scanning, fast hosting server, integration of multiple tools, easy communication between users and administrators.

REFERENCES

[1] O. S. Foundation, â œOpen source vulnerability database,â http://osvdb.org.
[2] P. Ammann, D. Wijesekera, S. Kaushik, a Scalable, Graph-Based Network Vulnerability Analysis,a Proceedings of the 9th ACM conference on Computer and communications security, 2002.
[3] http://sectools.org/
[4]http://en.wikipedia.org/wiki/Nessus_(software)#cite_ref-closed_3-1
[5]http://www.cirt.net/nikto/UPDATES/2.03/db_404_strings
[6] http://cirt.net/taxonomy/term/6
[7]David Barroso Berrueta, A practical approach for defeating Nmap OS Fingerprinting, http://voodoo.somoslopeor.com 2003.
[8] Fyodor. Nmap remote os detection via tcp/ip fingerprinting(2nd generation). http://insecure.org/nmap/osdetect, 2006.
[9] Postel, J. (Sep, 1981), RFC 793Transmission Control Protocol
[10] I. O. for Standardization. ISO 17799:2005 – Information Technology - Security Techniques - Code of Practice for information security management. ISO, 2005.
[11] Internet Security Systems â " Internet Scanner,
http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php
[12] http://www.itsecurity.com/
[13] http://www.idc.com/
[14] EDA, End-to-End Security Management in a Heterogeneous Environment, EDA 08-CAP-027, 2009.
[15] ArcSight_ESM.pdf, http://www.arcsight.com/
[16] E. Carter, et aI, "Intrusion Prevention Fundamentals: an introduction to network attack mitigation with IPS", Cisco press, 2006.
[17]http://www-935.ibm.com/services/in/en/it-services/unified-threat-management-utm-service.html
[18]http://www.alienvault.com/wiki/doku.php?id=documentation:agent
[19] http://en.wikipedia.org/wiki/OSSIM
[20]http://www-01.ibm.com/software/in/awdtools/appscan/
[21] http://public.dhe.ibm.com/common/ssi/ecm/en/rab14001usen/RAB14001USEN.PDF

