GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

How Safe is your Firewall?

© SANS Institute 2000 - 2002, Author retains full rights.

Name : Kam Chee Tat

Version : 1.0

Certification : GSEC

Course Attended : SANS at Kuala Lumpur

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This topic of this research paper is " How Safe is your firewall?"

This paper briefly describes concepts and do and don't about firewall deployment. The topic includes physical security, password management, and system security, log management and backup and recovery of the firewall that we deployed. There is also some brief description on concepts about design of firewall rules and the concerns that an administrator should take into consideration when administrating the firewall.

© SANS Institute 2000 - 2002 Author retains full rights.

HOW SAFE IS YOUR FIREWALL?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I am not an IS auditor by practice but I have noticed that there are many administrator or system engineer setting up firewall for their company or for their customer. Furthermore, with the current downsizing of the economy, there are many merger ands acquisition going around, many firewall administrator would have inherited some firewalls from their predecessors, they must be curious of what is the function of these firewall and who are they protecting and what are they protecting against.

There is also a huge debate in the industry on which type of firewall (Packet filtering, Stateful Inspection or Proxy firewall) is the best firewall that can provide the best security features and performance. Many big Multi-national Corporation have spent hundreds of thousands of dollars in investing a good firewall that can provide the best security features but all these will go to a waste if one of the firewall rules is misconfigured or if the firewall server is not properly secured. This paper aims to provide a general view of securing the firewall servers itself and some recommendations on how to build a secured firewall rulebase.

Securing Firewall Server

The methodology that we are using is to audit the firewall server itself and the firewall rules. Before we can start auditing the firewall rules, we would need to ensure that the firewall server is physically secured with controlled access.

Physical and Logical Security of Firewall

While we are putting a lot of emphasis on IT security or system security, there are many people who do not realise that physical security plays a very important role in IT security. I have personally come across some firewall administrator placing the firewall management console on his desk with the firewall management GUI operating (for convenience sake). By placing the firewall management console on his desk, at a place, which is accessible by many people, the console is susceptible to authorised access. If anyone can gain physical access and control the firewall console, there go the corporate security policies and all the corporate resources. Thus we would recommend that the physical to the various components such as the routers, firewall servers to be appropriately restricted to individuals who are authorised to access. It would be most appropriate that all these consoles and management tools be locked and secured in a network cabinet with control mechanisms over physical access such as biometrics, key and lock or access cards etc.

The password management features of the firewall are also an important aspect to consider during the implementation of the firewall. The construction of the password requirements of the operating system and the firewall system should be of at least 8 characters with a combination of upper case letters or lower case letters (A – Z or a –z); numbers (1-9) and special character (!#%^*>). There is also a need to ensure that the password is changed every 90 days and the password is not reused within a two-year period of time. The userid and password should also be encrypted across network and the automatic timeout features should also exist. The physical and logical access control

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

mechanisms should be in compliance to the Corporate Policies or Corporate IT Security Policies.

System Security of Firewall

Next we would need to ensure that the firewall operating system is fully secured. One way to reduce the system vulnerabilities is to minimise the number of softwares running on the server. The fewer the software components on the server, it would mean that the fewer security holes to detect and fill. Thus, by minimizing the number of operating system module installed on a server will not only improve the overall system security but also improve the performance of the firewall server as well. There are many standard checklists for systems security, which we can refer to in the Internet and some good secured operating system checklist, are as follows:

- Windows 2000
  - (http://nsa2.www.conxion.com/win2k/index.html)
- Windows NT
  - (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/tools.asp)
- Unix System
  - http://www.sans.org/newlook/resources/hard_solaris.htm
  - http://www.yassp.org/

The above checklist for securing systems provides a very detailed and step-by-step operation guidelines of securing the operating system. Due to the intensive "effort" needed for patching the operating system of the firewall, there is an upcoming trend of having appliances firewall. These firewall claims to have their own propriety operating system that claim to be "very secure". There is one thing which we can leverage on is that vulnerabilities of these operating system is yet to be discovered as such it is still very secured.

Next, we would also need to determine that the logical connections to the firewall are secured. We may be running Virtual Private Network (VPN) services or remote administration on the firewall and as such, we would need to determine that all communications to the firewall are secured (using ssh or MD5 etc) with encryption and enforced IP restriction on the remote machine to the firewall.

As we know that most software are bound to have some bugs and vulnerabilities and there may be vulnerabilities being discovered or enhancements by the software vendors, thus there is a need to ensure that the security patches of the operating system and firewall is of latest version and current. The firewall administrator should also solicit with Bugtraq, Ciac.org and other security bulletins and security news so as to be notified with the latest bugs and exploits and perform follow-up actions accordingly.

Secured Firewall Rulebase

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I think the question that we would ask is how to define a secured firewall rulebase for our firewall. A secured firewall rules plays a critical part of the firewall deployment and the keywords for a secured firewall rules in simplicity. As we know that the more rules we have, the more likely that there will be unnecessary services being open up and thus the chances of exposing the internal network to risk is higher.

We have personally came across some "heavy duty " firewall (inherited from some colleagues who have left the organisation) which serve a Class A network and there is more than 500 rules in the security policy but we did not dare to remove any of the rules as the risk is just too big to take. As such, the number of rules grows, the rule base becomes more complex and nobody would dare to do a cleanup of the firewall rules as we did not really know what is the impact after our cleanup and this may affect the actual production environment. After some impact analysis discussion with my colleagues, we decided to leave it as it is. Thus the morale of the story is that there is a need to evaluate the whole network and security architecture.

We do realise that there may be many different requirements by different groups of users and as such, we would recommend that additional firewalls to be set up to serve the different types of applications or services or even department so as to be able to keep the firewall rule to be as simple as possible. The segregation of the firewall can be caters for different business functions or for different types of traffic. This will not only assist to perform load distribution of the single firewall to different firewalls which will in turn enhance the performance of the firewall itself but also assist to reduce complexity of the firewall rules.

Implementation of Firewall Rules

The next thing that we should actually ask ourselves is what is the corporate security policies and how can the firewall comply with the policy. The firewall is no more than a technical implementation of the security policies. We would need to devise the firewall rules in compliance to the corporate security policies. We would need to identify the assets (routers, servers etc) that the firewall has been designed to protect and the objectives of the protection (Confidentiality, Integrity, Availability).

We would now need to convert the security policies to firewall rule for the organisation as such we would need to specify all the necessary services (such as http, ftp and smtp etc) that the internal LAN would require for their operational needs to the Internet. The source and destination of the network and objects need to be specific in order not to create any "broad" rule so as to control unnecessary access.

We can also create two DMZ zone in the network segment (Trusted and Non-Trusted). We can differentiate the Trusted and Non-Trusted zone by allowing traffic to directed to the internal LAN from the Trusted Zone only and not allowed any traffic to be directed to the internal LAN from the Non-Trusted Zone. As such, we can actually plan the network infrastructure and implement control mechanisms on the DMZ zone through the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Next we should also include a stealth rules and a lockdown rules as a standard template for the firewall rulebase. The stealth rule would block any communication from any machines to the firewall itself. This is to prevent attacks to the firewall and any traffic that need to establish communication with the firewall should be placed above the stealth rule. The lockdown rule should be placed as the last rule of the rule base and this rule would basically dropped all the traffic that is not explicitly specified on the firewall rulebase. We would recommend that the stealth rule and the lockdown rule to have long logs so as to be able to get as much information as possible for any attacks or attempts.

There are many firewall "administrator" who can implement firewall rules very efficiently but they do not really know or analyse the impact of the firewall rules to the overall security of the organisation. They would just process any request raised by the user and implement the rules accordingly without questioning the justification of the request. Thus as a firewall administrator or a security practitioner, we would recommend that they query on the justification of the request and perform impact analysis on the request before implementing the firewall rules and this would assist to minimise the organisation being exposed to risk.

There should also be change control mechanisms in place for the firewall rulebase administration. As we know that there are many administrators who implement firewall rules without putting comments, this has made future cleanup of the firewall rules very difficult. Thus we would recommend that for all request, the following information be updated on the comment field and they are:

- Name of person modifying the rule
- Name of requestor
- Date and time of rule change
- Reason for rule change

There is also some customised setting that the firewall administrator can consider in enhancing the security of the firewall server. We can actually review the connections table for time out limit and the number of connections. For Checkpoint FW-1, the default setting for the time-out limit is 3600 seconds and it is recommended to reduce it to 900 seconds, as this will decrease the "window of opportunity" for the hacker to fill up the connection table. As for the connection table, the default settings is 25,000 connections and it is recommended to change it to 50,000 so as to enable the firewall to process more connections and limit the chances of filling up the connection tables.

Tools for Firewall Security

The last step is to port scan the firewall to ensure no unauthorised ports is open on the firewall. This is to ensure that the firewall has no unnecessary services running on the firewall. There are also some commercial and free software available in the Internet to perform ping sweep and port scanning for firewalls and other systems. The tools will be able to perform certain hosts and network diagnostic scanning on the machine and the network and it is able to assist us to perform troubleshooting and scanning for the firewall

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

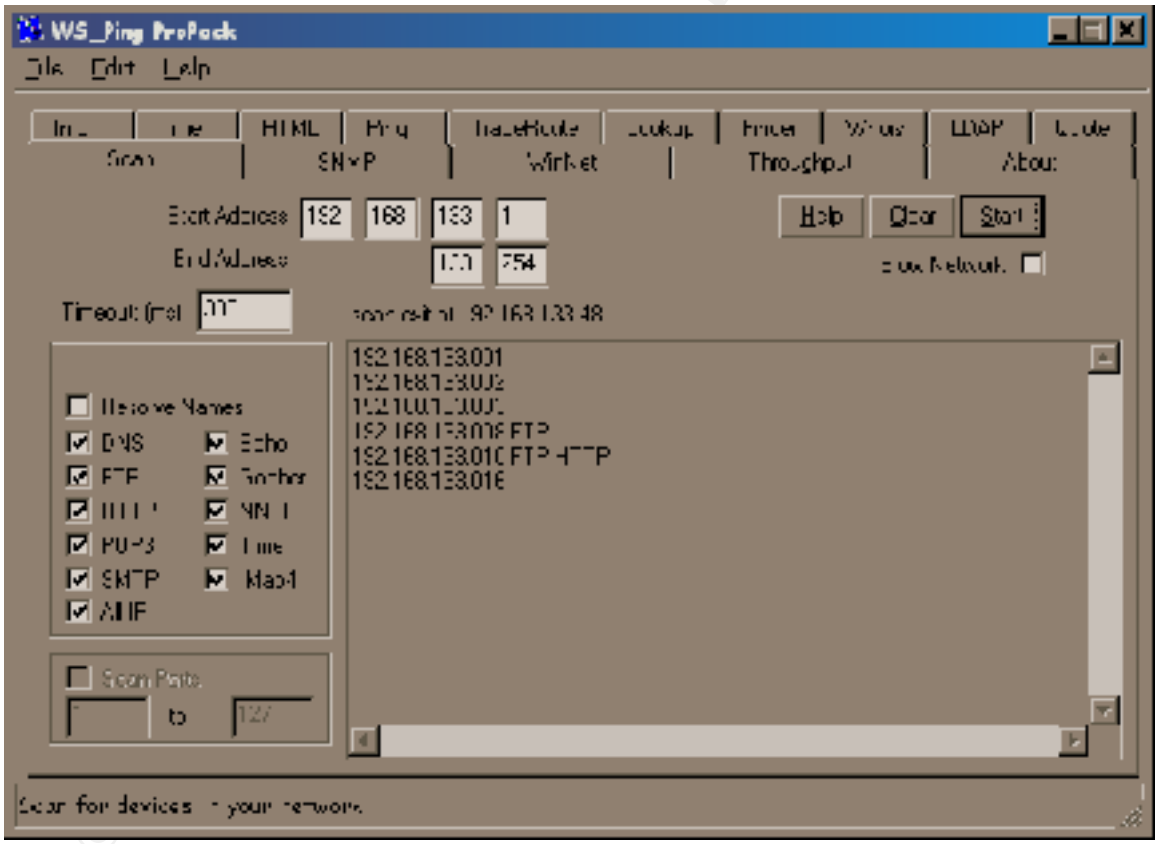
as well. There are two sets of tools that we would recommend and they are Nmap for Windows platform and WS Ping ProPack for Windows platform.

The software can be located at the following website:

- WS Ping ProPack

http://www.ipswitch.com/Products/WS_Ping/

The WS Ping ProPack is for Windows platform and it is able to provide a comprehensive set of tools to scan for the common services that is open on the machine. The tools also enable the user to perform network diagnostic and machine specific as well.



- Nmap

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.insecure.org/nmap/nmap_download.html

Nmap is also another host scanning tools, which we can use to determine the services and ports of a specific host. By using the tools, we can not only determine the security of the firewall server itself but also test the firewall rules to see whether the firewall picks up the stealth scan from the scanning hosts.

mozart #nmap -v -g53 -sS -sR -P0 -O -p1-65000 -o nmap.out victim6

Starting nmap V. 2.52 by fyodor@insecure.org (www.insecure.org/nmap/)
Initiating SYN half-open stealth scan against victim6 (172.16.1.106)
The SYN scan took 4086 seconds to scan 65000 ports.
Initiating RPC scan against victim6 (172.16.1.106)
The RPC scan took 2 seconds to scan 65000 ports.
For OSScan assuming that port 21 is open and port 22 is closed and neither are firewalled
Interesting ports on victim6 (172.16.1.106):
(The 64985 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
21/tcp	open	ftp
22/tcp	closed	ssh
23/tcp	closed	telnet
25/tcp	closed	smtp
53/tcp	closed	domain
79/tcp	closed	finger
80/tcp	open	http
109/tcp	closed	pop-2
110/tcp	closed	pop-3
111/tcp	closed	sunrpc
143/tcp	closed	imap2
443/tcp	open	https
512/tcp	closed	exec
513/tcp	closed	login
514/tcp	closed	shell

Extracted from http://www.auditnet.org/docs/firewall audit program.txt

Log Management

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After we have performed port scan and ping sweep on the firewall server, it is time that we verify from the firewall log to ensure all these attempts are being blocked and logged. Many of the administrators would leave the firewall as it is after deployment but did not take a proactive approach towards log management. They would only go through the logs only when things 'happens". We think that this approach is not correct as attempts would be left unnoticed and the administrator should take a proactive approach or outsource this portion to those Managed security services vendors to perform such tasks.

Recovery Plan

Lastly, we would like to discuss on the backup recovery plan, which I think is important for the firewall. In many organisations, the firewall is the gateway for the organisation to access the Internet or other partners. Thus this makes the firewall to be a critical servers as this the point of contact for the organisation to the rest of the world, as such, backup recovery plays a very important part in the maintenance of the firewall. Many organisation has noticed this and has purchased and set-up high availability firewall systems or load balancing systems. But ultimately, if the firewall servers crashed or due to unforeseen incidents that happened, do we have the latest firewall configuration on hand as we can continue our business as usual. Lastly, after we have also noticed that there are many administrator who perform backup very efficiently but they have never tested on performing recover of the firewall from tape, nor do they know that whether the backup will work. Thus it is also recommended that the administrator to perform recovery on a periodic basis so as to ensure that the backup is actually recoverable.

Summary

We have briefly discussed on the security aspect of the firewall in terms of physical security, password management and system security. There is also a few good practice and firewall configuration settings which can assist to enhance the security of the firewall which we have set-up. There are also a couple of tools, which we can use to scan the firewall, which we have set-up to provide us a better assurance that the firewall is secured. We have also briefly discussed on the backup recovery issue of the firewall server and how can we resume business if incidents do happen without affecting the whole organisation. But ultimately, the firewall is just a box; the most important factor of IT security is ultimately the " human factor". The firewall administrator should be trained on security concepts and procedure. There is a need to have Corporate IT Security procedure and all the users are being train to practise IT security at work and this is the most important factor to ensure that the organisation is safe from IT security breaches.

References:

1. Firewalls: What I Wish I'd Known When I Was Getting Started by William Davis
http://www.sans.org/infosecFAQ/start/fw_start.htm

2. Auditing Firewall Setup by Lance Spitzner
http://www.enteract.com/~lspitz/audit.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Building your Firewall Rules by Lance Spitzner
http://www.enteract.com/~lspitz/rules.html

4. Audit of Firewall Programs by Diane Rochette
http://www.auditnet.org/docs/firewall audit program.txt

5. Checkpoint Firewall Audit Work Program by Terry Cavender
http://www.auditnet.org/docs/CheckpointFirewall.txt

6.Solaris Operating Environment Minimization for Security :A Simple Reproducible and Secure Application Installation Methodology by Alex Noordergraaf and Keith Watson
http://www.sun.com/blueprint/1299/minimization.pdf

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.