International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 2: Feburary 2016, pp 1-5. www.aetsjournal.com ISSN (Online) : 2394-6237

Hardening Technique for Enhancing Security in Network

M Jenolin Rex, AVijayalakshmi, A S Subaira

Abstract— Computer Networks allows access to information and services in an organized as well as controlled manner. Security is needed to make your data immune to any kind of data breach or malicious virus attacks. Hardening is to make system hard to protect from unauthorized access and is an on-going process of providing security. As, LAN hardening is done to secure whole organization network from attacks. In this paper, model is proposed for LAN hardening to reduce security risk. LAN hardening is divided into three parts- client/server, hardware and topology hardening. By applying hardening techniques on all parts LAN is harden. In client hardening table is proposed to determine security steps of operating systems and server. In server hardening, concept of masking is introduced to protect user system and to create illusion for intruders. Hardware hardening is proposed using a Table to make whole network harder .hardening of topology can be done by choosing a best one. In this way hardening of LAN is performed.

Index Terms — Hardening, Honey pot, Masking, Security

I. INTRODUCTION

Internet is an electronic communication network that interconnects computer networks globally to serve users. Network security is key point to give user authorized accessto data on network. Without the security over network the data transmitted is cracked by unauthorized access. Network security identifies the threats and gives method to protect network from them.

Threats or attacks to network security can be viruses, Trojan horse program, denial-of-services attacks, access attacks, spoofing attacks and password based attacks etc. To make network secure from attacks or threats, security of network is essential. To protect network from attacks or unauthorized access is big challenge in today's world. By making network secure or hard; can prevent network from attacks by using various techniques or methods as encryption strategy, secure network infrastructure and applying anti-virus. Security ofnetworkis on-going process all methods together will makenetwork secure.

As, layers of OSI model require security at each step from bottom to up. In the same way, the need for LAN security has also become very essential to protect from unauthorized access in every small or big organization.

Attacks on LAN are very common by attackers to steal data or particular OS information.

II. LITERATURE REVIEW

OSI model open system interconnection model comprisesof seven layers that define network communication for implementing protocols in each layer [1]. Control is passed from one layer to next layer at both client and server side. In Table I security required at each layer is explained.

Topology of network architecture consist of links, nodesetc. LAN is example of network topology that can be physical or logical both [2]. Depending upon the need of user, network topology is selected so that LAN is secured from attacks.

LAN security issue Due to LAN insecurity, in April 2011 attack on Sony PlayStation network was made in which personal details of many accounts were stolen. At that time millions of customers were affected by this network attack. So security of network is very important everywhere whether it is organization network or home network.

III. HARDENING

Hardening is step by step process of securing system fromunauthorized access. It is on-going process and makes system secure and more reliable. Hardening means to remove all unnecessary process and disable unwanted services. Hardening is to hard whole system as operating system, network devices, services and programs. It also tightens the security of operating system [3].

Hardening is required to protect system from hackers.Hardening is important so that confidential data or information may not be stolen. Making more harden system sometimes make system more complex difficult to operate for normal user. As system hardening gets more tightens same system gets more complex. So system hardening should be done in such a way that to operate system is easy for normal user. In Table II hardening of different OS is determined.

By making system more harden, complexity to operate system increases and with system complexity cost also increases. So system should be hardened by keeping in mind the cost factor. System should be hardened according to user requirement. In different operating system settings are default user can make changes according to needs. It is up to user to which extent system should be hard [4].

IV. LAN HARDENING

LAN hardening is to harden or toughen the security. LANhardening can be done by choosing strong password. LAN hardening is required to reduce security risk and to

M Jenolin Rex, Department of Computer Science and Engineering, Mahendra College of Engineering, Salem.
AVijayalakshmi, Department of Computer Science and Engineering, Mahendra College of Engineering, Salem.
A. S Subaira , Department of Computer Science and Engineering, Mahendra College of Engineering, Salem.

prevent from unauthorized access or attacks. LAN hardening means to harden topology, client/server and hardware. With all these points included proper LAN hardening is completed [4].

Now, the main focus is on client hardening that is how to harden the client. For client security flowchart is discussed.

Flowchart Fig I contain 7 steps to provide client hardeningin proper manner [5].

1st step-*Install and update antivirus* First important step isto install good anti-virus software in system and anti-virus require updates regularly.

2nd step-*Focus on important computers that need protection*

Now, focus on computers that need more protection. Perform a test to know about the computers that need protection. As in organization, protect that system first which have confidential data. Focus on important systems to reduce risk.

3rd step-*Use NMAP to create a profile for computersidentified in above step* –The important system that requiredsecurity apply techniques on that systems. Use NMAP-network security scanner tool to identify that which system responds to attack how. With NMAP tool- it scans the version and operating system of any target host. And after getting response from all system protect that system which responds to attack well.

4th step-*Disable all unnecessary services running onidentified systems*- Now disable all unnecessary services onthe systems identified above. By disabling unnecessary services risk is eliminated from systems.

5th step-*Look after security monitor alerts*- security monitoralerts tell about the systems that required security when any unusual thing occur in system. When security alert is announced check the identified systems that were identified above.

6th step-*Write logs to central server through network*- Logsrecord when services accessed and at which time. By writing logs to central server it looks at all systems when any unusual thing occurs.

7th step-*Use Kerberos to remove user password*- Attackervery easily hack user id password from system by using different tools. Kerberos- a security service remove all user passwords from system and reduce risk.

To do LAN hardening all three parts are required to be hardened. With all parts harden equally can harden LAN in proper manner then only LAN is secured from any type of risk or attack. Topology, Client/Server and hardware all these parts need to be secured. Choose best and secure topology, make system secure by performing all steps required for hardening, also make hardware secure from risk. By securing all four parts LAN is secured [6].

The benefit of LAN hardening is to secure overall networkfrom attacks or unauthorized access. If LAN is hardened it is difficult for attacker to send threat or steal confidential data. By LAN hardening integrity, availability and confidentiality is maintained.

Client hardening means to harden or secure OS fromattacks and it reduces security risk. But hardening should not be so tight that it becomes difficult for user to operate system and server hardening is important to prevent from outside intruders. When user operates on network then secure server is required to protect system from unauthorized access.

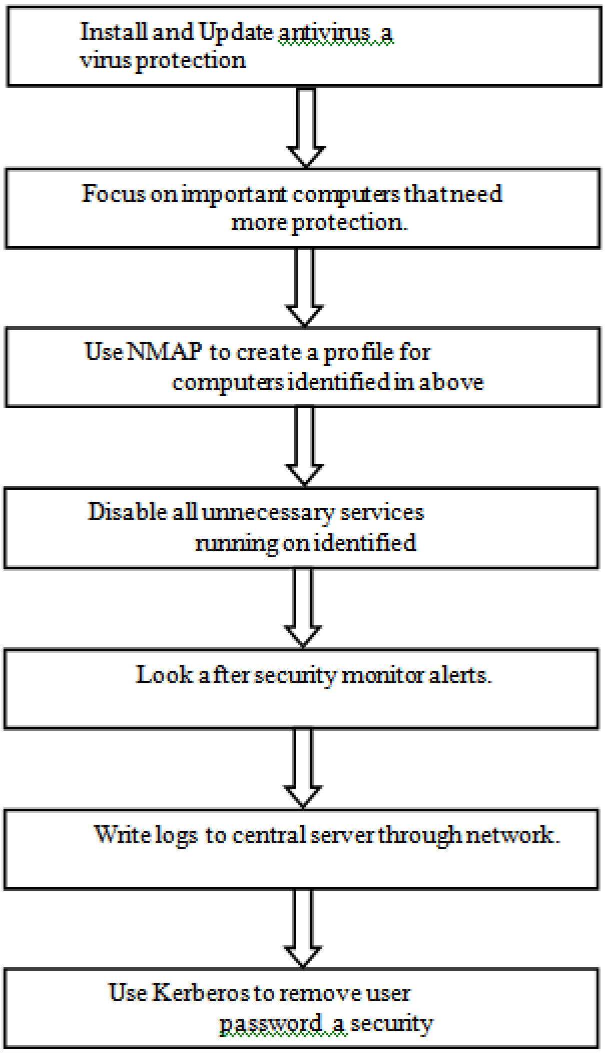

Install and Update antivirus a virus protection
Focus on important computers that need more protection.
Use NMAP to create a profile for computers identified in above
Disable all unnecessary services running on identified
Look after security monitor alerts.
Write logs to central server through network.
Use Kerberos to remove user password a security

Fig I- flowchart of Client Hardening

V. PROPOSED MODEL

In this paper model is proposed for LAN hardening based on overall security of topology, client, server and hardware. So it is required to hard each component individually to make LAN harden strong. *Proposed model isfocused on three components- topology, client/server and hardware hardening.*

Hardware hardening means to harden or secure thenetwork create illusion or to give wrong information to attacker about operating system. Masking provide irrelevant information about OS so that attacker send attacks to wrong operating system and in this case attacker will keep on trying different type of attacks but will not be able to get response from target machine. For example- operating system of target machine is windows 7 but with masking attacker will get wrong information about operating system as Linux and with this attacker will prepare Linux attack.

As in proposed model Fig II client/server, hardware and topology is hardened. In this way, LAN hardening is completed. First all hardware's- router, switch, hub and repeater are locked means they all are hardened with security. Secondly, clients are also hardened in same way. Thirdly, topology is also hardened as topology hardening is not performed but by choosing best and secure topology can create secure environment. By performing hardening of all three parts, LAN hardening is done. Not with only one part hardening can make LAN hard but it is contribution of all parts to be equally hardened to provide security over entire network.

Client hardening- Honeypot is like a trap used to detect anattempt of attacker on machine. Honeypot is used with virtual machine. Virtual machine look like same as original machine and attacker attack on machine connected on LAN but user create virtual machine to fool attacker, attacker attack on machine which is virtual in real. When attacker attack virtual machine then in honeypot all attacks made by attacker is collected. In honeypot log is created of attacks made on virtual machine and original machine is safe. From the logs created in honeypot user can protect machine by knowing which attacks were made by attacker on virtual machine [7].

By collecting all information security of client system is protected. Refer Fig III

Virtual machine is used as virtualization of originalmachine. Virtual machine is created for attackers to fool the so that they attack virtual machine by knowing it as original machine and their attacks are wasted. Virtual machine is used to create illusion to attackers and to protect original system of user. In this way client is made harden by using honeypot with virtual machine. Refer Fig IV.

Server hardening –As client and server hardening is sameand both protect system from attacks. Server hardening is done to protect system from intruders. Attackers use various network scanning tools to detect operating system of target machine. If operating system is known by attacker then according to OS detected attacker send attack to target machine to enter into system and if target machine respond to attack by mistake then attacker enters target machine and perform unusual activity. Here one new word is introduced masking- with this attacker will get wrong information about the operating system of target machine. Masking is used to Attacker attack LAN.

LAN connected with virtual machine

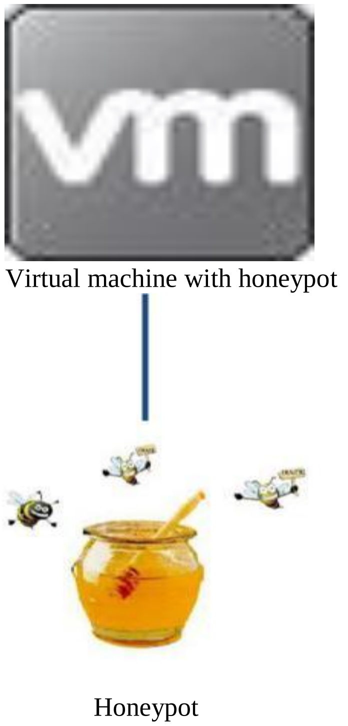


Fig III- client hardening using honeypot

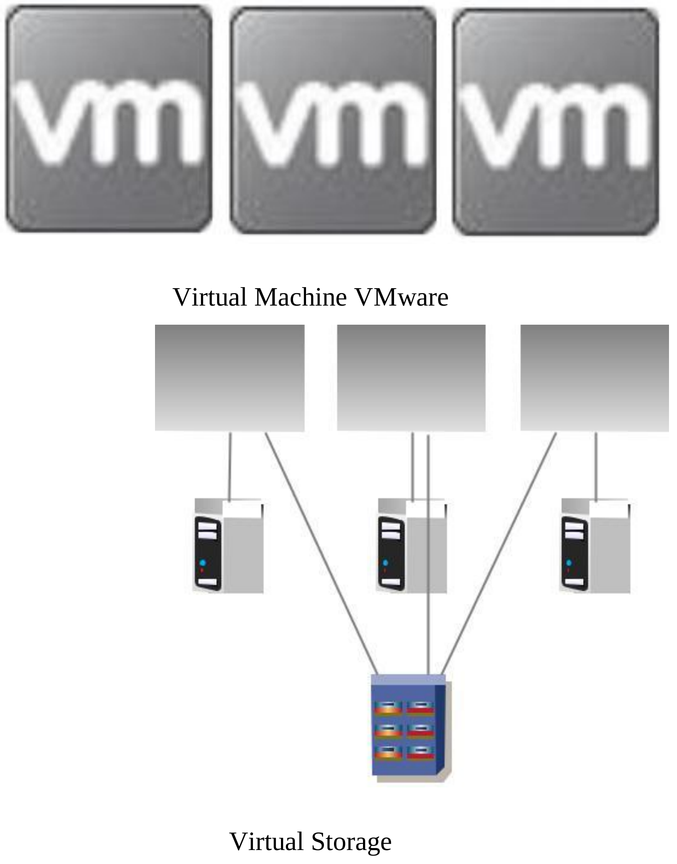


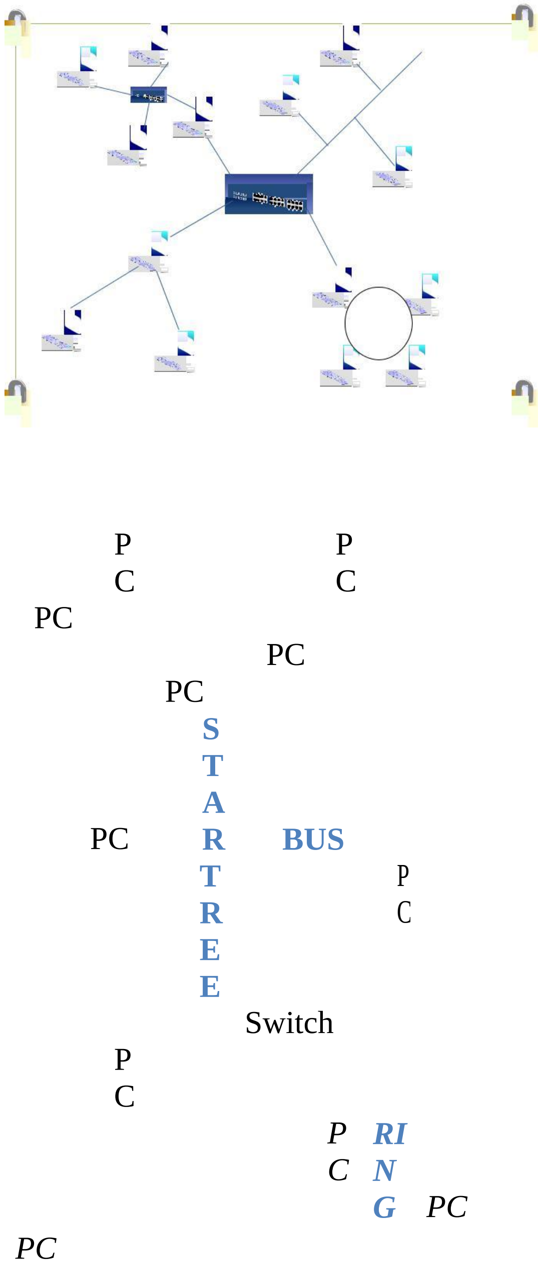
Fig IV- hardening with Virtual machine

Table III- Hardware Hardening

NETWORK HARDWARE	HARDENING TECHNIQUE
Bridge	Two measures to prevent from attack and by applying these changes security is obtained- layer 2 filter and static address entry. Filter bridge with IPsec (form of encryption.)
Hub	Two type of security- WPA- wireless protected access and WEP- wired equivalent policy.
Modem	In modem, security keys are used to protect user from attacker. As WEP security key- it is security code used on wireless network. Another technique is use strong password.
Repeater	Use security mode – WEP- wired equivalent policy.
Router	Keep strong password, disable HTTP configuration and IP source routing, and use anti-spoofing rules.
Switch	Switch security is maintained on two steps- what can see and connect means make changes accordingly that only some information can be seen by any user and to only some restricted area they can connect.

Hardware hardening means to make hard or securenetwork hardware as router, bridge, repeater, switch, hub and modem. By keeping all the hardening techniques of hardware in mind, hardening of hardware is maintained accordingly as in Table III.

Topology hardening- topology hardening is not done butby choosing secure topology for network can secure. Depending on the requirement of user or organization topology is choose so that secure network is maintained. The proposed model for topology is described in which star, bus, ring and tree topology is done and whole topology scenario is hardened to reduce risk.in this way choosing secure topology, topology hardening is done. Refer Fig V.



VI. IMPLEMENTATION

In implementation, tools as NMAP (windows and Linuxboth), XPROBE, WINFINGERPRINT are used. Attackersuse these tools to detect OS, version, ports open, ports filtered, ports closed, services and protocols. Attacker attack on target machine using ip address and should be on same network. These tools are used for attacks and prevention also.

Prevention as when user has to secure his machine or whole organization then user attack on each machine every time to know which information is leaked to attacker with the help of these tools and after getting information about attack area user hard the system or network to reduce security risk [8].

First tool window NMAP this tool is security scanner toolwhich create map of network when used and tell about the operating system of target machine, full operating system details, mac address, system name, ports, state, service, version, device type. All this information is collected by using this tool. In Fig VI screenshot of window Nmap tool is given.

Another tool of windows win finger print win finger print is security tool with strong scanning techniques tells about the computer name, MAC address, tracing route and RPC bindings. With this tool much other information can be gathered about target operating system by clicking on option provided. Also, in this ip range can also be defined to check different system collectively over same network. In FigVIIscreenshot of win fingerprint tool is given.

Next come with the implementation of Linux tools-Nmap and XPROBE2. Nmap tool in Linux is the samesecurity scanner tool but with different type of commands can detect various details of target system. In Fig VIII screenshot of Nmap tool in Linux is given. With command Nmap –sOip address of target system scans the ip protocol. This command tell about the protocols of target system over network their state and service. Xprobe2 tool works in Linux and is used for OS fingerprinting. With Xprobe2 identification of remote OS is done using packets. In Xprobe2 packet is send to target system.With Xprobe2 modules of target system are loaded using packets. In Fig IX screenshot of Xprobe2 tool is given [9].

VII. RESULT

With all tools Nmap, Xprobe2 and Win fingerprint attackers get exact information about operating system and ports open/closed of target system. After getting these information attackers plan to attack. If operating system of target system is Linux then, attacker will prepare attack or threats for that particular OS. This is the problem where security is reduced and risk on target system increases. To reduce this problem, hardening concept is used. If whole LAN is harden strong then there is very less chance to reduce security.

So concept of masking is introduced, masking is used to mask the original details and show fake details to intruder. If operating system of target system is windows but with masking it will show wrong information of operating system as Linux. And after getting this information attacker plans to attack wrong OS but never succeed as OS information is incorrect. Attacker keeps on trying with new attacks but every time fails as OS information is wrong. As in windows Nmap tool OS details are calculated wrong with false OS. In this way, with masking client/ server is secured and hardened. Also with concept of honeypot and virtual machine introduced above provide security from attackers and also inform about prevention methods.

In hardware hardening, table is introduced above how to make hard hardware devices. By using all that techniques hardware hardening is performed [10].

In topology hardening, there is no proper method to make topology hard but by choosing secure topology for network can provide security.

VIII. CONCLUSION

Hardening is process of securing system and reducing risk. To secure whole LAN hardening techniques is applied on all three parts- client/server, hardware and topology. So, in this paper model is proposed to secure whole LAN to prevent from attacks of attackers over network. By using various tools as Nmap, Probed attacks are identified and to prevent from attacks masking concept is proposed. Masking creates illusion for attackers. Hence, security of LAN is hardened is completed.

References

[1] M.Kayr , I.Kayri,"A proposed OSI based network troubles identification model" ,IJNGN, Vol.2,No.3,2010

[2] G.Bhatti, R.Singh and P.Singh,"A look back at issues in the layers of TCP/IP model", IJERMC,Vol.1,issue.2,2012

[3] White Paper, "securing (hardening) window server", Alpha Net solutions

[4] P.K.Patra, P.L.Pradhan, "Hardening of UNIX Operating system" , IJCCT, Vol.1,No.1,2009,P-72.79

[5] R.Bragg,"Hardening windows systems", McGraw-Hill/Osborne,2004

[6] J.Suess, M.Lukar and R.Petersen, "computer and network security in higher education ", Publication of EDUCAUSE,P-73.77

[7] Y.K.Jain, S. Singh, "HoneyPot based Secure network system", IJCSE,Vol.3, No. 2, Feb 2011.

[8] D.W.Richardson, S.D.Gribble and T.Kohno, "The limits of automatic OS fingerprint generation",AISec'10,2010,P-1.3

[9] W.H.Gilmore,S.R.Hogg, " Cisco Router/switch hardening", INS,2013,P-3.6

[10] D.Graesser,"cisco router hardening step by step", security Essential, Vol.1, 2001