Implementation of IEEE 802.1X Port-based Authentication Mechanism for Ethernet

ShaleenKachhara[#1], Dr. Kakelli Anil Kumar[*2]
[#] *SCOPE, Vellore Institute of Technology, Vellore, Tamil Nadu, India*
[*]*Associate Professor, SCOPE, Vellore Institute of Technology, Vellore, Tamil Nadu, India*

Abstract

We exploredsome mechanisms for securing corporate wired Ethernet, which are often more or less neglected. After a careful analysis of all possible solutions, we opted for IEEE 802.1X port based authentication mechanism. It uses radius server as an authentication server (on Windows Server 2012 r2) and Cisco switch as an authenticator. The main purpose of implementation of IEEE 802.1X is to restrict guest access to the LAN/wired network and authenticate only genuine users. Only the authenticated users have access to the network. The proposed mechanism monitors active users through centralized user access management using Microsoft Active Directory Servicesin Microsoft Server 2012 R2. The individual configurations of all the entities involved in the mechanism are discussed in detail to successfully deliver a pilot implementation of the protocol wherein one could debug all the errors and later deploy the same on a live network. By configuring the accounting tab on the Server Manager we will be able to keep track of all the users/employees activities on the organization's network.

Keywords – *Authentication, IEEE-802.1X, Radius server, switch, Network security.*

ABBREVIATIONS:

EAP- Extensible Authentication Protocol
PEAP– Protected Extensible Authentication Protocol
EAPoL- Extensible Authentication Protocol over LAN
VPN- Virtual Private Network
NAT- Network Address translation
IETF- Internet Engineering Task Force
RFC- Request for Comments
SSID- Service Set Identifier
DSL - Digital Subscriber Line
RADIUS- Remote Authentication Dial-In User Service

I. INTRODUCTION

In the world of information security, words like 'threat' or ‘vulnerability’ or ‘risk’mean anyone or anything that poses danger to the information,software or hardware or infact the users themselves. These threats or vulnerabilities or risks could be either from ‘insiders’ or from ‘outsiders’ who may not belong to the network [6]. In this era of technological advancement, more and more businesses are adopting newer technologies for multiple reasons ranging from better customer services to better working conditions for their own employees. Newer vulnerabilities are being discovered daily, and thereby making it more crucial for businesses to audit, map and understand their infrastructure in an increasingly secure and connected environment. Organizations need to be aware that cyber-criminal syndicates keep finding more sophisticated techniques to gain access on organization’s resources,mostly through their networks. Organizations today, need a meticulous view of their network infrastructurecovering hosts, VLANs, NAT,VPNs, routing protocols, network access rules, network components (current versions and updates), services running, and assets. Once this is done, security administratorscould use this network map to figure out existing vulnerabilities and device better security policies to counter them.

II. RELATED WORK

EAP [20] as described in RFC 3784 is mostly used between clients and switches. EAP operates over the data link layer such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP. EAP supports multiple authentication methods such as EAP-Md5, EAP-TLS, EAP-TTLS, PEAP and so on. The EAP packet has code, identifier, length, type and data, each of size 1 byte and variable [3, 8].

The EAPoLprotocol is a port-based authentication protocol used for IEEE 802.1X (Port Based Network Access Control). Transportation of EAP packets between the client and the authenticator is taken care by this protocol. Using EAPoL, an EAP authentication session can be started by either the client or the authenticator.The EAPoL frame format consists of MAC header, Ethernet type, version, packet type, packet body length, packet body, frame check sequence with length respectively 1, 2, 2, 1, 1, 2, variable, 4 bytes. EAP packets are also carried in the 802.11 by the EAPoL protocol as defined by Dot1x standard[8].

RADIUS [22] is a client/server protocol which operates between the authenticator server/RADIUS server and the switch. Radius protocol helps in identifying users/clients based on their login credentials. Only upon successful authentication, the users/clients can use the authorized resources. There are 3 key functions that uniquely define the Radius protocol, namely authentication, authorization, and accounting (AAA). RADIUS packet format includes code, identifier, length, authenticator and attribute, of sizes 1 byte, 1 byte, 2 bytes, 16 bytes, and variable respectively.

A. Network Access Control

From startups to multinational organizations, all have network access controls to define or guide how network access is granted to their employees. The same network has to reach different employees with multiple access permissions that are just sufficient enough for their day-to-day jobs. Now there are network access servers which help them in providing the necessary access authentication and authorization[6]. There are various automated tools available which help in realizing this strenuous job for network administrators. Technology giants like Cisco and IBM have developed solutions to counter the global problems of Network Access Controls.

B. Pilot Implementation

The approach should be to analyze possible vulnerabilities in organization's network and find a solution that could be implemented in their network infrastructure. So the very first task towards secured network environment is to get a clear understanding of all the network devices being deployed, their configuration and understanding the importance and contribution of every individual component in attaining a secure and feasible network access. It is required to first have a demo of working of any such security measure before implementing it on the live network as it runs the risk of affecting regular functioning of the organization's employees. One could modify and revise the mechanism in the test environment itself that suits thecompany's network infrastructure and policies well, before deploying iton to the main network.Once the pilot implementation is successful, the same could bedeployed on the company's network and monitored for proper functioning.

III. EXPLORING POSSIBLE SECURITY MEASURES FOR ETHERNET

Every organization has its unique network infrastructure with varied networking devices from varied vendors/companies, so there is no rock solid solution for network security. Some of these solutions are preliminary steps towards more secured environments while others ensure a great deal of security and auditing information of the users.

A. Physical Network Security

The physical security of network and its devices is also very crucialto protectagainst local threats and social engineering attacks. A nearby script-kiddie or even a grunted employee cancause harm to the proper functioning of the network if strong physical security of your premises and network devices is not warranted. It is very essential to guarantee that all the places where the network components are kept are physically securedfrom anyone without access rights using smart doors and cabinet locks wherever necessary. All the cables must be well protected by a plastic case and ensured that they are not in easy range of anyone to play with either out of curiosity or for malicious purposes. Ethernet ports which are not in present use must be disconnected to prevent unnecessary actions performed on them. But this would be just a preventive measure to limit the chances of attacks or breaches on your systems and nothing else.

B. Regularly UpdatedNetwork

The very first step is to have network auditing and mapping taken care of from time to time. Software or firmware updates for all network infrastructure components must be checked regularly. Default passwords and configurations must be changed at any cost prior to using any network component like a router or a switch, etc. Keep a tab on all the computers and devices connected to network. Make sure the antivirus is up and running properly and is timelyupdated, also more complex and secure passwords are used both by the admin consoles and the employees for better protection against brute force attacks.Hackers or cybercriminals will intend to exploit vulnerabilities in your operating system, software applications, web browsers, and browser plug-ins. Use updated software/hardware as most of the renowned software such as the Microsoft office suite, Adobe Acrobat and reader etc. regularly fix security loopholes in their framework and ensure a safe working environment to their customers.But it would be a mistake to consider yourself secured by merely updating your devices on a regular basis. It's just a preventive measure towards safeguarding your systems from attacks.

C. Implement MAC Address Filtering

Generally, in the case of a wired network, it's just plug and play for the network access which poses a major security issue for the wired networks. As compared to WEP, then WPA/WPA2 standards in wireless networks, the wired networks lack such well-defined security standards.MAC address filtering is basically allowing network access to devices whose MAC addresses are stored by the server. A table of

MAC addresses of all the devices in network perimeter is prepared and network access is granted only to those devices. Although it can be bypassed by a beginner level hacker by forging a legit MAC address, it could just serve as the first layer of security. It could help prevent an employee, a guest or an outsider to plug into the private network directly. The administrators will also have more control over devices on the network. But don't let it give you a false sense of security as MAC address could be very easily forged by any determined hacker, and also be prepared to regularly update the MAC address list every now and then if you opt for MAC address filtering.

D. Network Traffic Encryption

If security requirements are significantly high, consider encrypting your entire network traffic. Remember even with various security features in place, if your network traffic is not encrypted, it is very easy for an intermediate level hacker to just capture your traffic that might have user accounts, passwords, and other sensitive information.There are many proprietary network encryption solutions available nowadays, many of which operate at data link layerinstead of network layer, like IPsec to help reduce latency and overhead.But it runs the drawback of severe network lagging, hindering day to day functioning of all your employees. Encrypting data is only advisable in case of very sensitive data to share across and if you could afford a dime to ensure its security.

IV. PROPOSED IEEE-802.1X PORT BASED AUTHENTICATION

Authentication, encryption and other such security standards are often ignored on the wirednetworksdue to the complexity involved. While wireless networks are often encrypted and authenticated, but the wired networks should also be paid equal attention. Although deploying 802.1X won't secure the LAN network completely, it would at least restrict malicious peoples' access to network until they've authenticated themselves through their login credentials. To deploy 802.1X authentication, wefirst need a RADIUS server,commonly called as the Authentication Server, it is the component that authorizes/denies the network access to the users. On a Windows Server,RADIUS server is pre-installed withNetwork Policy Server (NPS) role,Standalone RADIUS servers can also be considered.The IEEE 802.1X standard defines a client-server authentication and access control protocol that restricts unauthorized users from connecting to a network. The authentication server authenticates each client that requests network access. [2].Authentication, Authorization, and Accounting (AAA) is ensured majorly by these three important roles:

Client: The user device (workstation) that requests access to the LAN network and switch. Often regarded as the 'supplicant'. Client workstation must be configured with802.1X-compliant client software. It is easily available in Windows operating systems.

Authentication server: The Radius server is the one which performs the actual authentication of the client. It validates the identity of the client through login information and notifies the switch whether or not the client is authorized to access the LAN and switchservices. [1]. The authentication data between the Radius-server and its clients is exchanged securely.

Switch: The switch is often termed as the authenticator and is basically a proxy between the RADIUS server(authenticator) and the client. On connecting to a switch port, it seeks login credentials from the client/user and then sends the data to the server for verification. After the server has successfully authenticated the particular client/user, network access is allowed on that port depending upon the access rights defined for that user by the admin.

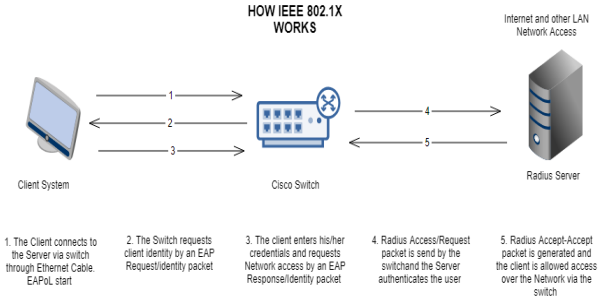

Fig. 1 Functioning of IEEE 802.1x protocol

A. IEEE 802.1X

The following Cisco flowchart describes the whole scenario of authentication via 802.1X [7] as shown in figure 2.

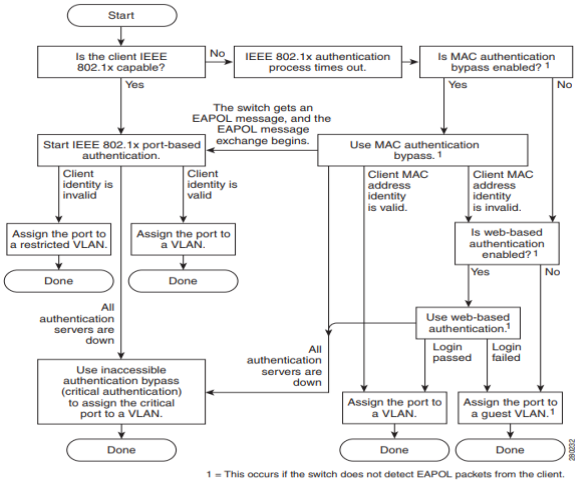

Fig. 2Flowchart of IEEE 802.1x protocol

B. RADIUS and its Application in 802.1X

The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on either a UNIX or a Windows NT machine.A Windows NT or a UNIX machine may usually support the RADIUS server while RADIUS client is typically a NAS [1, 2]. RADIUS servers receive network access request, authenticates the user, and allows network access or other resources that are meant for that user, as defined in the security policies by the Admin.RADIUS server and its clients share a secret key [15].Radius is the "backend server"(Authentication Server)in nearly all the 802.1X implementations. The client is referred to as "the supplicant" in EAP/802.1X terminology. Wired Ethernet switches typically implement EAP-PEAP (Microsoft, password-based authentication), EAP-TTLS (vendor-neutral, password-based and/or client-certificate-based) and EAP-TLS (client-certificate-based) protocols[4].For EAP/802.1X protocols, the NAS (a wired Ethernet switch) relays the EAP/802.1X messages between the wired client and the RADIUS server. [16, 18]. RADIUS server holds a database of users/clients containing their usernames and the passwords as stored by the network manager, and also the policies that define network access based on the employee that is seeking network access. There are numerous variations and customizations that could be achieved by the use of RADIUS SERVER and Dot1x implementation but discussing them all are out of scope in the current report but some of them are really useful that could be implemented with great ease.

C. IEEE802.1x with Guest VLAN

For cases when the authentications fails for some or the other reason or due to EAP request frame or the EAPoL packets getting lost in the way, a guest VLAN is configured to provide restricted network access to the users.

D. IEEE 802.1x with Inaccessible Authentication Bypass

For all the cases where the switch fails to connect with the RADIUS server, inaccessible authentication bypass feature is configured and the client is directed to a critical VLAN with restricted access rights [1].

E. IEEE 802.1x with MAC Authentication Bypass

For cases where the Dot1x enabled ports are connected to devices such as printers, IP telephones or some server etc, it is very important to deploy the MAC authentication bypass feature as these devices cannot authenticate themselves. The MAB feature would allow bypassing for these devices based on their MAC addresses that are stored in a separate table on the RADIUS server. Apart from the mentioned above, there are numerous other add-ons with the implementation of this protocol that could be incorporated with it depending upon the organization's requirements.

V.IMPLEMENTATION OF 802.1X AUTHENTICATION

A. Requirements for Testing

The following are required for testing 802.1x in a safe "off the grid" network.

1) Windows Server 2012 R2 -Authentication Server
2) Cisco Catalyst 2960x-48ts-ll Switch - Authenticator
3) Windows 10 Test PC – user
4) Connecting RJ-45 cables.

B. Configuring the Windows Sever by Sever Manager

The following steps are a detailed guide to successfully deploying the 802.1X port authentication (server side)

1) Open Control Panel > Change Adapter Settings > Right click on Ethernet > Properties >IP Version 4 (TCP/IPV4) > properties. Now, enter the IP address which is in the same groups as your cisco switch ie. 192.168.100.2, and subnet mask as 255.255.255.0 and the DNS server IP must also be the same as the IP.

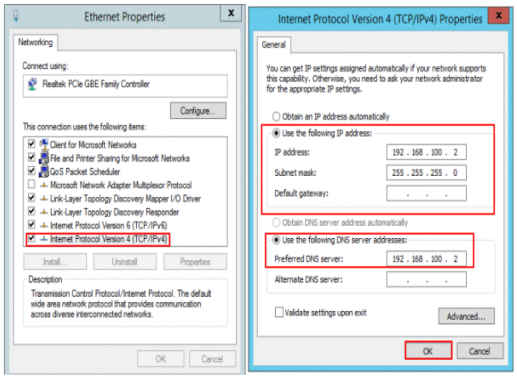

Fig.3 IP configuration of Windows server machine

2) Open Server Manager – Dashboard > Add roles and features > Install Active Directory Domain Services
3) Promote this Server to the Domain Controller and add the Domain name and other relevant details.
4) The Server System will reboot after this. Again open Server Manager > Add roles or feature> Add Active Directory Certificate Services.Similar Steps would be followed.This would serve as the Active Directory Certificate Authority that would help in authenticating the users as they attempt to connect to the network.
5) Now again, open Server Manager > Add roles or feature> Add Network Policy and Access Services (NAP)

Similar Steps would be followed.This is the place where all the policies, radius server and the radius client would be configured.
6) Once all these are installed, Open Server Manager > Tools > Active Directory Users and Computers > New Organizational Unit in the current container. Creating a new organizational unit named dot1x.Now add a group in this unit called the dot1xgroup. Within this group intended users will get the grant access of the network.

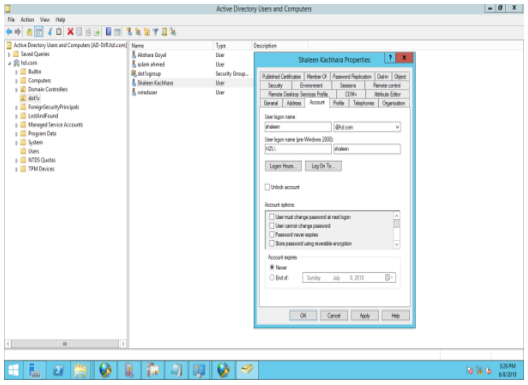

Fig.4Creating group of genuine users

Consider a user ShaleenKachhara with username: shaleen and password: hzl@123.
7) Right click on the NAP in Server manager and open Network Policy Server

Firstly, register this server in the Active Directory by right clicking NPS (Local). Now, in the Standard Configuration Dropdown, choose Radius Server for 802.1x Wireless or wired connections and then click on Configure 802.1X.To choose secured wired (Ethernet) connection add Cisco switch as a RADIUS client[9]. It is also specify the IP address of our Cisco switch and a secret key which uses during the configuring of Cisco switch.The IP address of the switch is: 192.168.100.15. The secret key is: secret. Now Choose Configuration Mode as Microsoft: Secured password(EAP-MSCHAP v2). Add user group as the group which made earlier called the dot1xgroup. Now Under Policies > Network Policies > Constraints > NAS Port Types > Tick mark Ethernet. Now Stop the NPS Service and then Start Again as shown in figure 5.

C. Configuring the Cisco Switch

Using PuTTY to take the switch on console, It could connect either through SSH or serial. SSH- enter the IP address of the switch in the host name and click open as shown in figure 6. Once the console is up, it can configure the switch using the following commands on the console. It shall implement the 820.1X authentication on PORT-GigabitEthernet0/45 as this port will connect to the TEST PC. [10, 13].

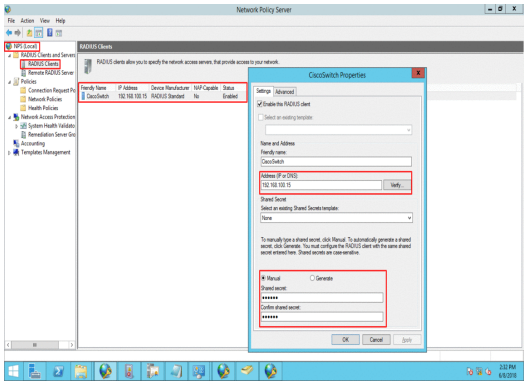

Fig. 5 Configuring Network Policy Server (NPS)

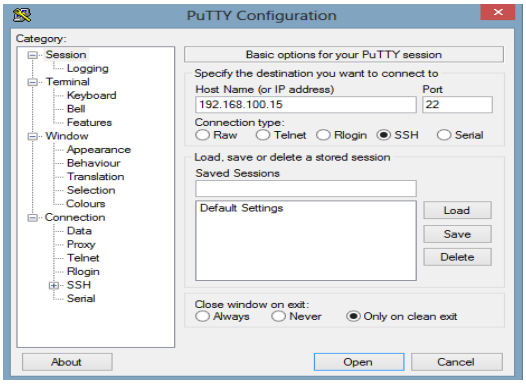

Fig. 6Access to switch console using PuTTy

Commands

MySwitch Enable
MySwitch# Configure Terminal
MySwitch(config-if)# aaa-new model
MySwitch(config-if)# aaa authentication dot1x default group radius
MySwitch(config-if)# dot1x system-auth-control
MySwitch(config-if)# radius server RADIUSSERVER
MySwitch(config-radius)# address ipv4 192.168.100.2 auth-port 1812 acct-port 1813
MySwitch(config-radius)# key secret
MySwitch(config-radius)# end
MySwitch(config)# interface GigabitEthernet0/45
MySwitch(config-if)# switchport mode access
MySwitch(config-if)# dot1x pae authenticator
MySwitch(config-if)# dot1x port-control auto
MySwitch(config-if)# end
MySwitch(config)#end
MySwitch#exit

Since it is a pilot implementation, we focus only on port 45 to deploy Dot1x.Thus the configuration is only for port 45. Because of regular updates in the Cisco ISO, some of the above mentioned commands may varyover time[10, 13]. Following is the text from the log file

generated by saving the running configuration of the switch:

```
MySwitch# show running-config
interface GigabitEthernet0/45
switchport mode access
 authentication host-mode multi-host
 authentication order dot1x mab
 authentication port-control auto
 dot1x pae authenticator
ip address 192.168.100.15  255.255.255.0
radius server hzl
 address ipv4 192.168.100.2 auth-port 1812 acct-port 1813
 key secret
```

D. Configuring the Client Computer

Add the test PC to the server domain i.e hzl.com and then sign in as the user to add in the Active Directory users and computers while configuring our Server. The user wish to authenticate by proposed 802.1X authentication protocol. As soon the user connects LAN cable to system, an authentication dialogue box would pop up and the user would have to enter the username password given to the user by the administrator that looks after the company's user accounts and authorizes the ones that the administrator wishes to grant access to the network.

1) Add the Test PC to the Server Domain, hzl.com in our case.

2)Add the system in the same IP pool as of the server ie. 192.168.100.5 and put the preferred DNS server IP address as the IP address of the Server i.e 192.168.100.2

3) Right Click on My PC > Manage> Services and Applications >Services >Auto Wired Configuration > choose Startup Type as Automatic and start the Service. Click on Apply and OK.

4)Open Control Panel > Network and Sharing Center > Change Adapter Settings > Right Click on Ethernet > Properties > ChooseAuthentication tab > Tick mark Enable IEEE 802.1X Authentication. Choose Network Authentication Method as - Microsoft: Protected EAP (Extensible Authentication Protocol)

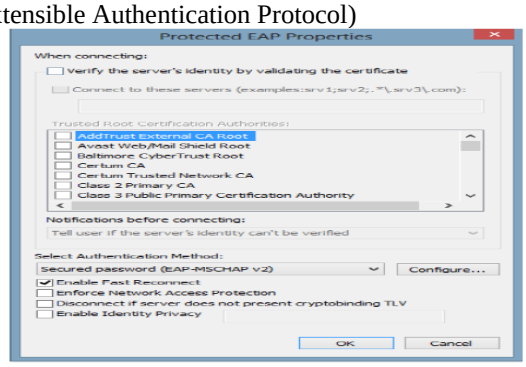

Fig. 7 Configuring EAP

Click on Configure – And uncheck Automatically use Windows Login Name and Password while connecting.Go to settings > Uncheck All Options. Select Authentications Method as Microsoft-Secured password(EAP-MSCHAP v2). Click Ok and open additional settings to specify the authentication mode. User authentication and click on OK for test setup.

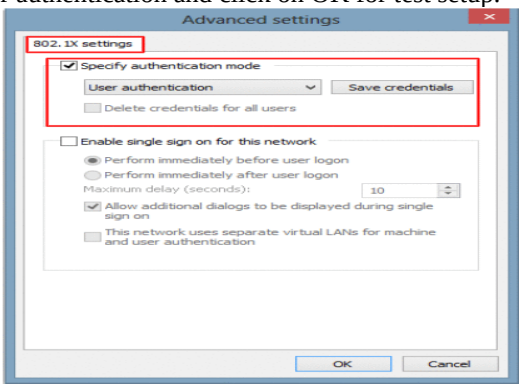

Fig. 8 Configuring advance settings of IEEE 802.1X

VI. RESULTS AND CONCLUSION

After the successful configuration of all the three i.e .the Supplicant (client), the Authenticator (Switch),and the Authentication Server (Windows Server), system is ready to test Lab Setup.

1)Open Change Adapter Settings in control panel. The status will be network cable unplugged.

2) Connect the LAN Cable now. The Status will now change to Attempting to Authenticate and a Authentication Dialogue Box will pop up.

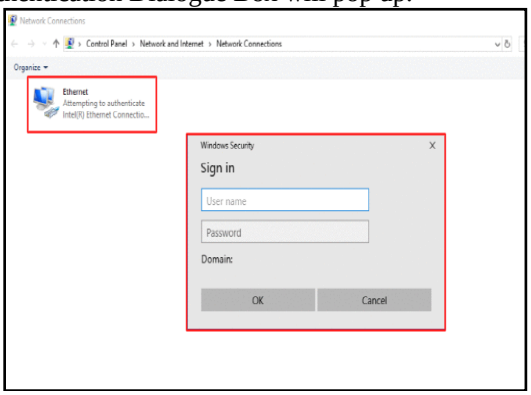

Fig9 Ethernet Connection status - Authenticating

3) Enter as follows and Hit Ok

Username: Domain name\username -- hzl/shaleen

Password: your password -- hzl@123

These are the credentials given to employees by the admin which could be later changed and managed depending upon the policies that the admin sets.

4) The status will finally change from identifying network to connect to an unidentified network which results the successfully authentication and joined the company's network. NPS server allows us to monitor the events on the Radius server. The admin can monitor from the server the login details of all the users(their IP address and other details) who attempt to login to the company's network through event viewer in windows server manager.

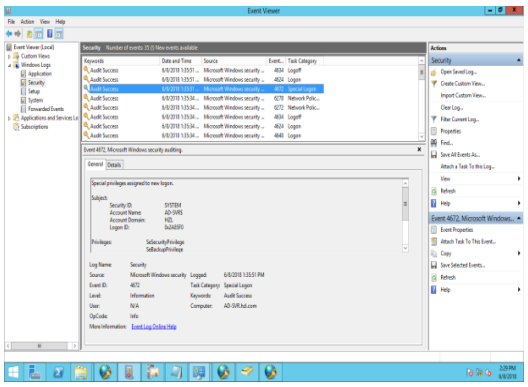

Fig. 10Event viewer- monitoring user activity

Also, an additional Log File is generated of every single attempt to login, which the admin can go through in case of any discrepancy in the company's network.

REFRENCES

[1] Cisco, "Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW - Understanding and Configuring VLANs [Cisco Catalyst 4500 Series Switches] - Cisco," February 15, 2018, 2018.

[2] J. Loos and R. Caudle, "Implementing IEEE 802.1x for Wired Networks," SANS Reading Room, 2014.

[3] G. López, O. Cánovas, A. F. Gómez, J. D. Jiménez, and R. Marín, "A network access control approach based on the AAA architecture and authorization attributes," Journal of Network and Computer Applications, 2007.

[4] C. Rigney, A. Rubens,W. Simpson and S.Willens. RFC 2865: Remote Authentication Dial In User Service (RADIUS).

[5] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in Proceedings ofI. Conf. on Dependable Systems and Networks, 2013.

[6] K. Y. Park, Y. S. Kim, and J. Kim, "Security enhanced IEEE 802.1x authentication method for WLAN mobile router," Advanced Communication Technology (ICACT), 2012 14th International Conference on, 2012.

[7] K. W. Kim, Y. H. Han, and S. G. Min, "An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks," Sensors (Switzerland), 2017.

[8] A. E. Maslov, S. L. Katuntsev, and A. A. Maliavko, "Study and implementation of authentication mechanism by RADIUS-server in switches and routers using NETCONF protocol," in International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices, EDM, 2017.

[9] Y. Y. Lu, Y. Yang, Z. H. Yin, and B. C. Yu, The research and design of campus network security development on Cisco AAA certification. 2013.

[10] Cisco, "OpenFlow," in Consolidated Platform Configuration Guide, Cisco IOS Release 15.2(5)E (Catalyst 2960-X Switches), 2017.

[11] D. Hannifin, N. J. Alpern, and J. Alpern, Microsoft Windows Server 2008 R2 Administrator's Reference. 2010.

[12] E. Vyncke and C. Paggen, LAN switch security: what hackers know about your switches. 2008.

[13] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," IEEE Network, 2015.

[14] C. Rigney, "RFC 2866 - RADIUS Accounting," Network Working Group, 2000.

[15] K. Y. Park, Y. S. Kim, and J. Kim, "Security enhanced IEEE 802.1x authentication method for WLAN mobile router," Advanced Communication Technology (ICACT), 2012 14th International Conference, 2012.

[16] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Rfc 3748," Extensible Authentication Protocol (EAP), 2004.

[17] J. C. Chen and Y. P. Wang, "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience," IEEE Communications Magazine, 2005.

[18] X. Huang, S. Wijesekera, and D. Sharma, "Secure communication in 802.11 networks with a novel protocol using quantum cryptography," in Proceedings 2010 4th International Conference on Network and System Security, NSS 2010, 2010.

[19] Md. Hashmathur Rehman, Dr.A. Govardhan T. Venkat Narayana Rao, "Design and Implementation of RADIUS, An Network Security Protocol", Global Journal of Computer Science and Technology,Page 48, vol. 10, issue 7, 2010.

[20] B. Shojaie, I. Saberi, and M. Salleh, "Enhancing EAP-TLS authentication protocol for IEEE 802.11i," Wireless Networks, 2017.