Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

Evaluation of the Security Mechanisms in the Notification Systems and Event Registration for Network Management

Ahmed Jaber Joudah

National University of Science and Technology
college of Pharmacy
Email :ahm12ahm1234t@gmail.com

Abstract

Network management systems provide facilities to alert critical conditions such as congestion, faults or intruder attacks. Syslog and SNMP protocols are usually used for this purpose, which nevertheless suffer from certain flaws as far as security is concerned. In this work, the notification and event log systems based on Syslog and SNMP are studied and evaluated in order to find possible security improvements that are relatively easy to implement. It describes the tests carried out with various protocols and technologies (PPTP, L2TP / IPSec, Kiwi Secure Tunnel and OpenVPN), which establish a secure channel ("tunnel") between the source and destination of the notification messages, creating thus what is known as VPN (Virtual Private Network). It also explains the use of virtual machines and virtual networks to carry out these tests. A virtual machine is essentially a way of having another computer running inside the real physical machine, simultaneously and independently. With virtual networks created with virtual machines, tunneling protocols and technologies can be tested, without requiring additional hardware resources.Among the different tunnel technologies studied and tested, the one that represents the best alternative to improve message security Notification and event logs is the Point-to-Point Tunnel Protocol (PPTP), due to its ease of use and transparency to the transported protocols. For future work it is recommended to test and evaluate the new version 3 of SNMP, which incorporates strong security mechanisms, although SNMPv3 agents are not yet readily available. It is also recommended to test and evaluate the different secure Syslog proposals, such as SDSC Secure Syslog, syslog-ng and msyslog, among others, which offer the possibility of using the TCP protocol for the transmission of messages, advanced filtering functions and the recording of messages directly in a SQL-like database.

Keywords: Security, Protocols, virtual networks, Syslog proposals

Introduction

The proliferation of the Internet as well as the growth of corporate networks have created a growing need to notify and record routine or extraordinary events that occur every day, so that technical staff and users themselves have access to information regarding conditions. of connectivity, errors, failures, alarms, access attempts, security breach and any other relevant information about the network and the equipment.[1]

Operating systems, applications, and the processes running on computer systems can send notifications about their own status and to indicate that certain events have occurred. These notification messages are of different categories and priorities in order to more quickly

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

distinguish severe problems from warnings that do not require urgent attention. The messages are usually sent to a centralized system where they appear on the operator's console and are also kept in a log for a certain period of time.[2]

Almost all activities carried out on a computer (such as a router or firewall) or in the operating system (such as Windows or Unix) are likely to be, to a greater or lesser extent, monitored and registered: from the hours of access of each user to the system to the most frequently visited web pages, including failed connection attempts, executed programs or even the CPU time that each user consumes. Obviously this facility to collect information has many advantages[3]. For example, it is possible to detect an attack attempt only when it occurs, as well as to detect improper use of resources or suspicious activities.

However, there are also disadvantages, as the large amount of information that is generated can create confusion and make it more difficult to detect problems. It can also cause a lot of traffic and create very large log files, all of which can be exploited for denial of service attacks.

Among the number of notification and event log systems that exist, Syslog is one of the most widely used. It is described in RFC3164 and was originally designed by the University of California for its BSD Unix system, but its versatility has made it a ubiquitous component in most modern versions of UNIX and in all kinds of equipment and systems where communications are based on TCP / IP. Despite the years that have elapsed since Syslog appeared, it has evolved relatively little because it has always been an extremely flexible service.

In very simple terms, the Syslog protocol provides a means of transport to allow a machine to send event notification messages over IP networks. These messages are sent to Syslog servers. The machine sending the notification can be a workstation, a web server, or a network device such as a switch, router, or firewall. The important thing is that said machine or equipment has the ability to send messages in the Syslog format.

The messages themselves can contain any kind of information that the machine is configured to generate and send. For example, it is common for a router to send a Syslog message when one or more of its interfaces change state (from up to down or vice versa). A router could also be configured to generate syslog messages when the access control list (ACL) is violated. It is important to note that the device sending the Syslog message must be able to establish network connectivity with the Syslog server and that the Syslog server must understand the format of the Syslog messages. Delivery of the Syslog message between the sending device and the Syslog server is not guaranteed, as Syslog is a "best effort" protocol.[4]

The architecture of a Syslog system consists of machines that generate the messages (called "devices" or "senders") and machines that receive the messages (called "collectors" or more commonly "Syslog servers"). A syslog system can also include machines (called "relays") that receive messages from one device and transmit other machines to them. Some devices can send syslog messages to multiple collectors and relays can also filter messages (for example, forwarding only urgent messages).Syslog messages are generally carried over UDP (User Datagram Protocol), although some devices and collectors may use TCP for reliability, since UDP is only a "best effort" service. The destination port assigned to Syslog is 514. When using TCP, the destination port is usually 1468.[5]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

In addition to Syslog, there is another mechanism that is commonly used to report events and it is through SNMP (Simple Network Management Protocol) traps. This is a protocol from the TCP / IP suite designed to facilitate the management of network devices, such as servers, workstations, routers, and switches. The SNMP architecture is shown in the following figure and includes 3 basic components. *Viz.*, MIB (Management Information Base), Agent & Manager. A trap is a special message generated by an agent to notify the manager of the occurrence of some significant event. The message includes the identification of the agent that generated the trap, when it was generated and what type of event it is.

SNMP has several security problems. For example, there is no way to ensure that the SNMP messages received by an agent actually come from the management station and not from another station that has spoofed its IP address. For this reason in principle it is possible to alter the MIB variables of a machine from any station through a SetRequest message, finding out the name of the community. On the other hand, SNMP does not define the mechanism by which a trap must be sent or explain what information the agent must send as part of the trap; it is only specified that it should include "interesting information". That is why the traps are specific to each implantation. Furthermore, they are only reported in pre-programmed events: when a different fault occurs, if the trap reports it, it will do so incorrectly[6]. The current research work with aimed to evaluation of the security mechanisms in the systems of notification and registry of events for the management of networks.

2.0 Methodology

To carry out this work, a methodology based on techniques, instruments and procedures typical of scientific research was used, since it is basically a research project and in this sense it is distinguished from the methodology based on feasible projects, typical of the engineering.

Differencesbetween "researchproject" and "feasibleproject"[7]

Researchproject	Feasibleproject
Raises a knowledgeproblem (somethingthatisunknown).	**It poses a problem of a practicalnature, generallydeterminedby a need.**
1. Researchobjectives are set, whichreflectstheaspects to be known..	1. Actionobjectives are drawn: tasks, activities, processes.
2. Itrequires a theoreticalframeworkthatsupportstherese arch to be carriedout.	2. Itdoesnotnecessarilyrequire a theoreticalstance. It places a lot of emphasisontheprojectjustification.
3. You can formulatehypotheses.	3. Formulateactionproposals and / oroperatingmodels as alternativesolutions.
4. Themethodology uses techniques, instruments and procedurestypical of scientificresearch.	4. Themethodologyvariesaccording to thephase and nature of theproject.
5. Thebasicelementsthat are included in a researchproject are: ➢ Statement of theproblem ➢ Objectives ➢ Justification ➢ Theoretical Framework	5. Thebasicelementsthat are included in a feasibleproject are: ➢ Objectives ➢ Justification ➢ Diagnosis of needs ➢ Formulation of

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

➢ Methodology ➢ In a project of thistypeitisinvestigated.	themodelorproposal ➢ Analysis of itsfeasibility ➢ In a project of thistypeitisplanned.

3.0 Results and Discussion

This chapter describes the experiences that were carried out to test the different solutions in order to establish a secure channel for the notification of events generated by Syslog and SNMP Traps.

3.1 Kiwi Secure Tunnel[8]: It began by experimenting with the Kiwi Secure Tunnel, as it is a product specifically designed for the secure sending of Syslog messages between 2 machines. The following figure 3.1 illustrates the arrangement using a real machine (host) and a virtual machine (guest), both connected to the Internet.

First, the client module was installed at one end of the tunnel. Then it was configured based on the following steps:

- Enter the IP address of the Kiwi Tunnel Server to which you are going to connect (200.84.32.129).
- Enter the login and password (they must be the same as in the Kiwi Tunnel Server).
- Set the server port (usually 22, the same as SSH).
- Select the encryption method.
- Enable or not data compression.
- Add an incoming port, usually 514, which is the default for Syslog.
- After those steps, the service was installed and activated.
- The installation and configuration of the server module at the other end of the tunnel is similar to that of the client.
- The Bind to: option allows incoming messages to be accepted only from the specified interface (in case the machine has several network interfaces). If left blank (the usual), accept messages from any interface.
- The Bind to Address: option allows outgoing messages to be sent only through the specified interface.
- If instead of the local host an IP address is entered, at the tunnel exit the decrypted message is forwarded to that IP address. This is useful if the Syslog server resides on a different machine than the Kiwi Tunnel Server.
- Furthermore, a Login and Password must be created for each incoming client connection.
- After completing these steps, the service was installed and activated.
- Finally, the tunnel between both machines was automatically established, which could be verified in the status window, as well as in the log.
- On the client side, it was also possible to verify that the tunnel is indeed established.

Traffic capture

- To verify that the Syslog messages were indeed encrypted, the Ethereal traffic analyser was used, which, in addition to being open source, has the advantage over

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

Iris that it also decodes the traffic on the virtual interface and Syslog test messages were generated. .

- As can be seen in the following figure, the traffic appears as an SSH protocol, since it uses port 22, which is the default port for that protocol. Also everything is encrypted.
- On the other hand, if you do not use the tunnel and the syslog messages are sent directly to the server (200.84.32.129) instead of to the tunnel entrance (127.0.0.1), the traffic obviously does not travel encrypted.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

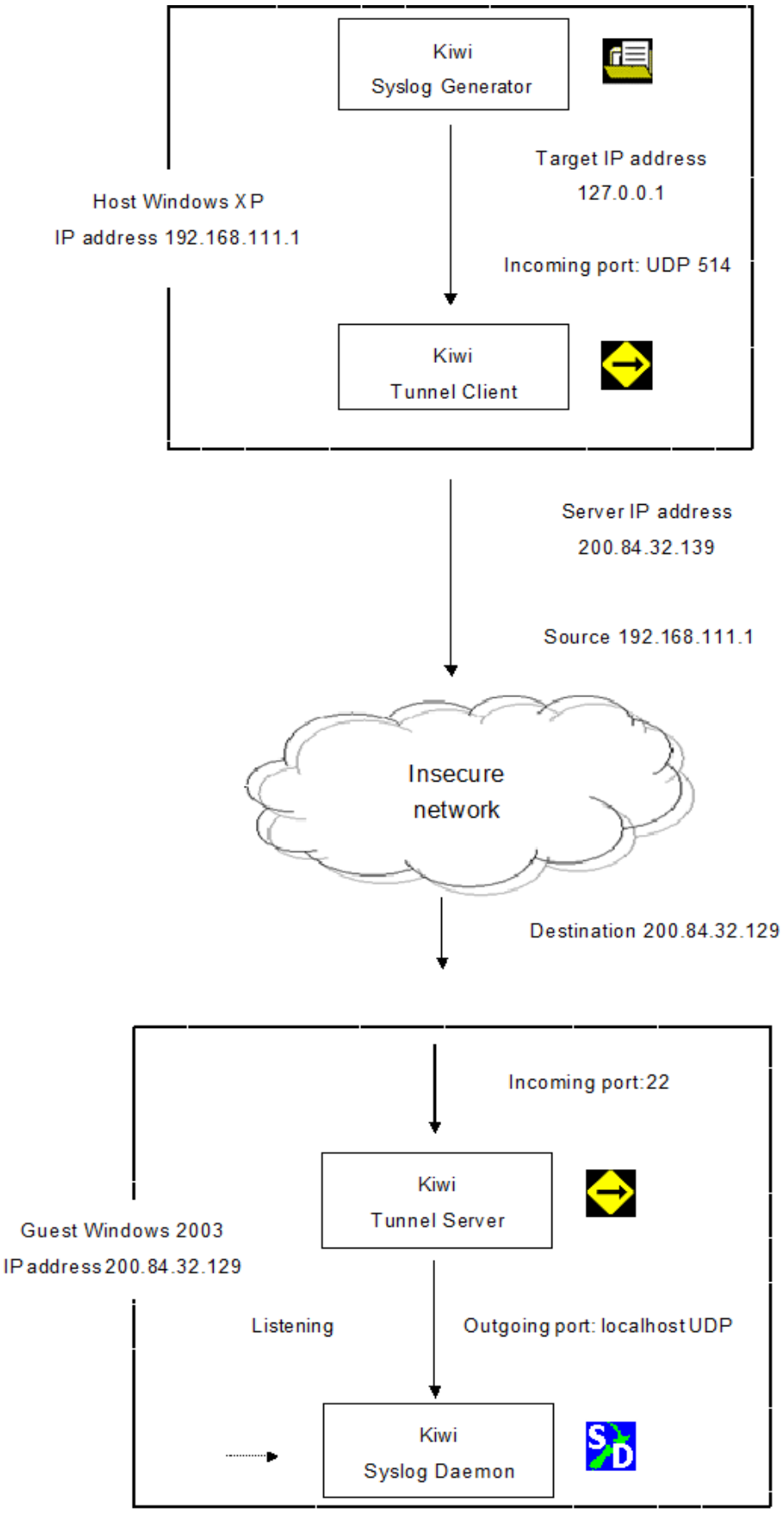

Figure 3.1 - Experimental arrangement of the Kiwi tunnel

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

3.2 VPN tunnel with PPTP[9]

To experiment with another possible solution regarding the security of syslog and SNMP trap messages, a VPN tunnel was configured using a Windows 2003 server. A VPN virtual lab was installed locally without having to be connected to the Internet, using VMware, as illustrated in the following figure. The VPN server has Windows Server 2000/2003. With Windows Server 2000 problems were encountered in issuing certificates for VPN with IPSec. The connection between the VPN client and the VPN server was made using the virtual interfaces VMnet1, VMnet2 and VMnet3.

- VMnet1, 2 and 3 were configured with their respective IP addresses, through the Edit menu
- | Virtual Network Settings | Host Virtual Network Mapping and then filling in the subnet boxes.
- Then a DHCP server was added and activated for VMnet2. (Note: If there is already a DHCP server in the private network, this is not necessary).
- The necessary Ethernet network adapters were added for the VPN server. NIC 2 is connected to VMnet2.
- The Windows 2003 server (host system) was started and then the VPN service was activated through the Start | Administrative tools | Routing and remote access.
- A user account for remote connection was created and activated.

Establishing the PPTP tunnel

- Once the previous phases were completed, on the host system side, a new network connection was created to establish a PPTP tunnel, according to the steps illustrated below.
    - Selection of the type of network connection
    - Network type connection mode selection
    - Selecting the name or address of the VPN server
    - VPN type selection on the client
- Using the correct login and password, the VPN connection via PPTP was quickly established.
- By clicking on the connection, interesting details about the PPTP tunnel could be seen.
- On the side of the VPN client, IPconfig was executed and the existence of a new temporary PPP adapter with its IP address corresponding to one end of the tunnel could be noticed.

Traffic capture

- To verify that Syslog messages and SNMP traps actually travelled encrypted, the Ethereal traffic analyzer was used and the traffic was captured in various parts of the network. The results are shown in the following steps
    - Syslog messages encrypted and compressed by the PPTP tunnel
    - Messages decrypted outside the PPTP tunnel

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

2.3 VPN tunnel with L2TP / IPSec[10]

This experience turned out to be much more complicated than the previous ones due to problems with digital certificates. The Windows operating system supports two authentication methods for L2TP / IPSec-based VPN connections: shared secret key or digital certificates. The first method is weak, so it is only recommended as a temporary measure while implementing the public key infrastructure (PKI) to obtain digital certificates.

Digital Certificate Server Installation

To have the certificate issuance service available on a Windows 2000/2003 server, the Web server known as IIS (Internet Information Services) must first be installed. Then using the Add / Remove Windows Components procedure, the Certificate Server service is installed.

- The Enterprise Root Certification Authority installation requires that the server be a member of a domain and that the Active Directory service be used. For simplicity, the independent root CA was used.
- In Common name for this certification authority, a descriptive name (VPN Authority) was put. The Full name suffix box was also filled in, separating the fields with a comma.
- Once the service was installed, it was managed through Configuration | Administrative Tools | Certificate Issuing Entity.
- It was configured so that the certificate is issued automatically when a user requests it via the Web.
- After the certificate service was installed, the VPN service was installed using Start | Administrative tools | Routing and Remote Access by selecting the first option in the Wizard.

Here the remote access option for VPN was chosen:

- Connection type for remote access
- In addition, the external and internal interface had to be carefully selected. The Enable security check box was also cleared to have fewer testing problems.
- At the end of the Wizard, the details of the service (Network Interfaces, Remote Access Clients, Ports, IP Routing) could be viewed. In particular, it was noted that part of the WAN miniports are of the PPTP type and the rest are L2TP.

Certificate for VPN server[11]

The next step was to obtain and install a digital certificate for the VPN server. It should be taken into account that when trying to establish a VPN L2TP / IPSec connection, the authentication of computers does not occur if the certificate of the VPN server does not have the purpose of Server authentication configured in the extensions in the extensions of Enhanced Use of Keys (EKU : Enhanced Key Usage) of the certificate. But although the VPN servers that terminate the remote user connections only need a certificate that has the Server Authentication purpose configured in the EKU extensions, a VPN server that is used as the endpoint of a VPN connection with another VPN server originates (as a client) and terminate (as a server) VPN connections. For this reason, the certificate of these servers must contain both the Server Authentication purpose and the Client Authentication purpose in the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

EKU extensions. Also, due to the way automatic certificate selection works, both purposes (Server Authentication and Client Authentication) must be contained in the same certificate.

- From the machine where the VPN server was installed (which is the same machine where the certificate server is installed), through Internet Explorer a connection was made to http: // servername / certsrv, where servername is the name of the certificate server, for example, http: / localhost / certsrv. Here was selected Request a certificate and then Advanced request.

In the next window, the first option was selected: Create and send a request to this CA. The form was filled out with the requested data. Under Type of certificate required, Other… was selected with OID 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, which corresponds to Server Authentication and Client Authentication. Mark keys as exportable and also Store the certificate in the certificate store of the local computer was activated.

- Upon submitting the request, the certificate was immediately granted and its installation proceeded.
- To manage the certificates, the Windows MMC (Microsoft Management Console) was used.
- Through MMC it was verified that the certificate appeared under Certificates (local computer), since otherwise it could not establish an IPSec tunnel. By double-clicking on the certificate, it was verified that the field Enhanced key usage showed Server authentication and Client authentication with their respective OIDs.
- It was verified if under Trusted Root Certification Authorities, the certificate of the issuing authority for that certificate was listed. Since it was not, it was searched under Intermediate Certification Authorities, from where it was copied and pasted to Trusted Root Certification Authorities, otherwise IPSec would not work.

Certificate for VPN client

When trying to establish an L2TP / IPSec VPN connection between a Windows client and a Windows 2000/2003 Server-based VPN server, authentication fails if the VPN client certificate located in the local computer's certificate store, does not have the Authentication purpose configured the client's extensions in the certificate's Enhanced Key Usage (EKU) extensions.

From a PC equipped with Windows XP and using Internet Explorer, the same procedure that was previously described for the VPN server was repeated, only that in the type of certificate required, Client Authentication Certificate was selected.

The certificate was verified to appear under Certificates (local computer), otherwise it could not establish an IPSec tunnel.

It was verified if under Trusted Root Certification Authorities, the certificate of the issuing authority for that certificate was listed. Since it was not, it was searched under Intermediate Certification Authorities, from where it was copied and pasted to Trusted Root Certification Authorities, otherwise IPSec would not work.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

L2TP / IPSec tunnel establishment

Once the certificate was installed, a new network connection was created to establish a tunnel with IPSec, following the same steps as for creating a PPTP connection, except that in network type, L2TP / IPSec was selected.

Using the correct login and password, the VPN connection using PPTP was established not as quickly as in the case of PPTP, although at times it could not be established due to problems with certificates or IP addresses. By clicking on the connection, interesting details could be observed, such as the type of encryption (IPSec, ESP, 3DES) and the IP address of the server and client. Those internal virtual addresses are temporary and are supplied by the VPN server in conjunction with the DHCP server.

Traffic capture

To verify that the Syslog and SNMP Traps messages actually travel encrypted, the Ethereal traffic analyzer was used and the traffic was captured in various parts of the network. The results are shown in the following figures. It was observed that the IPSec packets are of the ESP (Encapsulated Security Payload) type.

- Encrypted messages inside the L2TP / IPSec tunnel
- Messages decrypted outside the L2TP / IPSec tunnel
- Encrypted Trap Messages within the IPSec / L2TP Tunnel

3.4 VPN tunnel with OpenVPN

A third solution that was tested to improve the security of Syslog and SNMP messages was using OpenVPN.

The first step in creating a tunnel was to verify that the two machines were able to see each other through their real IP addresses. Then a common static key was generated to be used by both machines. This key is saved in a key.txt file in the folder where OpenVPN was installed and that same file is then copied to the other PC.Next we proceeded to edit the configuration file config.ovpn, which contains the tunnel parameters:

Details of the config.ovpn file on PC A

Edit this file, and save to a .ovpn extension

so that OpenVPN will activate it when run as a service. # Change 'myremote' to be your remote host,

or comment out to enter a listening # server mode.

remote 200.84.32.129 ⇦ In the remote parameter, enter the IP address of the PC to which you want to make the connection

Uncomment this line to use a different # port number than the default of 5000.

; port 5000

ifconfig 10.3.0.1 255.255.255.0 ⇦ In the**ifconfig** parameter, the address that the PC will have in the tunnel with its respective subnet mask is placed

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

10.3.0.1 is the local VPN IP address and

10.3.0.2 is the remote VPN IP address.

secret key.txt ⇦ The secret parameter contains the name of the file with the shared secret key.

Details of the config.ovpn file on PC B

Edit this file, and save to a .ovpn extension

so that OpenVPN will activate it when run as a service. # Change 'myremote' to be your remote host,

or comment out to enter a listening # server mode.

remote 192.168.111.1

Uncomment this line to use a different # port number than the default of 5000.

; port 5000

ifconfig 10.3.0.2 255.255.255.0

secret key.txt

Once OpenVPN was configured, the tunnel was activated through the Start OpenVPN quick menu that appears when you press the right mouse button on the config.ovpn file. This must be done on both machines.

After this action, a DOS window was automatically opened showing how the connection is being established and the different parameters of the same.

- OpenVPN connection status window

Traffic capture

To verify that the Syslog and SNMP Traps messages actually traveled encrypted, the Ethereal traffic analyzer was used at various points on the network. The results are shown in the following steps. The use of port 5000 and the UDP protocol could be noticed.

- Syslog messages encrypted in the OpenVPN tunnel
- Syslog messages decrypted outside OpenVPN tunnel
- Encrypted Trap messages inside the OpenVPN tunnel

CONCLUSIONS AND RECOMMENDATIONS

Modern organizations increasingly depend on the proper functioning of communication systems and their computing resources to carry out their daily activities. The expression "the network is down" or "the network is slow" is less and less justifiable and in this sense a good management system must be available to supervise its correct operation.

The use of event notification mechanisms such as Syslog and SNMP traps is vital to determine critical situations, for example congestion, failure or hacker attack. However, these mechanisms suffer from a series of weaknesses from the point of view of security, as it was

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

verified during the development of this work. In fact, notification messages are not encrypted or authenticated, so they are relatively easy to forge or adulterate (for example, capturing an authentic message and then modifying and forwarding it).

In order to find possible security enhancements that were relatively easy to implement, a number of commercial and open source technologies were tested and evaluated, essentially establishing a secure channel ("tunnel") between the source and destination of email messages, notification. These technologies are sometimes called VPN (Virtual Private Network).

The strengths and weaknesses of the solutions studied in this work are summarized below.

Point to Point Tunneling Protocol (PPTP): It is a protocol that only works under a Windows environment and also requires a Windows Server 2000 or 2003 as VPN server. It is relatively easy to use and perfectly transports both Syslog and SNMP.

Layer 2 Tunneling Protocol (L2TP) with IPSec:IPSec is more complicated to use, since it requires digital certificates at both ends of the tunnel, and also usually does not work behind a NAT (Network Address Translation). It perfectly transports both syslog and SNMP. When using it with L2TP under Windows environment, a Windows Server 2000 or 2003 is required, as VPN server.

Kiwi Syslog Tunnel: It is a commercial product optimized for the secure transport of syslog and can function as a gateway, carrying the traffic of multiple syslog clients. In addition, the Kiwi Tunnel Client can be used to concentrate the traffic of different machines and equipment that need to send syslog messages to a remote syslog server, but it does not carry other protocols other than syslog, for example SNMP traps.

As a final conclusion, among the different technologies evaluated, the one that represents the best alternative for improving security in notification messages and event logs is the Point-to-Point Tunnel Protocol (PPTP), due to its ease of use and transparency to the transported protocols.

For future work it is recommended to test and evaluate the new version 3 of SNMP, which incorporates strong security mechanisms, although SNMPv3 agents are not yet readily available.

It is also recommended to test and evaluate the different secure syslog proposals, such as SDSC Secure Syslog, syslog-ng and msyslog, among others, which offer the possibility of using the TCP protocol for the transmission of messages, advanced filtering functions and the recording of messages directly in a SQL-like database.

References

1 O'Mahony, Donal. (1994). Security considerations in a network management environment. Network, IEEE. 8. 12 - 17. 10.1109/65.283929.

2 Ahmad, Nadeem & Habib, M.. (2010). Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution. http://www.bth.se/fou/cuppsats.nsf. I. 93.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 18154 - 18166
Received 25 April 2021; Accepted 08 May 2021.

3 Afonso, João& Monteiro, Edmundo & Ferreira, Carlos. (2005). Monitoring and alarm management for system and network security a web-based comprehensive approach.. 348-355.
4 Shadmanov, Istam&Shadmanova, Kamola&Rakhimov, Rakhimjon. (2016). A Survey on Security Services and Mechanisms in Distributed Systems. International Journal of Trend in Research and Development. 3. 2394-9333.
5 El Jaouhari, Saad&Bouabdallah, Ahmed. (2018). Dynamic Security Management of Smart WoT Infrastructures Using SDN. 10.1109/VTCFall.2018.8690740.
6 Mekelleche, Fatiha&Hafid, Haffaf&OuldBouamam, Belkacem. (2018). Monitoring of Wireless Sensor Networks: Analysis of Intrusion Detection Systems. 421-426. 10.1109/CoDIT.2018.8394844.
7 Rolstadas, Asbjorn&Tommelein, Iris &Schiefloe, Per & Ballard, Glenn. (2014). Understanding project success through analysis of project management approach. International Journal of Managing Projects in Business. 7. 10.1108/IJMPB-09-2013-0048.
8 Kiwi Enterprises Website, http://www.kiwisyslog.com/index.htm
9 Jahan, Sohely& Rahman, Md&Saha, Sajeeb. (2017). Application Specific Tunneling Protocol Selection for Virtual Private Networks. 10.1109/NSysS.2017.7885799.
10 Fan, Ya-qin& Li, Chi & Sun, Chao. (2012). Based on combination of L2TP and IPSec VPN security technology research. JNW. 7. 141-148. 10.4304/jnw.7.1.141-148.
11 Aljumaily, Mustafa &Kodituwakku, Angel. (2018). Final Project Virtual Private Network (VPN) Lab. 10.13140/RG.2.2.17464.24323.