Network security audit report

Atheer ahmed

Collage: HBSA

Date: 1/1/2022

# Abstract

* In this audit report I will carry out security audit of the network.
* State the IDS built-in and 3rd party software.
* Analyze the network traffic and identify security threats and make recommendations regarding improvements.
* Review password policies, OS logs, hardware, and system configuration.
* Implement security changes and record it in help-desk software.

Copyright © 2021 by Atheer Alghamdi.

All rights reserved.

Table of Contents

[Abstract 2](#_Toc123114022)

[Table of figures 4](#_Toc123114023)

[Scope of audit 5](#_Toc123114024)

[Areas to be reviewed 6](#_Toc123114025)

[Utilities to be used 7](#_Toc123114026)

[Wireshark installation steps 8](#_Toc123114027)

[Definition 8](#_Toc123114028)

[Uses 8](#_Toc123114029)

[benefits 8](#_Toc123114030)

[Color coding 8](#_Toc123114031)

[Installation 9](#_Toc123114032)

[Review password policy 20](#_Toc123114033)

[Definition 20](#_Toc123114034)

[Importance 20](#_Toc123114035)

[Review operating system logs 21](#_Toc123114036)

[Discover event viewer 21](#_Toc123114037)

[Method 1 21](#_Toc123114038)

[Method 2 22](#_Toc123114039)

[How to filter error 22](#_Toc123114040)

[Review configuration of hardware & software on network 25](#_Toc123114041)

[Currant 25](#_Toc123114042)

[Recommendation 25](#_Toc123114043)

[Identify threats using Wireshark 26](#_Toc123114044)

[Identify threats using antivirus 27](#_Toc123114045)

[Audit table 28](#_Toc123114046)

[Security measure taken 29](#_Toc123114047)

[Update help desk software 30](#_Toc123114048)

[Conclusion 31](#_Toc123114049)

[Reference 32](#_Toc123114050)

# Table of figures

# Scope of audit

* Firewall.
* Intrusion Detection System (IDS).
* Antivirus definitions up to date.
* Password policy.
* Operating System logs.

# Areas to be reviewed

* Password Policy.
* Operating system Logs.
* Hardware & software configuration.
* Security Policy.

# Test that can be automated

* Antivirus scan.
* Identify threats using Wireshark.
* Review OS logs using Event viewer.

# Utilities to be used

* Wireshark.
* Antivirus.
* Event viewer.

# Wireshark installation steps

## Definition

Wireshark Is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

## Uses

analyze network traffic in real time and is often the best tool for troubleshooting issues on your network. Common problems that Wireshark can help troubleshoot include dropped packets, latency issues, and malicious activity on your network, moreover Wireshark is a 3rd party software.

## benefits

* Free software.
* Available for multiple platforms – Windows & UNIX.
* Can see detailed information about packets within a network
* Not proprietary can be used on multiple vendors unlike Cisco Prime

## Graphical user interface, application Description automatically generatedColor coding

Figure 1 coloring rules

Figure 2 color in wireshark

## Installation

|  |
| --- |
| Turn on your PC by pressing the power button (Windows will start automatically).    Figure |
| Use msinfo32 (press Windows key, type "run", then type "Msinfo32") to display the system type. The system type will either be X86-based PC or X64-based PC. X86-based PC is a 32-bit system. X64-based PC is a 64-bit system.  How to Tell if Your Computer Is 32 or 64 Bit Windows 10 - EaseUS  Open a web browser.    Navigate to <http://www.wireshark.org>.  Select Download Wireshark.  How to install Wireshark to monitor your network – or use with NMAP packet  scanner | University of South Wales: Cyber University of the year: Three  years running: 2019, 2020, 2021  Select the Wireshark Windows Installer matching your system type, either 32-bit or 64-bit as determined in Activity 1. Save the program in the Downloads folder.  5.7. Exporting Data  Close the web browser. |
| Locate the version of Wireshark you downloaded, double-click on the file to open it.  Wireshark User's Guide |
| If you see a User Account Control dialog box, select Yes to allow the program to make changes to this computer.  Disable Do You Want to Allow This App to Make Changes  Select Next > to start the Setup Wizard.  Setup Wizard I Antamedia software |
| Review the license agreement. If you agree, select I Agree to continue.  electron - How to show accept terms and conditions window after click on  application exe file - Stack Overflow  Select Next > to accept the default components.  DOWNLOAD AND INSTALL Rtools  Select the shortcuts you would like to have created. Leave the file extensions selected. Select Next > to continue.    Select Next > to accept the default install location.    Select Install to begin installation.  Standard Installation Procedure  Select Next > to install WinPcap.  Install Winpcap - an overview | ScienceDirect Topics |
| Select Next > to start the Setup Wizard.  Install Winpcap - an overview | ScienceDirect Topics  Review the license agreement. If you agree, select I Agree to continue.  Licence Agreement | Deltarune | Know Your Meme |
| Select Install to begin installation.  Custom Installation Procedures  Select Finish to complete the installation of WinPcap.  Installing GNS3 Network Simulator | Pluralsight  Select Next > to continue with the installation of Wireshark.  Installation and setup | Mastering Wireshark 2 |
| Select Finish to complete the installation of Wireshark.  Installing GNS3 Network Simulator | Pluralsight |

# Review password policy

## Definition

Password policies help you define the structure and complexity of passwords to be used. You can either make use of the predefined policies or create new policies to suit the needs of your organization.

Importance

The IT system and processes are secure and that users are correctly identified and authorized. / Protect your business and your employees from cyber-attacks.

## Review wireless router password policy

Screenshot

First screenshot simple password

Second screenshot after changing it to complex password.

# Review operating system logs

Event Viewer is a component of Microsoft's Windows NT operating system that lets administrators and users view the event logs on a local or remote machine.

## Discover event viewer

### Method 1

|  |
| --- |
| Open Windows Control Panel |
| Click System and Security |
| How to Show or Access Administrative Tools in Windows 10Click Administrative Tools |
| What Is the Windows Event Viewer, and How Can I Use It?EVDouble-click Event Viewer |

|  |
| --- |
| Open Run dialog by pressing Windows+R. |
| Clear Windows Event Viewer Logs - IT SUPPORT PERTHType eventvwr.msc (or eventvwr.exe) and click OK. |

### Method 2

### How to filter error

|  |
| --- |
| Open Event viewer |
| expand windows log |
| Right click system |
| Filter current log > error > ok. |
| Error |

# Review configuration of hardware & software on network

## Currant

(From system information)

|  |  |
| --- | --- |
| CPU | I-5 |
| RAM | 8 GB |
| DISK storage | 500 GB |
| Software | Windows 8.1.  Wireshark.  Microsoft Visual C++. |

## Recommendation

(Should be Higher than the current one and).

Write **why should we** change here (……) not in the table.

|  |  |
| --- | --- |
| CPU |  |
| RAM |  |
| DISK storage |  |
| Software |  |
| Network |  |

# Identify threats using Wireshark

Just Screenshot

3 pictures

# Identify threats using antivirus

Antivirus software, also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses.

Examples:

* Norton
* McAfee
* Kaspersky

(Scan antivirus in the lap)

# Audit table

identified security threats (from password policy from "local security", event viewer, antivirus scan, Wireshark scan).

|  |  |
| --- | --- |
| Threat | recommendation |
| Simple password set in wireless router | Configure wireless router with a complex password (explain with example…) |
| Broadcasting of SSID Enabled | Disable SSID (explain why) |
| Firewall disabled | Enable the firewall (explain why) |
| Minimum p/w length: 2  (3 threats from password policy | An eight-character password is recommended because it's long enough to provide adequate security and still short enough for users to easily remember. |
| event viewer (ID – تعريف) |  |
| event viewer |  |
| event viewer |  |
| antivirus scan |  |
| antivirus scan |  |
| antivirus scan |  |
| Wireshark scan (black) same as event viewer |  |
| Wireshark scan (black) same as event viewer |  |
| Wireshark scan (black) same as event viewer |  |

# Security measure taken

(Screenshot)

Block port 21 (ctrl panel>s/m security>windows Firewall>Adv settings>Outbound rules>New Wizard>port)

Block IP address 216.27.61.137 (ctrl panel>s/m security>windows Firewall>Adv settings>Outbound rules>New Wizard>custom>All programs>add IP address)

Block Hotmail.com (Find IP address from command prompt and block. Ns lookup www.Hotmail.com [204.79.197.212])

Block Telnet (port 23)

Enable remote access (ctrl panel>s/m & security>S/m>Adv settings>Remote access)

# Update help desk software

(Access- help desk ticketing)

Record the changes made using the help-desk software.

Attach the screenshot

In Fault Log

Problem: Simple password

Solution: changed to complex password.

2. Problem: Firewall disabled

Solution: Firewall enabled (Blocked port 21, Blocked telnet, Blocked Hotmail.com, Blocked 216.27.61.137 and enabled remote access)

# Conclusion

In this audit

# Reference