CYBR 306 - Information Security and Assurance

Exercise 03

Submitted by:

Kadeem Reid

Submitted to:

Benjamin Yankson, Ph.D.

TABLE OF CONTENTS

Objective:

This exercise aims to give you significant experience in conducting security analyses, analyzing the requirements for organization security policies, and conducting vulnerability assessments using GFI Languard's vulnerability scanning software.

Part B: Install and Configure OpenVAS– Perform Network vulnerability scan

Task 2:

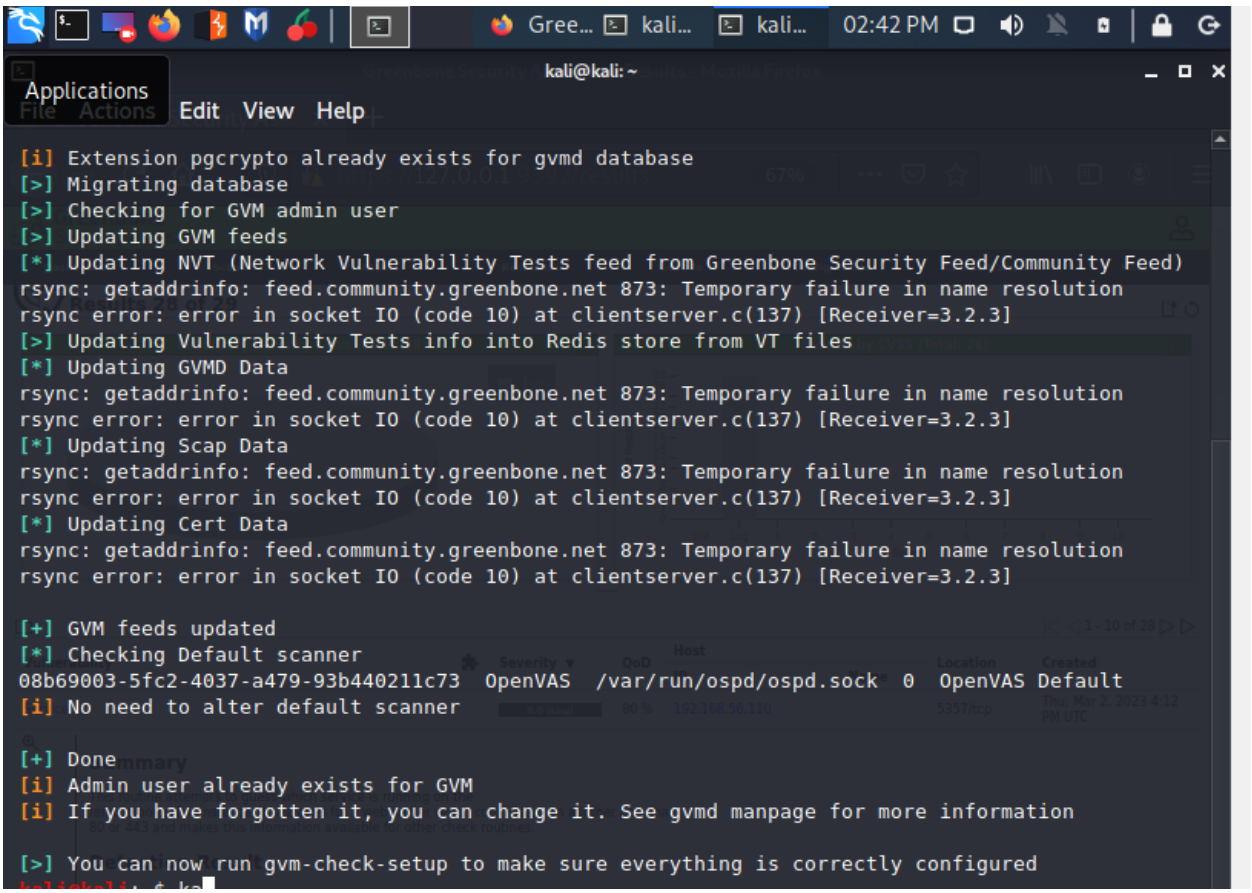


Figure 1. Successful download and install of the necessary plugins

Task 4:

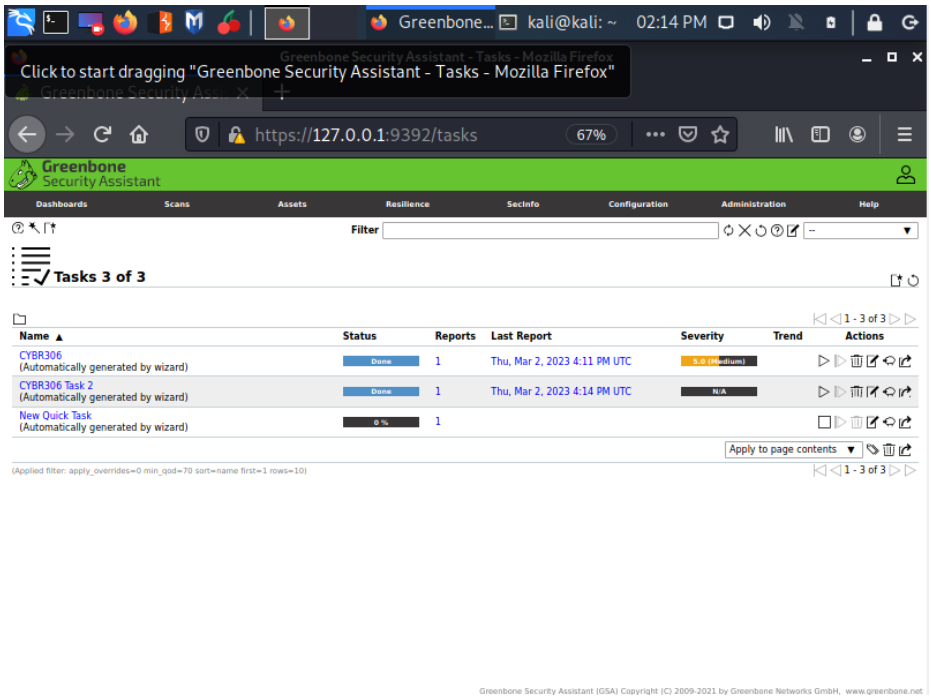


Figure 2. Successful vulnerability scan

Task 5:

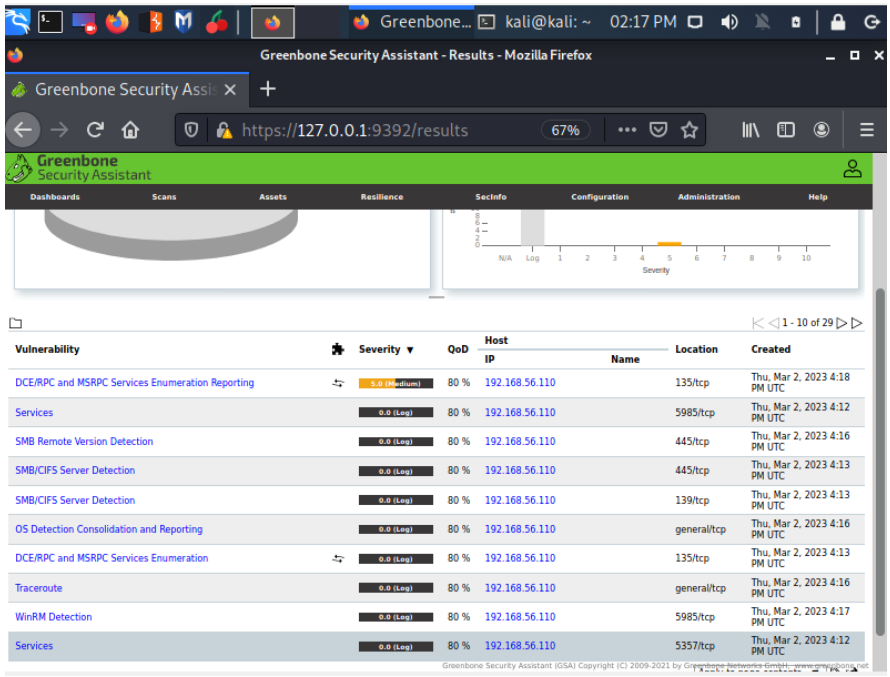


Figure 3. List of found vulnerabilities

After doing the vulnerability scan, I discovered that there are a few vulnerabilities on my network. The main one was DCE/RPC and MSRPC Services Enumeration Reporting, which an attacker could use to gain more knowledge about the remote host. This is considered a medium risk vulnerability. These services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. The vulnerability scan also showed the list of DCE/RPC or MSRPC services running on this host via the TCP protocol. According to the scan the recommended solution for this vulnerability is mitigation, simply filtering incoming traffic to these ports.

Part C: Install and Configure GFI Languard– Threat & Vulnerability Scan

****For this section I had to download an alternative version of GFI Languard, therefore some screenshots of the setup are missing, but I promise this is my work****

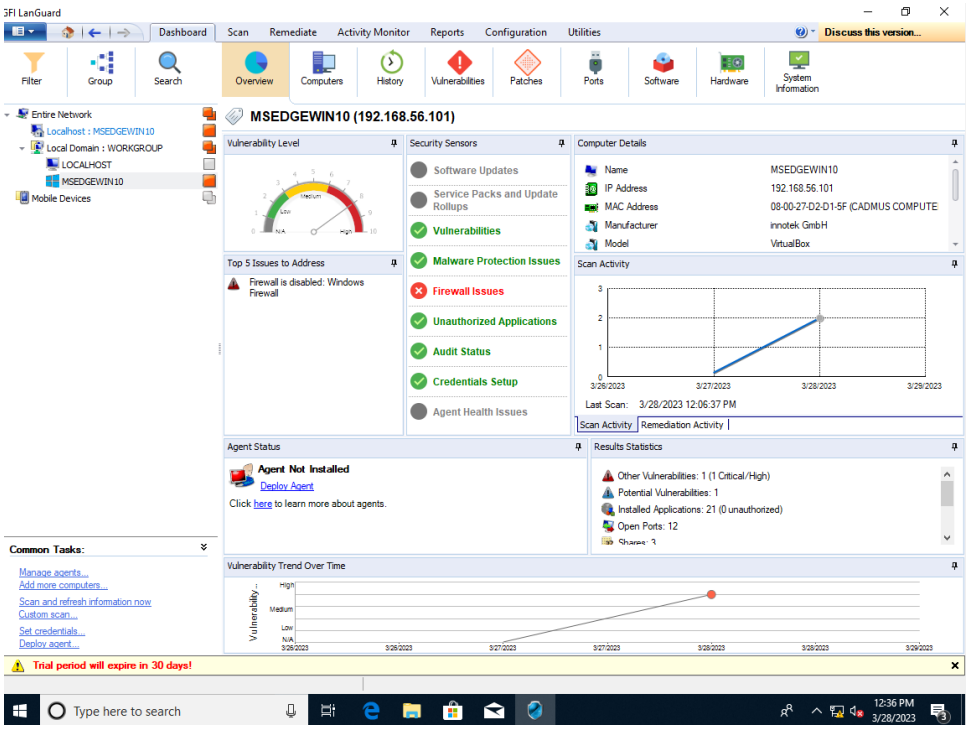
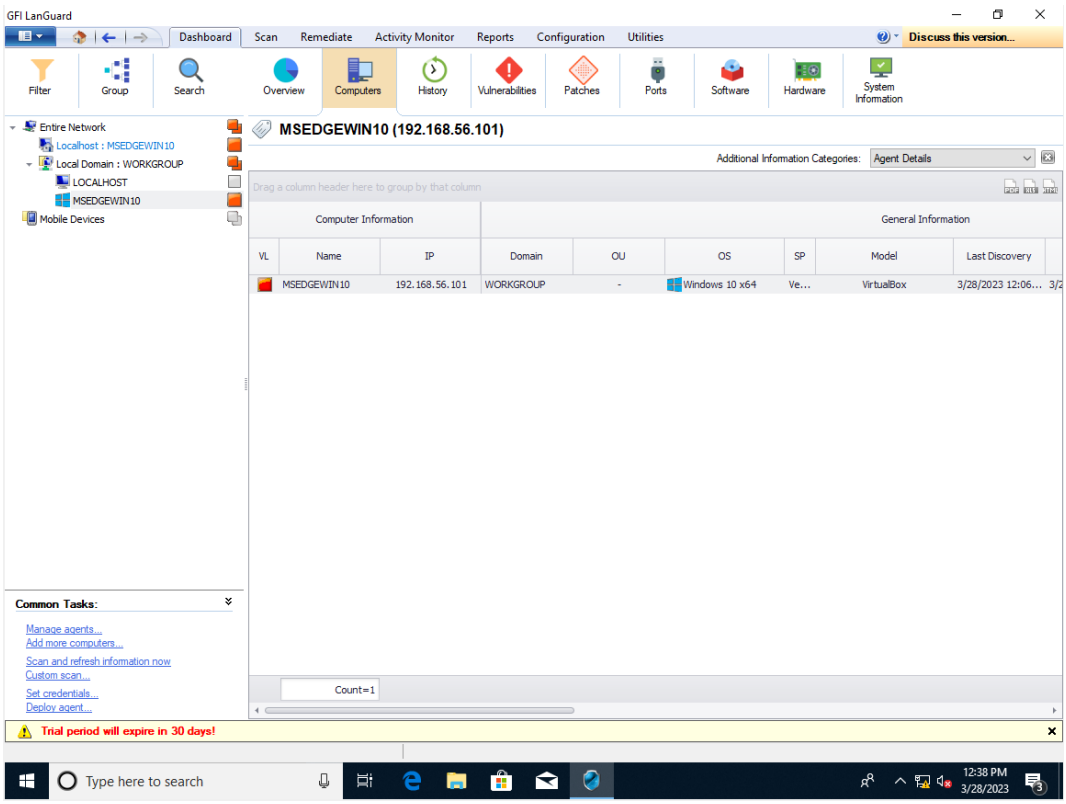
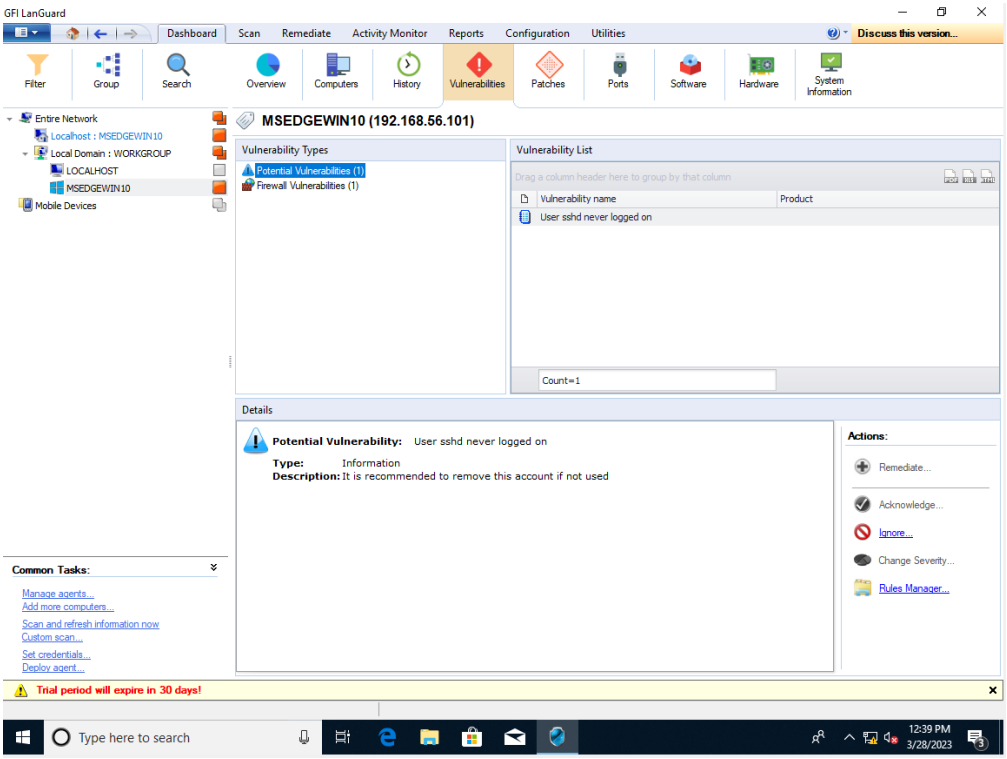
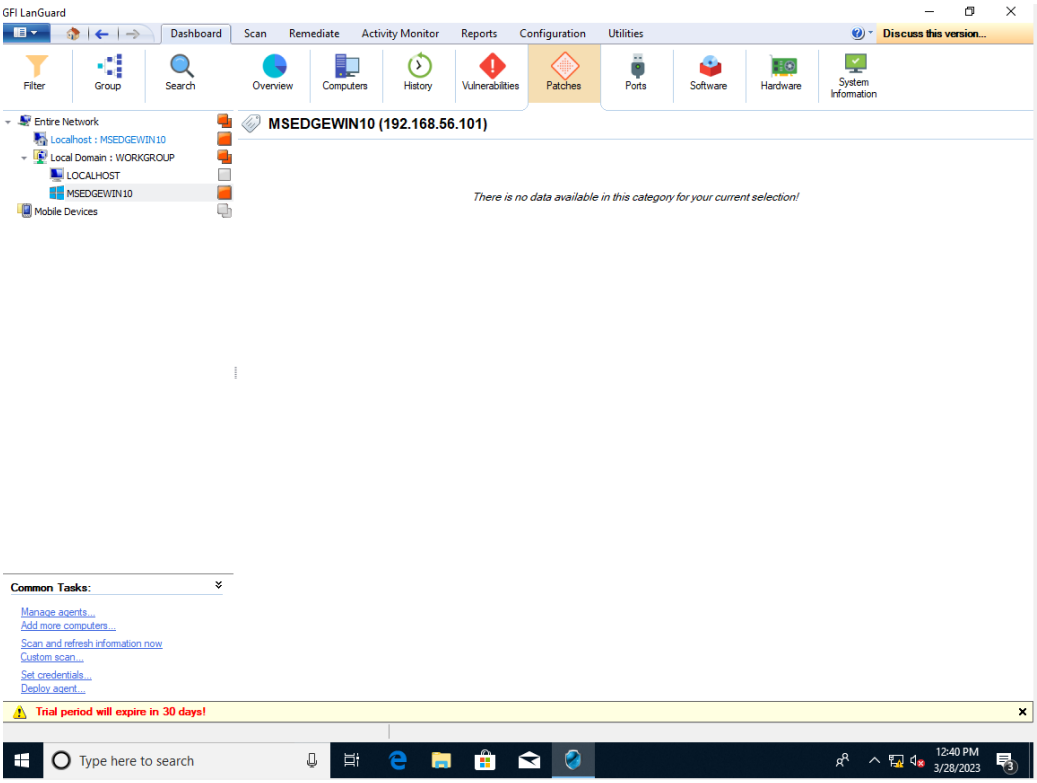


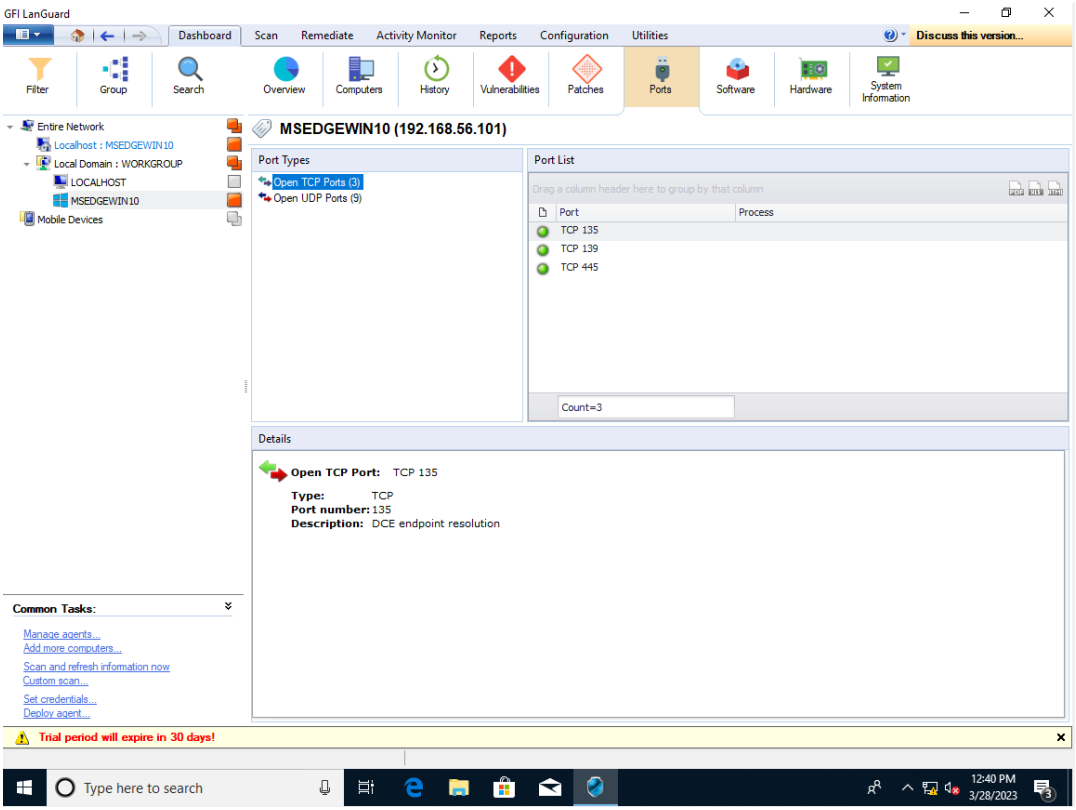
Figure 4. Depiction of successful installation of GFI Languard

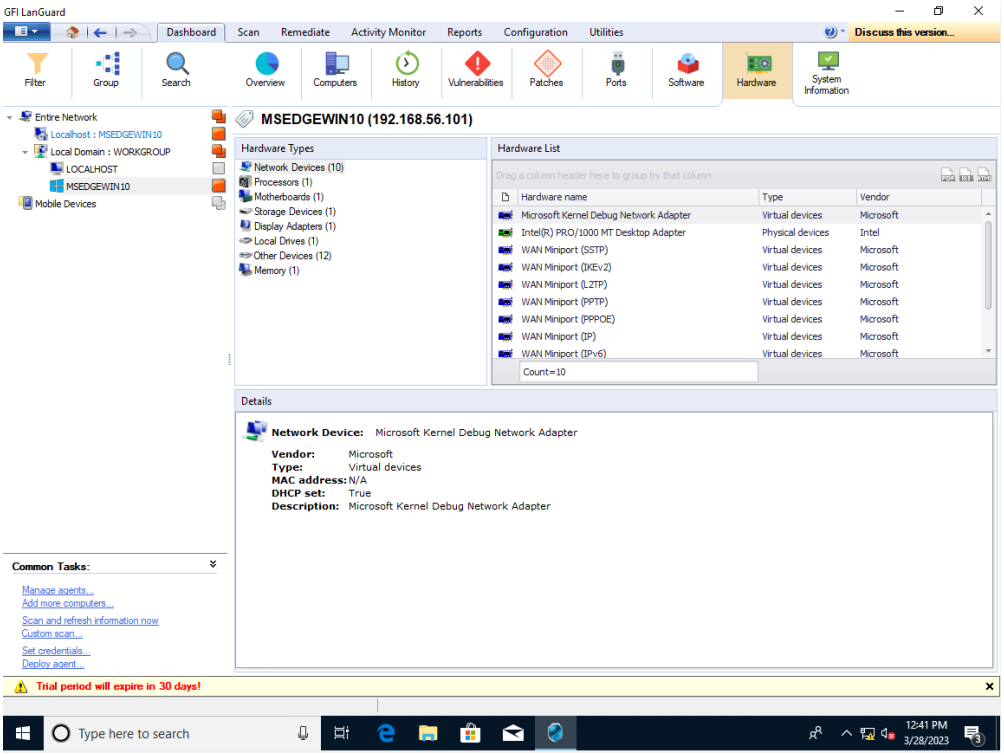
III.

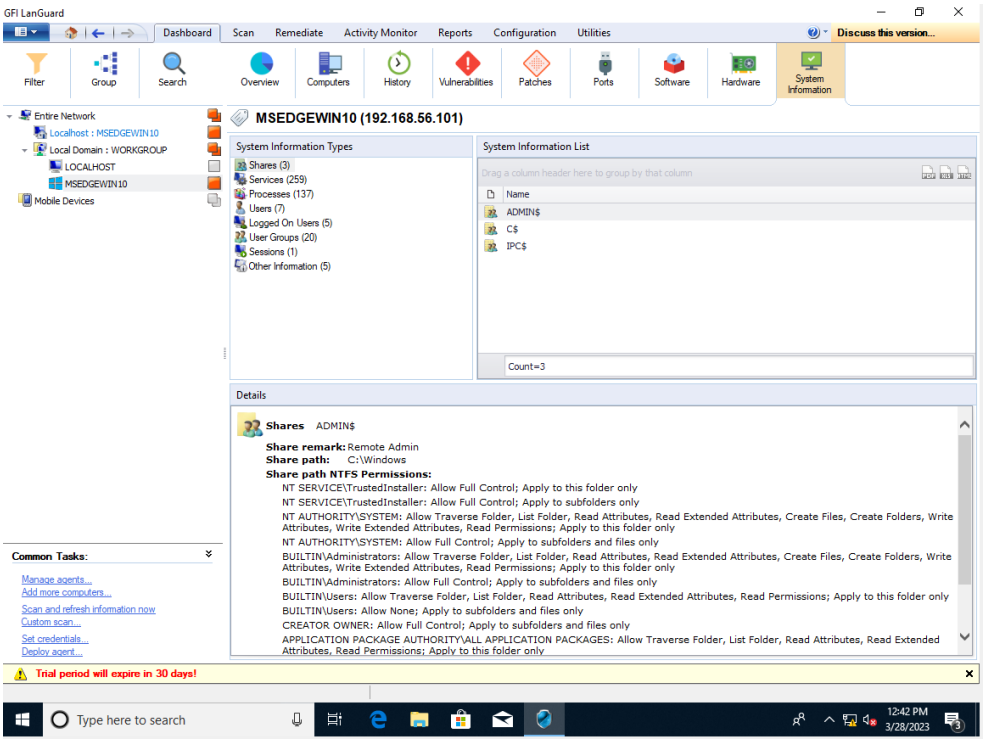

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
Additional Information Categories:
Agent Details
Computer Information
General Information
VL
Name
IP
Domain
OU
OS
SP
Model
Last Discovery
MSEDGEWIN10
192.168.56.101
WORKGROUP
Windows 10 x64
VirtualBox
3/28/2023 12:06...
Count=1
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:38 PM
3/28/2023

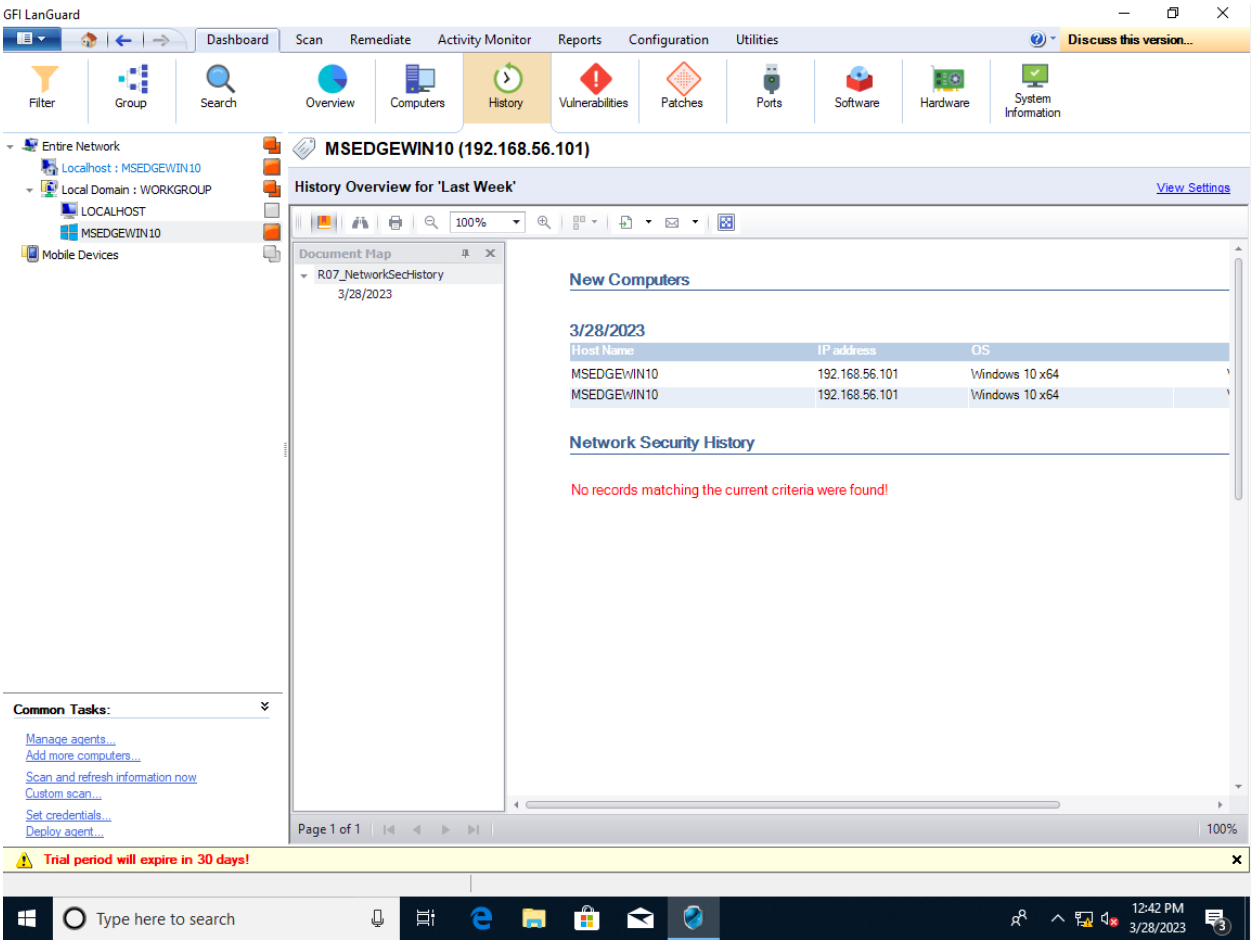

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
Vulnerability Types
Potential Vulnerabilities (1)
Firewall Vulnerabilities (1)
Vulnerability List
Vulnerability name
Product
User sshd never logged on
Count=1
Details
Potential Vulnerability: User sshd never logged on
Type: Information
Description: It is recommended to remove this account if not used
Actions:
Remediate...
Acknowledge...
Ignore...
Change Severity...
Rules Manager...
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:39 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
There is no data available in this category for your current selection!
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:40 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
Port Types
Open TCP Ports (3)
Open UDP Ports (9)
Port List
Drag a column header here to group by that column
Port
Process
TCP 135
TCP 139
TCP 445
Count=3
Details
Open TCP Port: TCP 135
Type: TCP
Port number: 135
Description: DCE endpoint resolution
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:40 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
Hardware Types
Network Devices (10)
Processors (1)
Motherboards (1)
Storage Devices (1)
Display Adapters (1)
Local Drives (1)
Other Devices (12)
Memory (1)
Hardware List
Drag a column header here to group by that column
Hardware name
Type
Vendor
Microsoft Kernel Debug Network Adapter
Virtual devices
Microsoft
Intel(R) PRO/1000 MT Desktop Adapter
Physical devices
Intel
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IP)
WAN Miniport (IPv6)
Count=10
Details
Network Device: Microsoft Kernel Debug Network Adapter
Vendor: Microsoft
Type: Virtual devices
MAC address: N/A
DHCP set: True
Description: Microsoft Kernel Debug Network Adapter
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:41 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
MSEDGEWIN10 (192.168.56.101)
System Information Types
Shares (3)
Services (259)
Processes (137)
Users (7)
Logged On Users (5)
User Groups (20)
Sessions (1)
Other Information (5)
System Information List
Drag a column header here to group by that column
Name
ADMIN$
C$
IPC$
Count=3
Details
Shares ADMIN$
Share remark: Remote Admin
Share path: C:\Windows
Share path NTFS Permissions:
NT SERVICE\TrustedInstaller: Allow Full Control; Apply to this folder only
NT SERVICE\TrustedInstaller: Allow Full Control; Apply to subfolders only
NT AUTHORITY\SYSTEM: Allow Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files, Create Folders, Write Attributes, Write Extended Attributes, Read Permissions; Apply to this folder only
NT AUTHORITY\SYSTEM: Allow Full Control; Apply to subfolders and files only
BUILTIN\Administrators: Allow Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files, Create Folders, Write Attributes, Write Extended Attributes, Read Permissions; Apply to this folder only
BUILTIN\Administrators: Allow Full Control; Apply to subfolders and files only
BUILTIN\Users: Allow Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Read Permissions; Apply to this folder only
BUILTIN\Users: Allow None; Apply to subfolders and files only
CREATOR OWNER: Allow Full Control; Apply to subfolders and files only
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES: Allow Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Read Permissions; Apply to this folder only
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:42 PM
3/28/2023



Figures 5-11. Successful scan on MSEdge- Win 10 Clone(information from Dashboard)

IV.

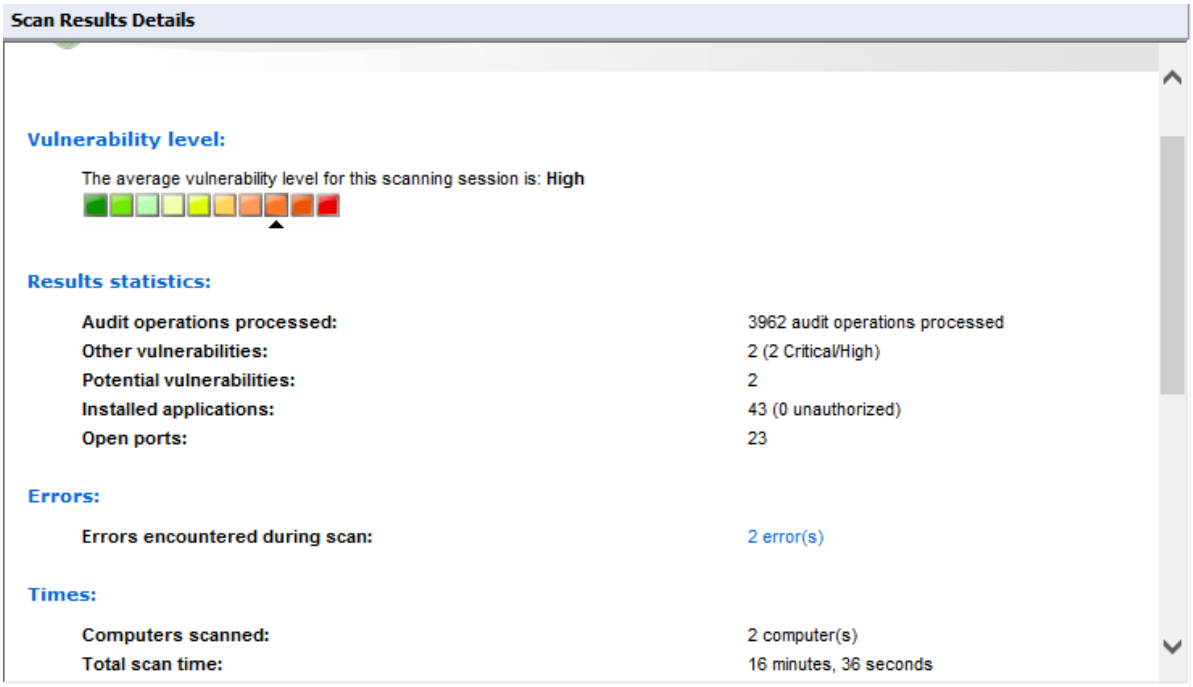
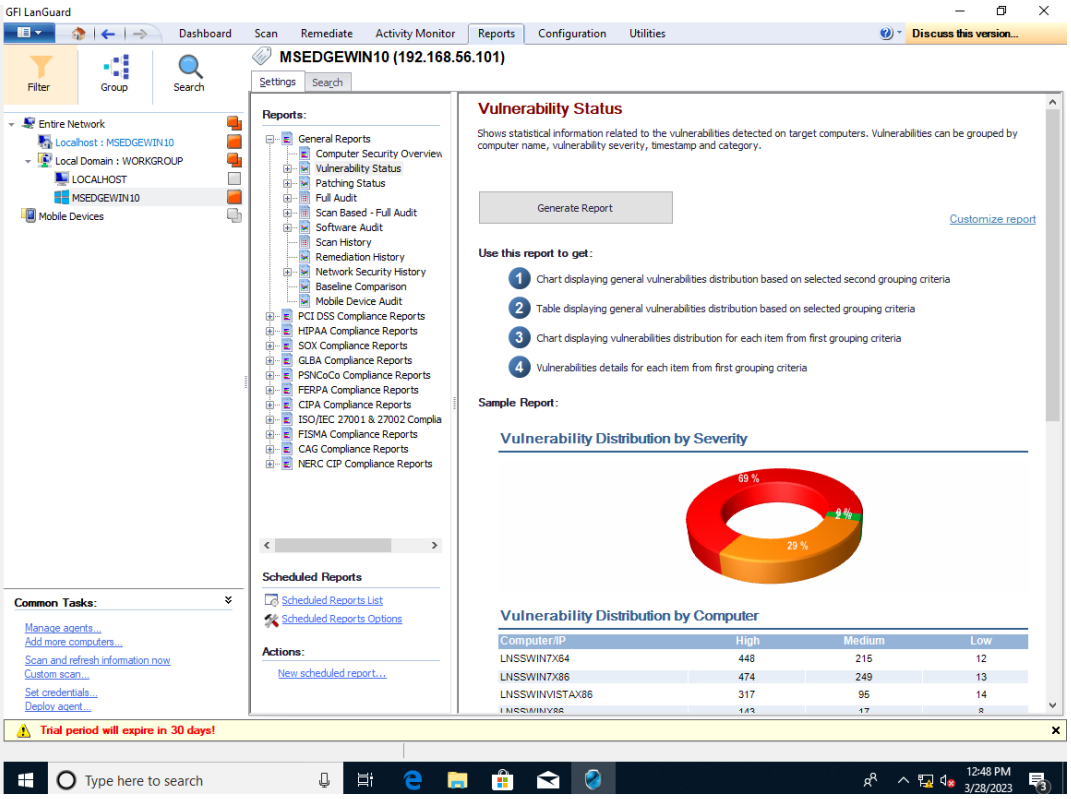
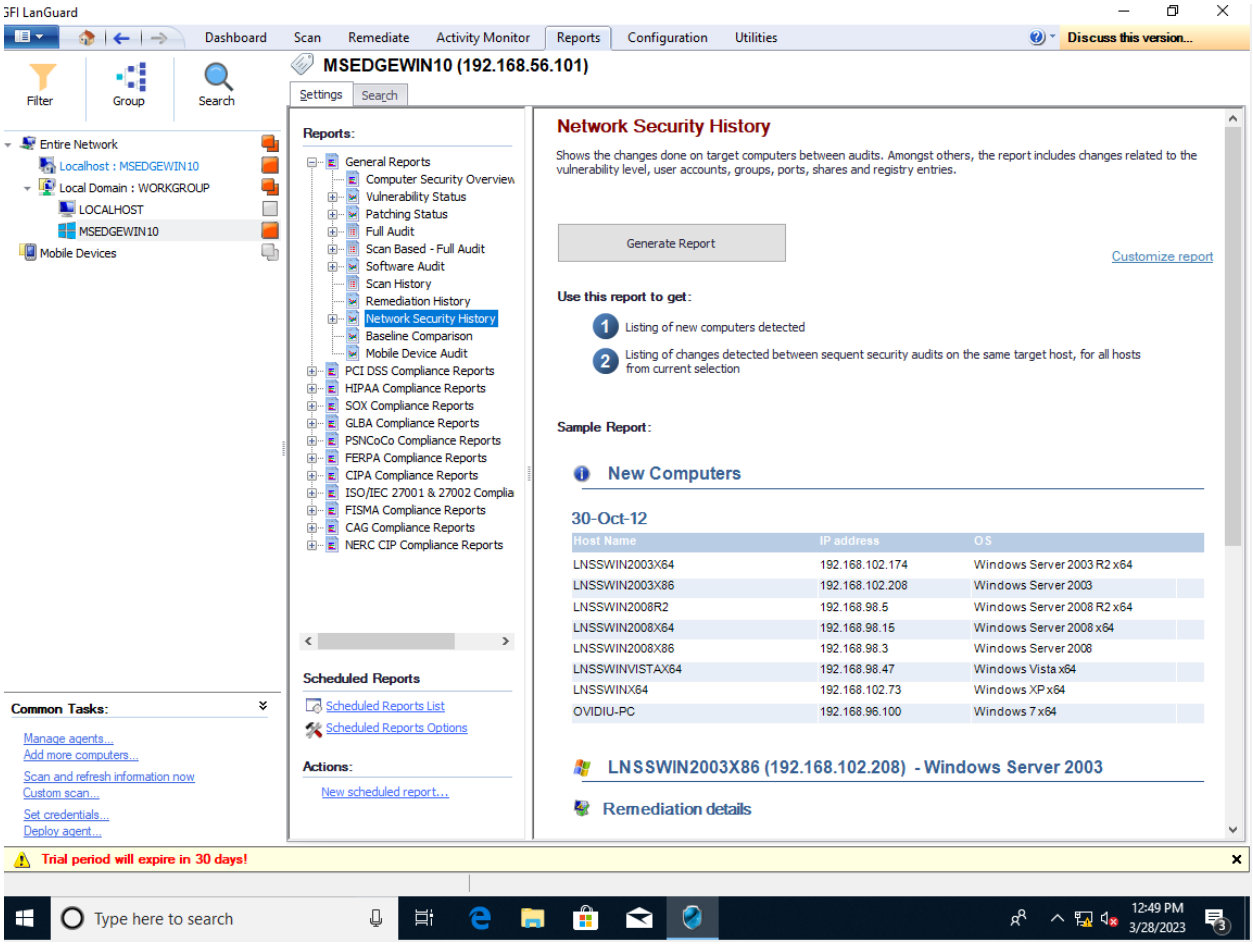
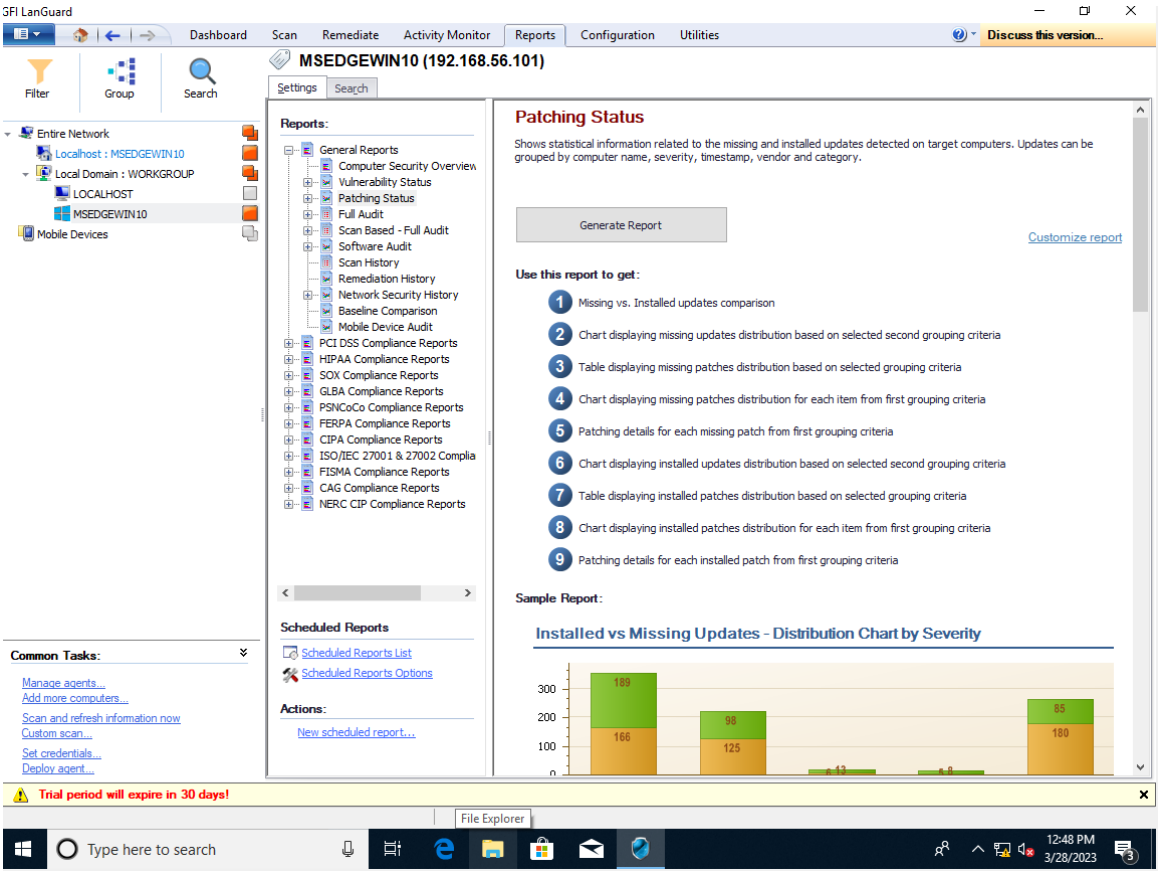


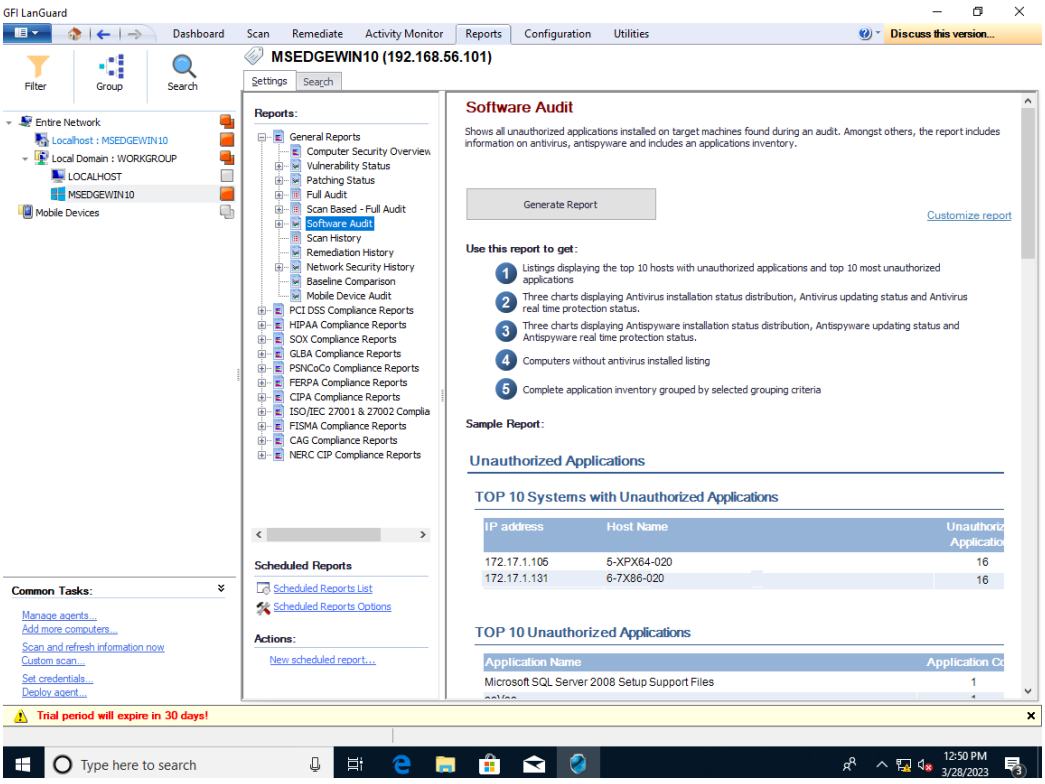
Figure 12. Scan result details

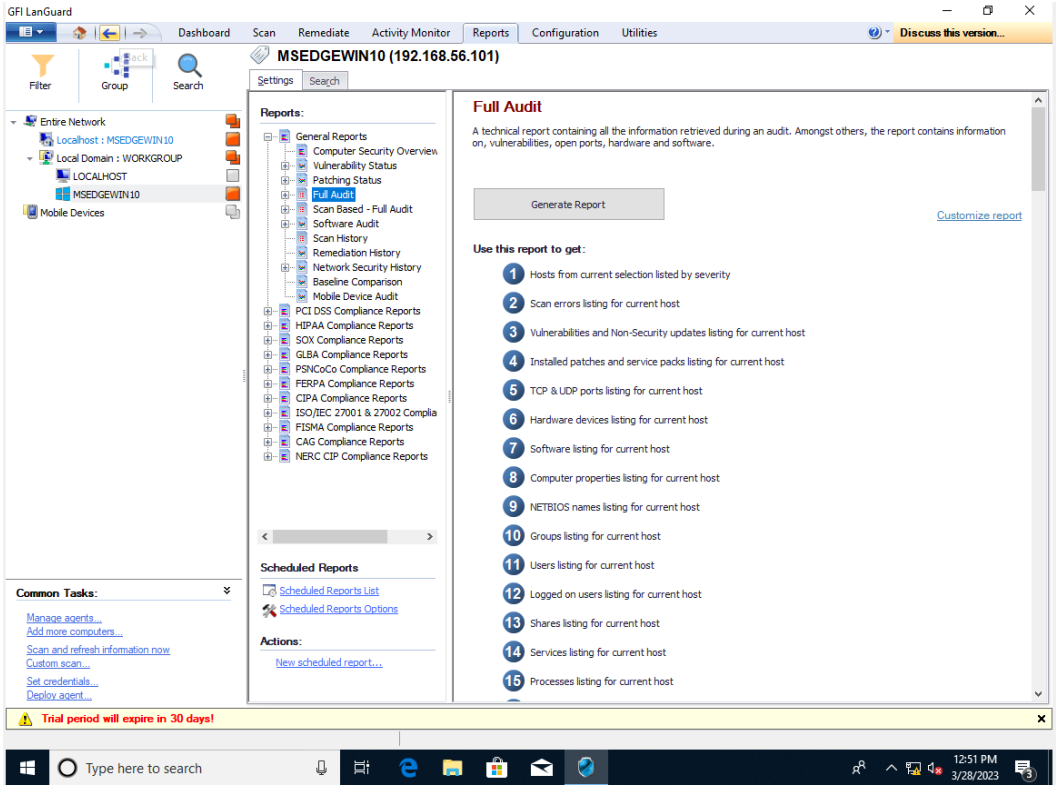
V.



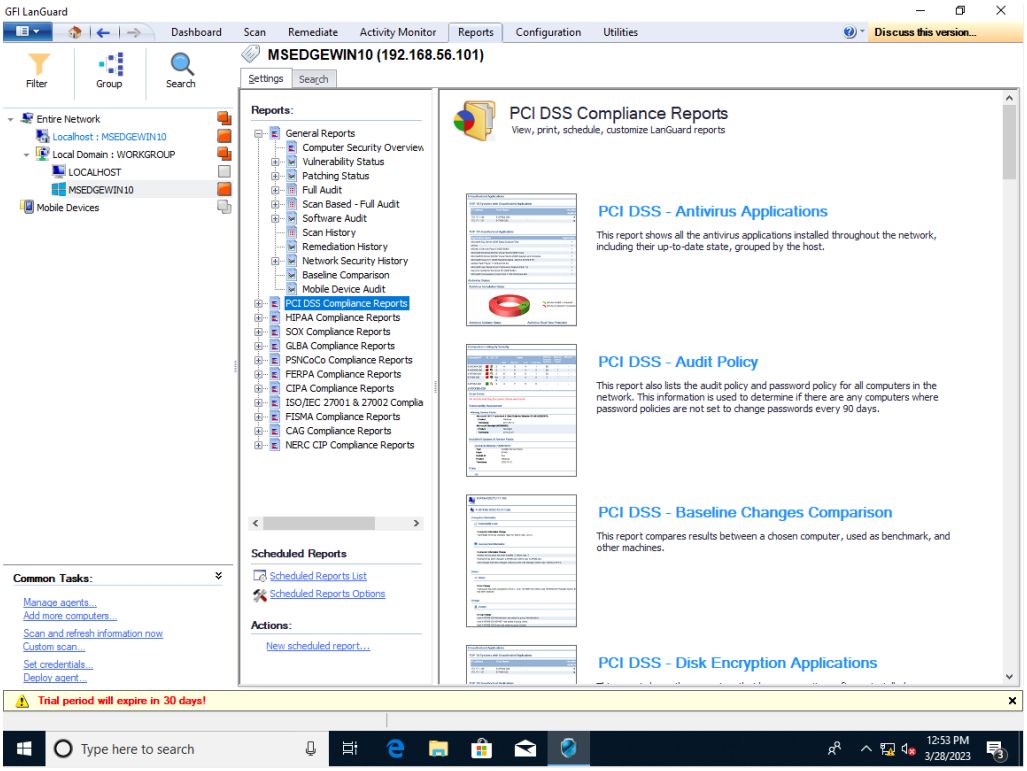

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
MSEDGEWIN10 (192.168.56.101)
Settings
Search
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
Reports:
General Reports
Computer Security Overview
Vulnerability Status
Patching Status
Full Audit
Scan Based - Full Audit
Software Audit
Scan History
Remediation History
Network Security History
Baseline Comparison
Mobile Device Audit
PCI DSS Compliance Reports
HIPAA Compliance Reports
SOX Compliance Reports
GLBA Compliance Reports
PSNCoCo Compliance Reports
FERPA Compliance Reports
CIPA Compliance Reports
ISO/IEC 27001 & 27002 Complia
FISMA Compliance Reports
CAG Compliance Reports
NERC CIP Compliance Reports
Network Security History
Shows the changes done on target computers between audits. Amongst others, the report includes changes related to the vulnerability level, user accounts, groups, ports, shares and registry entries.
Generate Report
Customize report
Use this report to get:
1 Listing of new computers detected
2 Listing of changes detected between sequent security audits on the same target host, for all hosts from current selection
Sample Report:
New Computers
30-Oct-12
Host Name | IP address | OS
LNSSWIN2003X64 | 192.168.102.174 | Windows Server 2003 R2 x64
LNSSWIN2003X86 | 192.168.102.208 | Windows Server 2003
LNSSWIN2008R2 | 192.168.98.5 | Windows Server 2008 R2 x64
LNSSWIN2008X64 | 192.168.98.15 | Windows Server 2008 x64
LNSSWIN2008X86 | 192.168.98.3 | Windows Server 2008
LNSSWINVISTAX64 | 192.168.98.47 | Windows Vista x64
LNSSWINX64 | 192.168.102.73 | Windows XP x64
OVIDIU-PC | 192.168.96.100 | Windows 7 x64
LNSSWIN2003X86 (192.168.102.208) - Windows Server 2003
Remediation details
Scheduled Reports
Scheduled Reports List
Scheduled Reports Options
Actions:
New scheduled report...
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:49 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
MSEDGEWIN10 (192.168.56.101)
Settings
Search
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
Reports:
General Reports
Computer Security Overview
Vulnerability Status
Patching Status
Full Audit
Scan Based - Full Audit
Software Audit
Scan History
Remediation History
Network Security History
Baseline Comparison
Mobile Device Audit
PCI DSS Compliance Reports
HIPAA Compliance Reports
SOX Compliance Reports
GLBA Compliance Reports
PSNCoCo Compliance Reports
FERPA Compliance Reports
CIPA Compliance Reports
ISO/IEC 27001 & 27002 Complia
FISMA Compliance Reports
CAG Compliance Reports
NERC CIP Compliance Reports
Patching Status
Shows statistical information related to the missing and installed updates detected on target computers. Updates can be grouped by computer name, severity, timestamp, vendor and category.
Generate Report
Customize report
Use this report to get:
1 Missing vs. Installed updates comparison
2 Chart displaying missing updates distribution based on selected second grouping criteria
3 Table displaying missing patches distribution based on selected grouping criteria
4 Chart displaying missing patches distribution for each item from first grouping criteria
5 Patching details for each missing patch from first grouping criteria
6 Chart displaying installed updates distribution based on selected second grouping criteria
7 Table displaying installed patches distribution based on selected grouping criteria
8 Chart displaying installed patches distribution for each item from first grouping criteria
9 Patching details for each installed patch from first grouping criteria
Sample Report:
Installed vs Missing Updates - Distribution Chart by Severity
300
200
100
0
189
166
98
125
85
180
Scheduled Reports
Scheduled Reports List
Scheduled Reports Options
Actions:
New scheduled report...
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
File Explorer
Type here to search
12:48 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
MSEDGEWIN10 (192.168.56.101)
Settings
Search
Reports:
Software Audit
Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on antivirus, antispyware and includes an applications inventory.
Generate Report
Customize report
Use this report to get:
1 Listings displaying the top 10 hosts with unauthorized applications and top 10 most unauthorized applications
2 Three charts displaying Antivirus installation status distribution, Antivirus updating status and Antivirus real time protection status.
3 Three charts displaying Antispyware installation status distribution, Antispyware updating status and Antispyware real time protection status.
4 Computers without antivirus installed listing
5 Complete application inventory grouped by selected grouping criteria
Sample Report:
Unauthorized Applications
TOP 10 Systems with Unauthorized Applications
IP address
Host Name
172.17.1.106
5-XPX64-020
16
172.17.1.131
6-7X86-020
16
TOP 10 Unauthorized Applications
Application Name
Microsoft SQL Server 2008 Setup Support Files
1
Trial period will expire in 30 days!
Type here to search
12:50 PM
3/28/2023


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
MSEDGEWIN10 (192.168.56.101)
Settings
Search
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
Reports:
General Reports
Computer Security Overview
Vulnerability Status
Patching Status
Full Audit
Scan Based - Full Audit
Software Audit
Scan History
Remediation History
Network Security History
Baseline Comparison
Mobile Device Audit
PCI DSS Compliance Reports
HIPAA Compliance Reports
SOX Compliance Reports
GLBA Compliance Reports
PSNCoCo Compliance Reports
FERPA Compliance Reports
CIPA Compliance Reports
ISO/IEC 27001 & 27002 Complia
FISMA Compliance Reports
CAG Compliance Reports
NERC CIP Compliance Reports
Full Audit
A technical report containing all the information retrieved during an audit. Amongst others, the report contains information on, vulnerabilities, open ports, hardware and software.
Generate Report
Customize report
Use this report to get:
1 Hosts from current selection listed by severity
2 Scan errors listing for current host
3 Vulnerabilities and Non-Security updates listing for current host
4 Installed patches and service packs listing for current host
5 TCP & UDP ports listing for current host
6 Hardware devices listing for current host
7 Software listing for current host
8 Computer properties listing for current host
9 NETBIOS names listing for current host
10 Groups listing for current host
11 Users listing for current host
12 Logged on users listing for current host
13 Shares listing for current host
14 Services listing for current host
15 Processes listing for current host
Scheduled Reports
Scheduled Reports List
Scheduled Reports Options
Actions:
New scheduled report...
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:51 PM
3/28/2023

VI.


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
MSEDGEWIN10 (192.168.56.101)
Settings
Search
Entire Network
Localhost : MSEDGEWIN10
Local Domain : WORKGROUP
LOCALHOST
MSEDGEWIN10
Mobile Devices
Reports:
General Reports
Computer Security Overview
Vulnerability Status
Patching Status
Full Audit
Scan Based - Full Audit
Software Audit
Scan History
Remediation History
Network Security History
Baseline Comparison
Mobile Device Audit
PCI DSS Compliance Reports
HIPAA Compliance Reports
SOX Compliance Reports
GLBA Compliance Reports
PSNCoCo Compliance Reports
FERPA Compliance Reports
CIPA Compliance Reports
ISO/IEC 27001 & 27002 Complia
FISMA Compliance Reports
CAG Compliance Reports
NERC CIP Compliance Reports
PCI DSS Compliance Reports
View, print, schedule, customize LanGuard reports
PCI DSS - Antivirus Applications
This report shows all the antivirus applications installed throughout the network, including their up-to-date state, grouped by the host.
PCI DSS - Audit Policy
This report also lists the audit policy and password policy for all computers in the network. This information is used to determine if there are any computers where password policies are not set to change passwords every 90 days.
PCI DSS - Baseline Changes Comparison
This report compares results between a chosen computer, used as benchmark, and other machines.
PCI DSS - Disk Encryption Applications
Scheduled Reports
Scheduled Reports List
Scheduled Reports Options
Actions:
New scheduled report...
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...
Trial period will expire in 30 days!
Type here to search
12:53 PM
3/28/2023

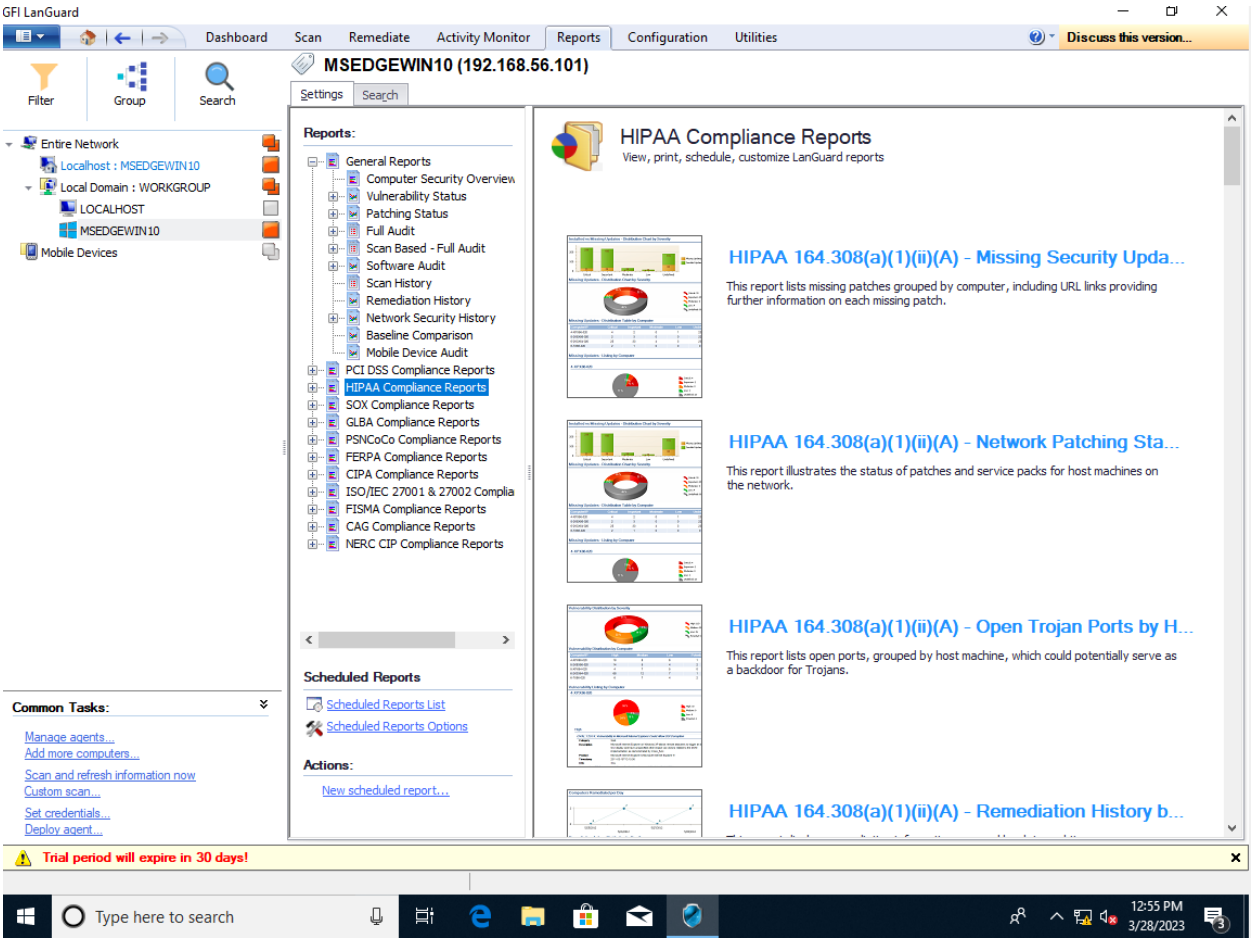


Figure 13-19. Information from Report Tab

Part D: Security Analysis and Security Policy

I.

1. **Unprofessional security guard who doesn't question the potential attackers entering the building.**
2. **No cameras in the elevator lobby.**
3. **No requirements to enter building (i.e. sign in, identification).**
4. **Safe has keypad instead of normal dial combination.**
5. **Employee ID cards did not have sleeves which made it easy to be cloned.**

II.

1. **Employee passwords should not relate to anything on their social medias.**
2. **Employees should not post anything work related that can result in sensitive data loss.**
3. **Employee should not use work devices on public Wi-Fi networks.**

Conclusion:

Throughout this exercise I successfully gained significant experience in conducting security analyses, analyzing the requirements for organization security policies, and conducting vulnerability assessments using GFI Languard's vulnerability scanning software.