Scan Task Vulnerabilities Report

Scan:	BD_quetTT1_sang_040518_1
Submit by:	admin
Generated Time:	Oct. 5, 2018, 1:55 p.m.

Table Of Contents

Scan Task Detailed Information

Information

Scan Task:		BD_quetTT1_sang_040518_1	
Create by:		admin	
Project:	Eximbank System 2018	**Processed:**	No
Start Time:	May 4, 2018, 4:30 a.m.	**Finished Time:**	May 4, 2018, 4:53 a.m.
Created Date:	Sept. 10, 2018, 3:30 a.m.	**Updated Date:**	Sept. 10, 2018, 3:30 a.m.

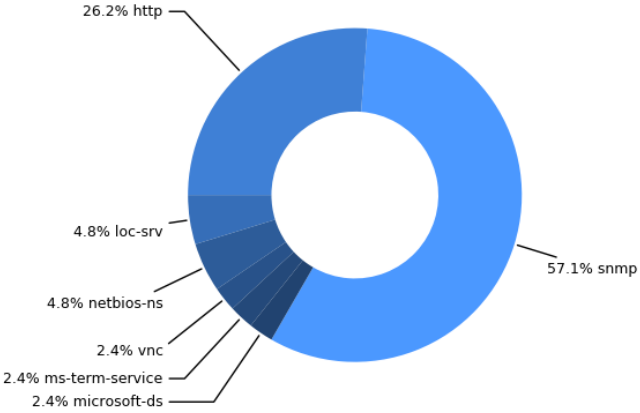
Description:
NA#

Vulnerabilities

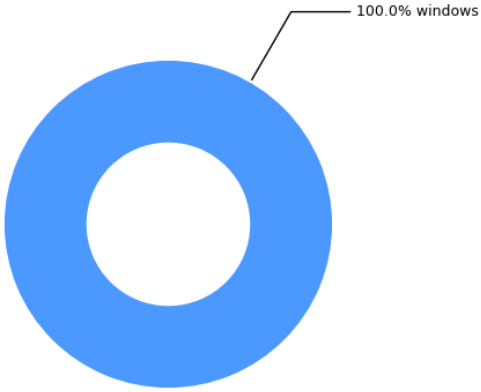
Overview

In this section, this report contains overview information that includes statistics by services (in graph-1), OS (in graph-2) and current categorized vulnerabilities (in graph-3) into groups:

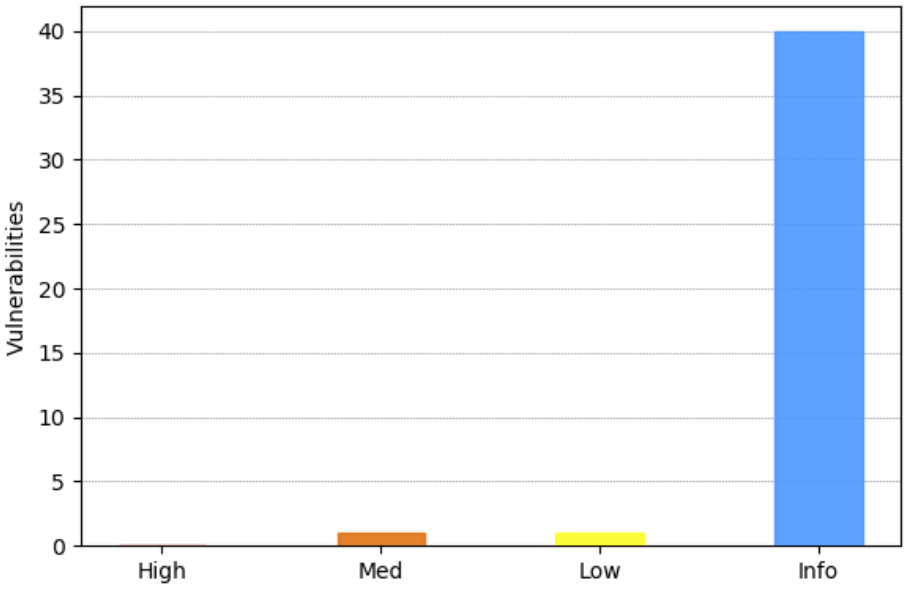
- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g. standard user) to the machine over a remote connection.
- **Low Risk** - The vulnerability discovered on the system provides enticement data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker gaining some form of access to the machine over a remote connection.
- **Informational Risk** - A finding on the system that provides data to an attacker that is of lesser value to an attacker than the enticement data provided by a low risk vulnerability.



Graph 1: Vulnerabilities statistic by services



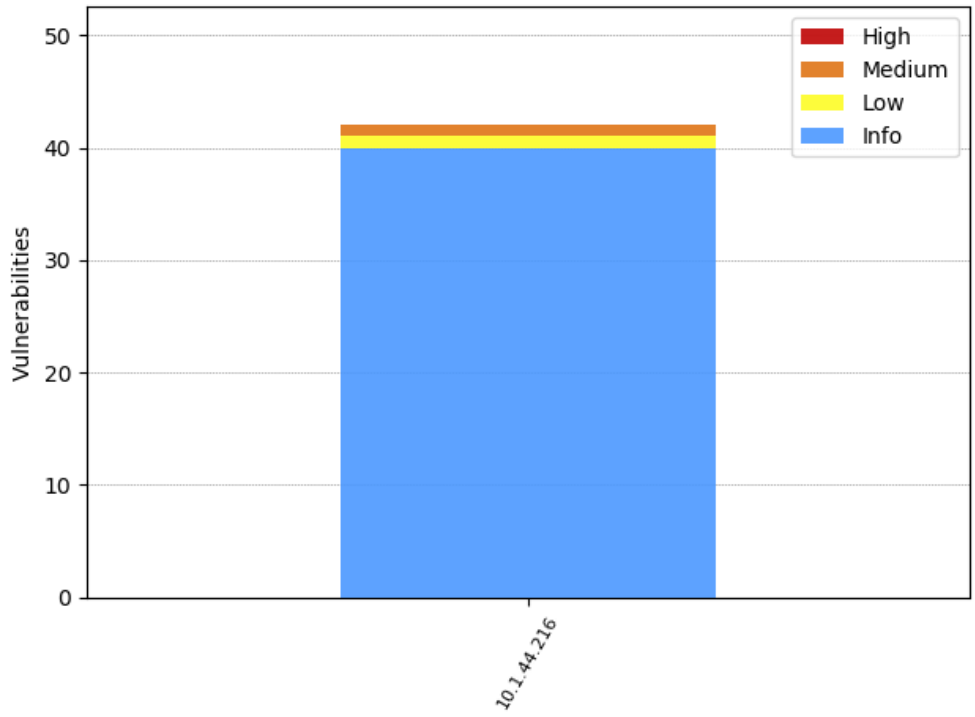
Graph 2: Vulnerabilities statistic by OS



Graph 3: Vulnerabilities statistic

Vulnerabilities in Scan Task

In this section, the report contains scan brief information of vulnerabilities that were discovered by this scan task.



Graph 4: Vulnerabilities of scanned hosts

Scan Result:

Hostname	Ip Address	Vulnerabilities			
		High	Med	Low	Info
WEB-GATEWAY01	10.1.44.216	0	1	1	40

Table 1: Vulnerabilities in Scan Task

Vulnerabilities by Host

In this section, Discovered Vulnerabilities are grouped by host.

WEB-GATEWAY01 - 10.1.44.216

Vulnerabilities	Service	Level Risk
SNMP Default Community Name	snmp	6.0
Microsoft IIS Tilde Character Short File Name Disclosure (142982)	http	3.0
SNMP Printers State Information Detected	snmp	0.0
SNMP IP Routing Table Information	snmp	0.0
SNMP Process Table Information Detected	snmp	0.0
SNMP Network Information Detected	snmp	0.0
SNMP Remote Host General Information	snmp	0.0
Microsoft IIS Anonymous Access Enabled	http	0.0
NetBIOS Names Information Accessible	netbios-ns	0.0
SNMP Established TCP Connection Information Detected	snmp	0.0
SNMP CPU List Information Detected	snmp	0.0
Microsoft ASP.NET HTTP Handlers Enumeration	http	0.0
NetBIOS Bindings Information Detected	netbios-ns	0.0
SNMP Server With SNMPv2 Enabled	snmp	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
SNMP Network Interface List Detected	snmp	0.0
Microsoft ASP.NET State Service Detected	http	0.0
SNMP Remote SMB Shares Information Disclosure	snmp	0.0
SNMP Server With SNMPv1 Enabled	snmp	0.0
LSASS RPC Interface Detected	loc-srv	0.0
SNMP Microsoft Windows Logon Users Detected	snmp	0.0
Microsoft Windows IIS ASP.NET Version Detection	http	0.0
SNMP Active SMB Connections Information Disclosure	snmp	0.0

Vulnerabilities	Service	Level Risk
Microsoft Windows Terminal Service	ms-term-service	0.0
Microsoft IIS Basic Authentication Scheme Disabled	http	0.0
SNMP Storage Devices Detected	snmp	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
SNMP ARP Table Information	snmp	0.0
Microsoft IIS Server Extensions Enumerated	http	0.0
SNMP Partition Table Information Detected	snmp	0.0
Microsoft IIS NTLM Authentication Disabled	http	0.0
SNMP Active TCP Sockets Information Detected	snmp	0.0
SNMP Device List Detected	snmp	0.0
Microsoft IIS Host Name Setting Enumerated	http	0.0
Microsoft IIS Server Detected	http	0.0
SNMP LanManager Service Information Detected	snmp	0.0
VNC Server Detected	vnc	0.0
SNMP Active UDP Sockets Information Detected	snmp	0.0
Installed Software Information Detected Using SNMP	snmp	0.0
SNMP Other NT Domains Information Detected	snmp	0.0
Web Server HTTP Protocol Version Detected	http	0.0
SNMP IP Address Table Information Detected	snmp	0.0

Vulnerabilities In Detail

SNMP Default Community Name

Vulnerbility:		SNMP Default Community Name	
Level Risk:		6.0	
Service:	snmp	**CVE:**	CVE-1999-0472

Observation:

SNMP (Simple Network Management Protocol) is a standard for internetwork management.A SNMP agent is running with a known default community string. Community strings act as passwords that allow user access to the system. Using a known default community string, attackers may gain valuable information about the system and networks. If the community string allows write privileges, the attacker can make modifications to the system.

Recommendation:

Disable the SNMP service, modify the agent to only accept packets from individual, trusted hosts, or change the community string to something else other than a known default. ------ To disable SNMP on Windows 2000/XP/2003:1. Right-click My Computer and select Manage.2. Click Services and Applications, then select Services.3. Locate SNMP on the list of services, then select it and click Stop. 4. Click Startup, and then click Disabled.5. Click OK to close the dialogue. 6. Close the Computer Management window. To modify SNMP on Windows 2000/XP/2003 to only accept packets from individual hosts:1. Right-click My Computer and select Manage.2. Click Services and Applications, then select Services.3. Locate SNMP on the list of services, then double-click to get its properties. 4. Click the Security tab. 5. A community string should exist. 6. Make sure the 'Only Accept SNMP Packets from these hosts' option is selected. On Windows 2003, this is option is labeled 'Accept SNMP Packets from these hosts'. Add hosts as needed, then click Apply.To modify SNMP on Windows NT to only accept packets from individual hosts: 1. Go to Start, Settings, Control Panel then select Network. 2. Click the Services tab and select SNMP Service. 3. Click Properties to display the SNMP Properties dialog box. 4. Click the Security tab. 5. A community string should exist 6. The Only Accept SNMP Packets from These Hosts option is selected 7. Make changes in the Registry if need be.To disable SNMP on Windows NT: Uninstall the SNMP Protocol.For UNIX:Unix systems SNMP services are usually provided by a process called snmpd, which runs continuously. Modifying your system startup scripts should disable it. The read/write community string can be changed by editing /etc/snmp/conf/snmpd.conf. For other platforms running SNMP, consult your vendor on how to disable SNMP default community strings.Reference: Microsoft Knowledge Base Article Q99880 http://support.microsoft.com/default.aspx?scid=kb;en-us;Q99880

Description:

A SNMP community name is set to the default value (e.g. public or private).

Microsoft IIS Tilde Character Short File Name Disclosure (142982)

Vulnerbility:		Microsoft IIS Tilde Character Short File Name Disclosure (142982)	
Level Risk:		3.0	
Service:	http	**CVE:**	-

Observation:
IIS is a web server application and a set of feature extension modules created by Microsoft.There is an information disclosure vulnerability present in some versions of Microsoft IIS. This flaw can be exploited by sending a GET request with a tilde character "~" in the request, it could allow remote attackers to disclose files and folders names based on return status code. The same vulnerability could also cause a denial of service condition.

Recommendation:
McAfee is currently unaware of a vendor-supplied patch or update (2016-11-10) The vendor has released an advisory describing a workaround that can be used to mitigate this issue. More information can be found at: http://support.microsoft.com/kb/121007 http://support.microsoft.com/kb/142982/en-us

Description:
There is an information disclosure vulnerability present in some versions of Microsoft IIS.

SNMP Printers State Information Detected

Vulnerbility:		SNMP Printers State Information Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Printers state information was obtained through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Printers state information was obtained through the Simple Network Management Protocol (SNMP) service.

SNMP IP Routing Table Information

Vulnerbility:		SNMP IP Routing Table Information	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. SNMP IP routing table information was obtained from the SNMP server.

Recommendation:
Ensure that the SNMP server is compliant with policy.

Description:
SNMP IP routing table information was obtained from the SNMP server.

SNMP Process Table Information Detected

Vulnerbility: SNMP Process Table Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Process table information was obtained through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Process table information was obtained through the Simple Network Management Protocol (SNMP) service.

SNMP Network Information Detected

Vulnerbility: SNMP Network Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. Network information was obtained from the host through SNMP service.

Recommendation:
Ensure that SNMP configuration complies with organizational policy.

Description:
Network information was obtained from the host through SNMP service.

SNMP Remote Host General Information

Vulnerbility: SNMP Remote Host General Information
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. General information about the remote host was obtained via SNMP.

Recommendation:
Ensure that the SNMP server on the host is compliant with policy.

Description:
General information about the remote host was obtained via SNMP.

Microsoft IIS Anonymous Access Enabled

Vulnerbility:		Microsoft IIS Anonymous Access Enabled	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS anonymous access is enabled.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy.

Description:
Microsoft Internet Information Services (IIS) anonymous access is enabled.

NetBIOS Names Information Accessible

Vulnerbility:		NetBIOS Names Information Accessible	
Level Risk:		0.0	
Service:	netbios-ns	**CVE:**	-

Observation:
Microsoft NetBIOS is a service developed to communicate with different computers over a local networkMicrosoft NetBIOS names information was detected on the host.

Recommendation:
Ensure that Microsoft NetBIOS complies with organizational policies.

Description:
Microsoft NetBIOS names information was detected on the host.

SNMP Established TCP Connection Information Detected

Vulnerbility:		SNMP Established TCP Connection Information Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Established TCP connection information was obtained from the host through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Established TCP connection information was obtained from the host through the Simple Network Management Protocol (SNMP) service.

SNMP CPU List Information Detected

Vulnerbility: SNMP CPU List Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. CPU information was obtained from the host through SNMP service.

Recommendation:
Ensure that SNMP configuration complies with organizational policy.

Description:
CPU information was obtained from the host through SNMP service.

Microsoft ASP.NET HTTP Handlers Enumeration

Vulnerbility: Microsoft ASP.NET HTTP Handlers Enumeration
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft .NET is a Software Framework for applications designed to run under Microsoft Windows. HTTP handlers in ASP .NET are used for processing different kinds of file types(file extensions). A list of file extensions handled by the ASP.NET server was obtained.

Recommendation:
Ensure that the list of file extension handlers found on the ASP.NET server is allowed by policy.

Description:
A list of file extensions handled by the ASP.NET server was obtained.

NetBIOS Bindings Information Detected

Vulnerbility: NetBIOS Bindings Information Detected
Level Risk: 0.0
Service: netbios-ns **CVE:** -

Observation:
NetBIOS is a service which allows different computers to communicate with each other over a local area network.NetBIOS bindings information was detected on the host.

Recommendation:
Ensure that NetBIOS service complies with organizational policies.

Description:
NetBIOS bindings information was detected on the host.

SNMP Server With SNMPv2 Enabled

Vulnerbility:		SNMP Server With SNMPv2 Enabled	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices. The target host is running an SNMP server with SNMPv2 enabled. SNMPv2 is an insecure protocol.

Recommendation:
Ensure that the SNMP server with SNMPv2 enabled complies with enterprise policyDisable or remove the insecure service if it is not necessary for the business. If running the insecure service is necessary, make sure that the risk posed by use of this protocol is justified, documented and accepted by the organization.

Description:
The target host is running an SNMP server with SNMPv2 enabled.

Microsoft Remote Procedure Call Service Detected

Vulnerbility:		Microsoft Remote Procedure Call Service Detected	
Level Risk:		0.0	
Service:	loc-srv	**CVE:**	-

Observation:
Microsoft Remote Procedure Call Service (MSRPC) service is the DCE RPC mechanism implemented by Microsoft. It supports inheritance of interfaces, Unicode strings and implicit handles. Microsoft Remote Procedure Call Service was detected on the host.

Recommendation:
Ensure that MSRPC complies with organizational policy.

Description:
Microsoft Remote Procedure Call Service was detected on the host.

SNMP Network Interface List Detected

Vulnerbility:		SNMP Network Interface List Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. Network interface list configured on the host was obtained through SNMP.

Recommendation:
Ensure that SNMP configuration complies with organizational policy.

Description:
Network interface list configured on the host was obtained through SNMP.

Microsoft ASP.NET State Service Detected

Vulnerbility:		Microsoft ASP.NET State Service Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
The Microsoft ASP.NET State Service is used to manage session state on computerMicrosoft ASP.NET State Service was detected on the host.

Recommendation:
Ensure that Microsoft ASP.NET State service complies with corporate policy.

Description:
Microsoft ASP.NET State Service was detected on the host.

SNMP Remote SMB Shares Information Disclosure

Vulnerbility:		SNMP Remote SMB Shares Information Disclosure	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. SMB shares information was obtained via SNMP.

Recommendation:
Ensure that SNMP service complies with corporate policy.

Description:
SMB shares information was obtained via SNMP.

SNMP Server With SNMPv1 Enabled

Vulnerbility:		SNMP Server With SNMPv1 Enabled	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices. The target host is running an SNMP server with SNMPv1 enabled. SNMPv1 is an insecure protocol.

Recommendation:
Ensure that the SNMP server with SNMPv1 protocol enabled complies with enterprise policyDisable or remove the insecure service if it is not necessary for the business. If running the insecure service is necessary, make sure that the risk posed by use of this protocol is justified, documented and accepted by the organization.

Description:
The target host is running an SNMP server with SNMPv1 enabled.

LSASS RPC Interface Detected

Vulnerbility:		LSASS RPC Interface Detected	
Level Risk:		0.0	
Service:	loc-srv	**CVE:**	-

Observation:
LSASS RPC Interface Detected.

Recommendation:
It is recommended to block the following ports at the network perimeter: 135/TCP,UDP,137/UDP, 138/TCP,UDP, 139/TCP,UDP 445/TCP,UDP, 593/TCP, 1025/TCP, 1026/TCP.

Description:
LSASS RPC Interface Detected.

SNMP Microsoft Windows Logon Users Detected

Vulnerbility:		SNMP Microsoft Windows Logon Users Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Microsoft Windows users information was obtained through the SNMP service.

Recommendation:
Ensure that SNMP configuration complies with organizational policy.

Description:
Microsoft Windows users information was obtained through the Simple Network Management Protocol (SNMP) service.

Microsoft Windows IIS ASP.NET Version Detection

Vulnerbility:		Microsoft Windows IIS ASP.NET Version Detection	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft IIS ASP.NET is a software service for applications designed to run under Microsoft Windows. The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

Recommendation:
Ensure that the ASP.NET service is allowed to be running on the host.

Description:
The server is running the Microsoft Windows IIS ASP.NET service, and the version information was obtained.

SNMP Active SMB Connections Information Disclosure

Vulnerbility: SNMP Active SMB Connections Information Disclosure
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. Active SMB connection information was obtained via SNMP.

Recommendation:
Ensure that SNMP service complies with corporate policy.

Description:
Active SMB connection information was obtained via SNMP.

Microsoft Windows Terminal Service

Vulnerbility: Microsoft Windows Terminal Service
Level Risk: 0.0
Service: ms-term-service **CVE:** CVE-MAP-NOMATCH

Observation:
Terminal Services allows the remote, full-access administration of any server running Microsoft Windows. This service is optional, and can be disabled at any time. If an attacker gains a valid username and password, he can use this service to gain further access on the remote host. Windows XP uses Terminal Services to provide additional functionality such as Fast User Switch, and Remote Assistance. Vulnerable Systems: Microsoft Windows 2000, NT, XP, 2003

Recommendation:
Disable Terminal Services if not in use. Ensure that account policies for Terminal Server users is as restrictive as possible.To disable Terminal Services: For Windows 2000 and NT1. Click Start > Settings > Control Panel. 2. Double click Add/Remove programs. 3. In the Add/Remove programs window, click Add/Remove Windows Components. 4. Scroll down and click Terminal Services. Then click Next twice to remove it.

Description:
Microsoft Windows Terminal service has been detected on the target host.

Microsoft IIS Basic Authentication Scheme Disabled

Vulnerbility: Microsoft IIS Basic Authentication Scheme Disabled
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS Basic Authentication scheme is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy.

Description:
Microsoft Internet Information Services (IIS) Basic Authentication scheme is disabled on the host.

SNMP Storage Devices Detected

Vulnerbility:		SNMP Storage Devices Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Information about available storage devices on the host was obtained through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Information about available storage devices on the host was obtained through the Simple Network Management Protocol (SNMP) service.

NetBIOS Null Session Enabled

Vulnerbility:		NetBIOS Null Session Enabled	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
A NetBIOS null session allows users to connect to a host remotely with no username and password and perform a limited set of administrative tasks. Null sessions allow the remote user to gather information such as: 1. List users 2. List groups 3. List shares (including hidden shares) 4. Policies (such as minimum password length, etc.) While the enumerated information is not an immediate risk, much of the information can be leveraged to launch an attack to gain user or administrative privilege. All steps should be taken to eliminate the vulnerability and/or reduce the information available to the attacker. This check only attempts to establish a NetBIOS null session with the host. It does not attempt to determine what information is accessible with the null session.

Recommendation:
Disable or restrict null session access to network shares. For Windows operating systems, the configuration steps may vary based on the type of operating system and Domain or Local Security policies. Contact the operating system vendor for hardening steps specific to the operating system and setup environment. For Unix Samba based server, make sure that samba's configuration parameter "guest ok" is set to "no" and set the "restrict anonymous" parameter. Workaround: Block access to TCP port 139 (NetBIOS) and TCP port 445 using a firewallNote: Blocking access for MVM to both TCP ports 139 and 445 will also block MVM's credential based scans. This should only be done if credential based scans are not needed.

Description:
NetBIOS Null sessions are enabled on the host.

SNMP ARP Table Information

Vulnerbility: SNMP ARP Table Information
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. ARP table information was obtained from the SNMP server.

Recommendation:
Ensure that the SNMP server is compliant with policy.

Description:
ARP table information was obtained from the SNMP server.

Microsoft IIS Server Extensions Enumerated

Vulnerbility: Microsoft IIS Server Extensions Enumerated
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS server extensions were enumerated on the host.

Recommendation:
Ensure that Microsoft IIS complies with organizational policy.

Description:
Microsoft Internet Information Services (IIS) extensions were enumerated on the host.

SNMP Partition Table Information Detected

Vulnerbility: SNMP Partition Table Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Partition table information was obtained through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Partition table information was obtained through the Simple Network Management Protocol (SNMP) service.

Microsoft IIS NTLM Authentication Disabled

Vulnerbility: Microsoft IIS NTLM Authentication Disabled
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS NTLM Authentication is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enforce NTLM authentication for Microsoft IIS.

Description:
Microsoft Internet Information Services (IIS) NTLM Authentication is disabled on the host.

SNMP Active TCP Sockets Information Detected

Vulnerbility: SNMP Active TCP Sockets Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Active TCP sockets information was obtained from the host through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Active TCP sockets information was obtained from the host through the Simple Network Management Protocol (SNMP) service.

SNMP Device List Detected

Vulnerbility: SNMP Device List Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Information about available server devices on the host was obtained through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Information about available server devices on the host was obtained through the Simple Network Management Protocol (SNMP) service.

Microsoft IIS Host Name Setting Enumerated

Vulnerbility:		Microsoft IIS Host Name Setting Enumerated	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS "Use Host Header Name" setting is disabled on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: It is advised to enable "Use Host Header Name" setting.

Description:
Microsoft Internet Information Services (IIS) "Use Host Header Name" setting is disabled on the host.

Microsoft IIS Server Detected

Vulnerbility:		Microsoft IIS Server Detected	
Level Risk:		0.0	
Service:	http	**CVE:**	-

Observation:
Microsoft Internet Information Services (IIS) is a popular web server for the Windows platformMicrosoft IIS was detected on the host.

Recommendation:
Ensure that Microsoft IIS complies with the corporate policy. Note: Conceal the IIS Server status by modifying the banner.

Description:
Microsoft Internet Information Services (IIS) was detected on the host.

SNMP LanManager Service Information Detected

Vulnerbility:		SNMP LanManager Service Information Detected	
Level Risk:		0.0	
Service:	snmp	**CVE:**	-

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. LAN Manager service table information was obtained from the host through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
LAN Manager service table information was obtained from the host through the Simple Network Management Protocol (SNMP) service.

VNC Server Detected

Vulnerbility: VNC Server Detected
Level Risk: 0.0
Service: vnc **CVE:** CVE-MAP-NOMATCH

Observation:
An open VNC connection will allow an attacker to obtain sensitive information about the host and possibly gain access to the system.

Recommendation:
A VNC Server application was detected. The affected system should be examined to determine which VNC application is installed. Once determined, it should be removed unless being used for legitimate business purposes. To uninstall VNC for Windows NT/2000/XP: ----- To uninstall using the Add/Remove Programs control panel: 1. Go to the Start menu, select Settings and then Control Panel. 2. Double-click the Add/Remove Programs icon. 3. Select VNC. 4. Click the Add/Remove button.

Description:
A VNC server has been detected on the host.

SNMP Active UDP Sockets Information Detected

Vulnerbility: SNMP Active UDP Sockets Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. Active UDP socket information was obtained from the host through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
Active UDP socket information was obtained from the host through the Simple Network Management Protocol (SNMP) service.

Installed Software Information Detected Using SNMP

Vulnerbility: Installed Software Information Detected Using SNMP
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. Installed software information was detected on the host via SNMP.

Recommendation:
Ensure that SNMP service complies with corporate policy.

Description:
Installed software information was detected on the host via SNMP.

SNMP Other NT Domains Information Detected

Vulnerbility: SNMP Other NT Domains Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP based network protocol. SNMP is used to remotely monitor and administer devices with a network interface. NT Domain information was obtained from the host through the SNMP service.

Recommendation:
Ensure that SNMP configuration complies with organizational policy.

Description:
NT Domain information was obtained from the host through the SNMP service.

Web Server HTTP Protocol Version Detected

Vulnerbility: Web Server HTTP Protocol Version Detected
Level Risk: 0.0
Service: http **CVE:** -

Observation:
Web servers are widely used to serve static and dynamic content and render it in the client's browser. HTTP protocol version was obtained from the host through web server.

Recommendation:
Ensure that web server complies with organizational policy.

Description:
HTTP protocol version was obtained from the host through web server.

SNMP IP Address Table Information Detected

Vulnerbility: SNMP IP Address Table Information Detected
Level Risk: 0.0
Service: snmp **CVE:** -

Observation:
Simple Network Management Protocol (SNMP) is a UDP-based network protocol. SNMP is used to monitor and administer devices with a network interface remotely. IP address table information was obtained from the host through the SNMP service.

Recommendation:
Ensure that the SNMP configuration complies with organizational policy.

Description:
IP address table information was obtained from the host through the Simple Network Management Protocol (SNMP) service.