Scan Task Vulnerabilities Report

Scan:	BD_quetTT1_sang_090518_1
Submit by:	admin
Generated Time:	Oct. 2, 2018, 2:28 p.m.

Table Of Contents

Scan Task Detailed Information

Information

Scan Task:		BD_quetTT1_sang_090518_1	
Create by:		admin	
Project:	Eximbank System 2018	**Processed:**	No
Start Time:	May 9, 2018, 4:41 a.m.	**Finished Time:**	May 9, 2018, 5:01 a.m.
Created Date:	Sept. 10, 2018, 3:31 a.m.	**Updated Date:**	Sept. 10, 2018, 3:31 a.m.

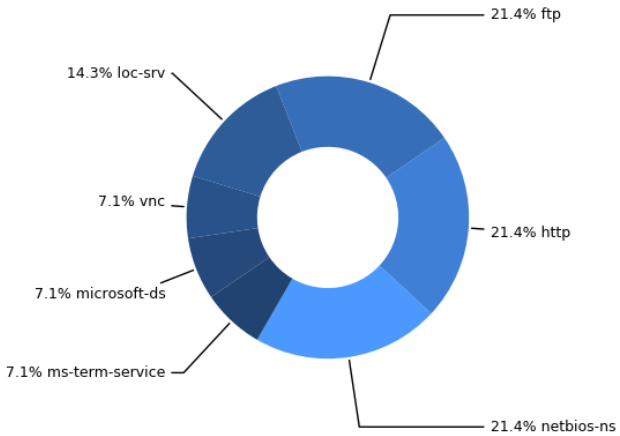
Description:
NA#

Vulnerabilities

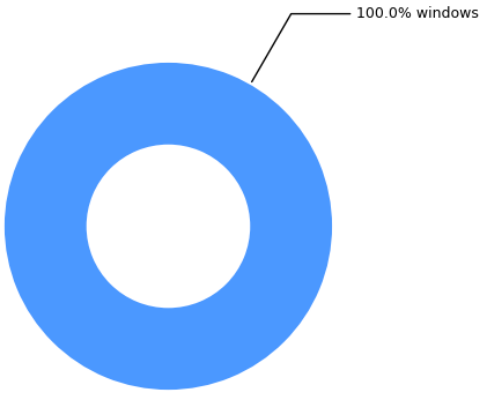
Overview

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:

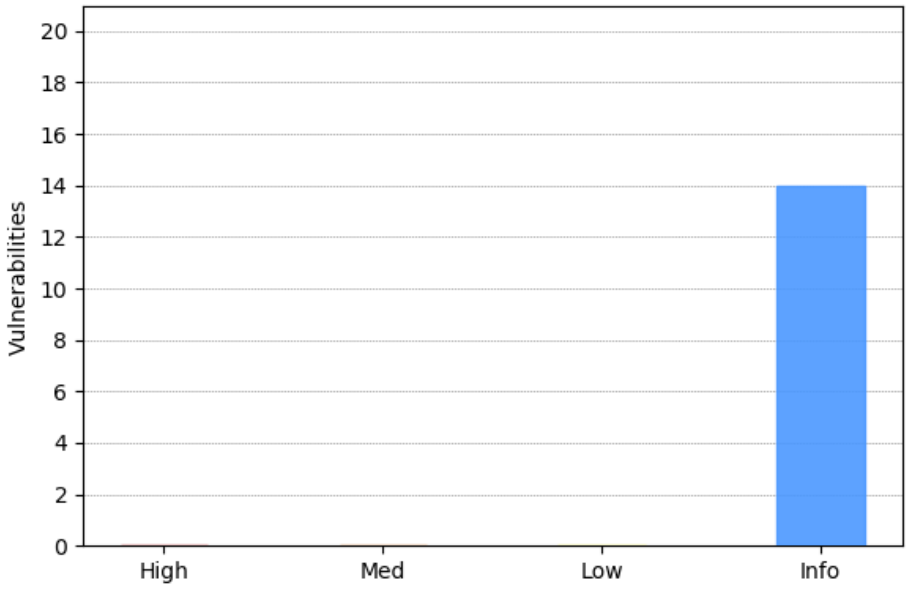
- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining 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



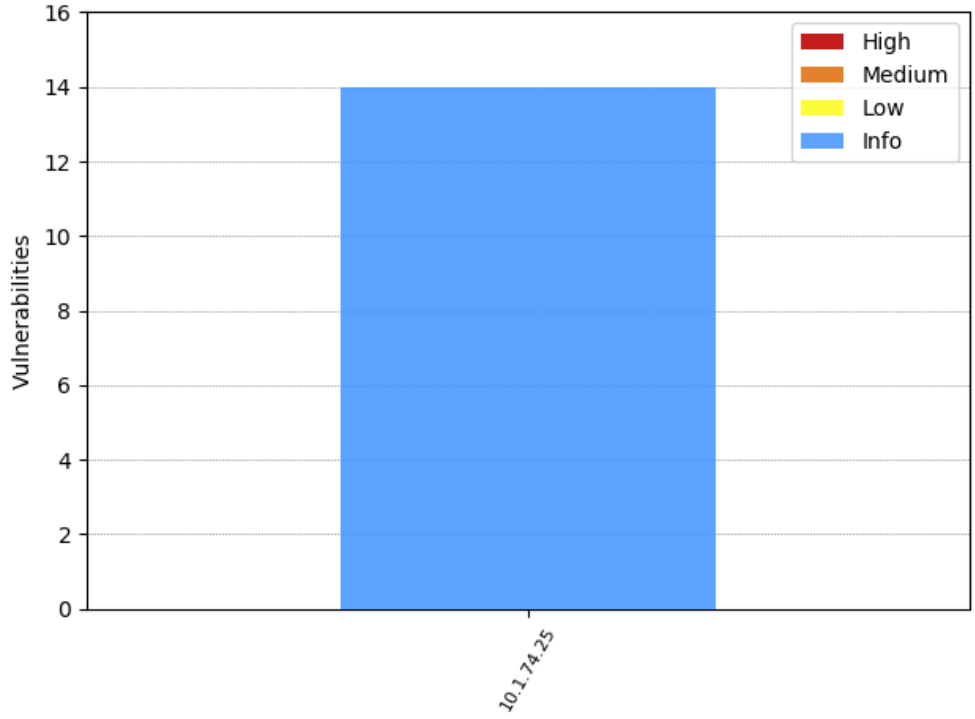
Graph 2: Vulnerabilities statistic by OS



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
SERVER-BFNNH0D5	10.1.74.25	0	0	0	14

Table 1: Vulnerabilities in Scan Task

Vulnerabilities by Host

In this section, Discovered Vulnerabilities are grouped by host.

SERVER-BFNNH0D5 - 10.1.74.25

Vulnerabilities	Service	Level Risk
NetBIOS Names Information Accessible	netbios-ns	0.0
Hidden WWW Server Name Detected	http	0.0
LSASS RPC Interface Detected	loc-srv	0.0
NetBIOS Bindings Information Detected	netbios-ns	0.0
FTP Server Detected	ftp	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0
FTP Server With Clear Text Authentication Detected	ftp	0.0
VNC Server Detected	vnc	0.0
FTP Server Found	ftp	0.0
VNC HTTP Console	http	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
Web Server HTTP Protocol Version Detected	http	0.0
NetBIOS NBTSTAT -A	netbios-ns	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0

Vulnerabilities In Detail

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.

Hidden WWW Server Name Detected

Vulnerbility: Hidden WWW Server Name Detected
Level Risk: 0.0
Service: http **CVE:** -

Observation:
WWW server is a computer application for delivering web based contents using HTTPHidden WWW server name detected. Web server name can be hidden as a security measure.

Recommendation:
Ensure that web server complies with corporate policy.

Description:
Hidden WWW server name detected.

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.

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.

FTP Server Detected

Vulnerbility: FTP Server Detected
Level Risk: 0.0
Service: ftp **CVE:** -

Observation:
A FTP server is used for transferring files to and from remote systems connected in a network. A FTP server was detected on the host.

Recommendation:
Ensure that the FTP server complies with organizational policy.

Description:
A FTP server was detected on the host.

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.

FTP Server With Clear Text Authentication Detected

Vulnerbility: FTP Server With Clear Text Authentication Detected
Level Risk: 0.0
Service: ftp **CVE:** -

Observation:
A FTP server is used for transferring files to and from remote systems connected in a network.FTP server with clear text authentication was detected on the host.

Recommendation:
Ensure that the FTP server complies with organizational policy.

Description:
FTP server with clear text authentication was detected on the host.

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.

FTP Server Found

Vulnerbility: FTP Server Found
Level Risk: 0.0
Service: ftp **CVE:** -

Observation:
The File Transfer Protocol (FTP) is a protocol used for transferring files over an Internet Protocol (IP) network. An FTP server was detected on the host.

Recommendation:
Verify that the FTP server's configuration complies with corporate policy.

Description:
An FTP server was detected on the host.

VNC HTTP Console

Vulnerbility:		VNC HTTP Console	
Level Risk:		0.0	
Service:	http	**CVE:**	CVE-MAP-NOMATCH

Observation:
The Virtual Network Computing (VNC) software package allows for a user to remotely access a graphical desktop environment. The VNC package includes functionality that allows for a user to gain remote console access by connecting a Java enabled web browser to a VNC HTTP serverPerforming an HTTP GET for the root directory returned one or more files that are part of the VNC HTTP remote console package. For more information see: VNC http://www.uk.research.att.com/vnc/

Recommendation:
If VNC is not required on the server, it is highly recommended to remove all of its files.To do so, follow the instructions below: Removing VNC ----- For Microsoft Windows:1. Go to start, settings, and then control panel. 2. Then click on Add/Remove programs. 3. In there, you should see VNC Server. 4. Uninstall VNC Server.

Description:
A VNC HTTP remote desktop console was detected.

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.

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.

NetBIOS NBTSTAT -A

Vulnerbility: NetBIOS NBTSTAT -A
Level Risk: 0.0
Service: netbios-ns **CVE:** CVE-MAP-NOMATCH

Observation:
All Microsoft Windows platforms include support for the NetBIOS network protocol stack. The NetBIOS protocol provides the underlying support for Microsoft Windows file and resource sharing. One component of all Microsoft Windows NetBIOS implementations is the NetBIOS Name Service. The NetBIOS Name Service listens for name service requests on UDP port 137. It can be queried to retrieve a listing of currently logged in user accounts and groups. In addition, the MAC address for the network interface over which the query is performed is included in the response to a nbtstat -A request. The DOS nbtstat command can be used to perform this operation. To do so, open a DOS command prompt and run the following command: nbtstat -A target_system Where target_system is the IP address or hostname of the target system.

Recommendation:
Disable the NetBIOS Name Service to prevent access to NBTSTAT -A information. Workaround: Block access to UDP port 137 using a firewall. Contact the operating system vendor for hardening steps specific to the operating system.

Description:
It is possible to retrieve NetBIOS Name Service information.

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.