Scan Task Vulnerabilities Report

Scan:	BD_quetTT1_sang_080518_1
Submit by:	admin
Generated Time:	Oct. 2, 2018, 1:50 p.m.

Table Of Contents

Scan Task Detailed Information

Information

Scan Task:		BD_quetTT1_sang_080518_1	
Create by:		admin	
Project:	Eximbank System 2018	**Processed:**	No
Start Time:	May 8, 2018, 4:30 a.m.	**Finished Time:**	May 8, 2018, 4:58 a.m.
Created Date:	Sept. 10, 2018, 3:31 a.m.	**Updated Date:**	Sept. 10, 2018, 3:31 a.m.

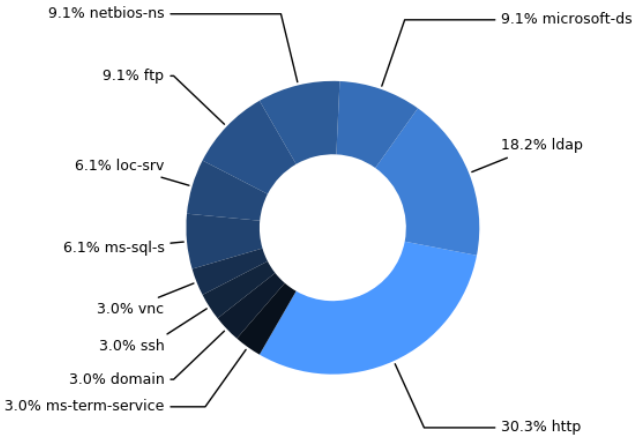
Description:
NA#

Vulnerabilities

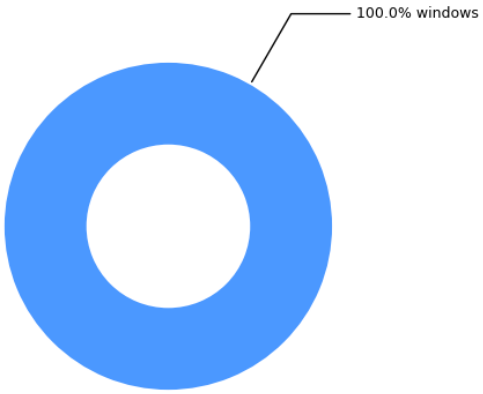
Overview

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:

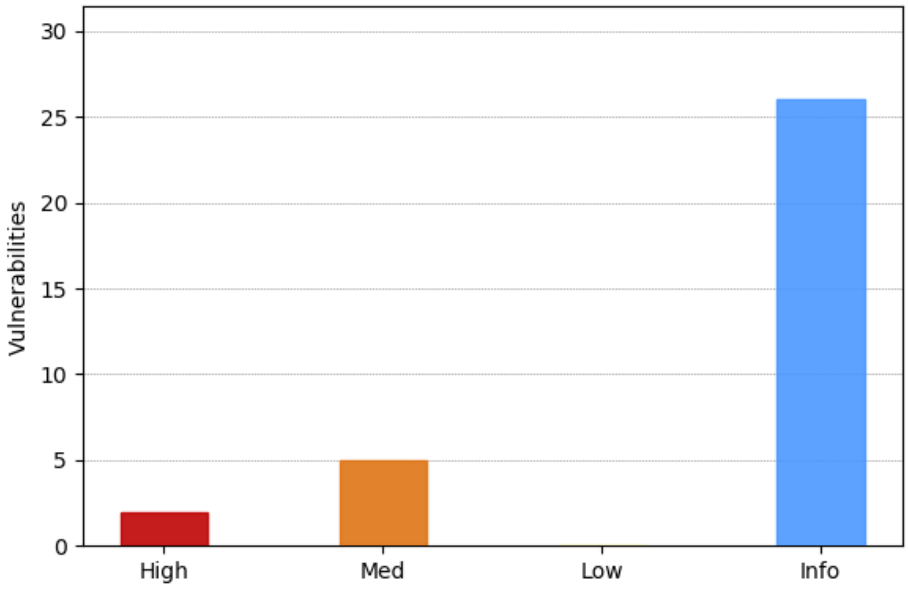
- **High Risk** - Exploitation of the vulnerability discovered on the system can directly lead to an attacker gaining privileged access (e.g. administrator, root) to the machine over a remote connection.
- **Medium Risk** - The vulnerability discovered on the system can directly lead to an attacker gaining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



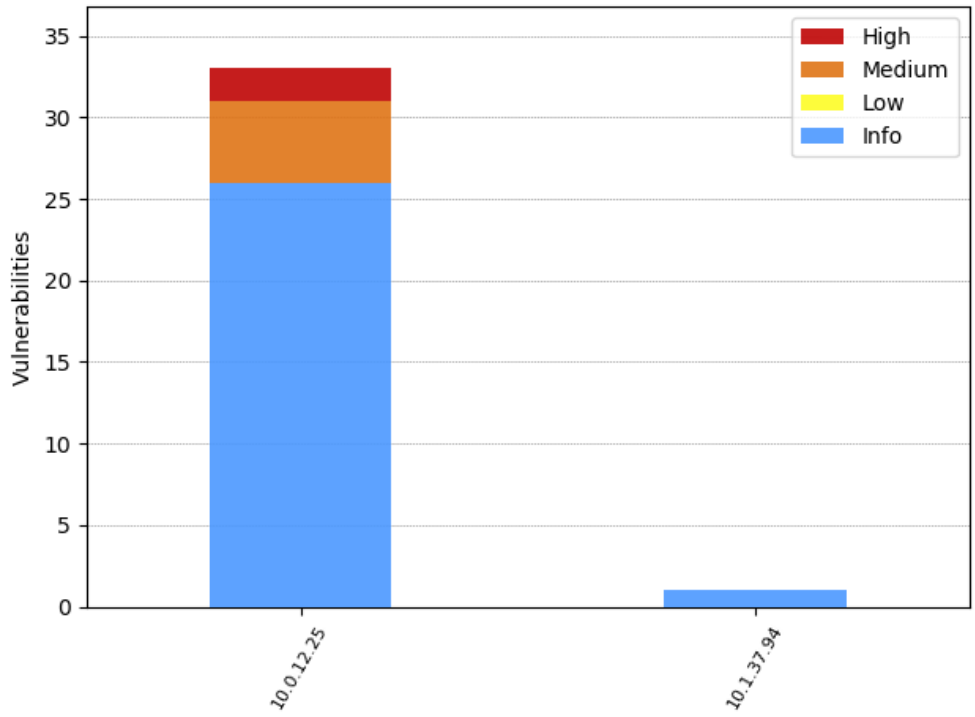
Graph 2: Vulnerabilities statistic by OS



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
WIM-01	10.0.12.25	2	5	0	26
[Unknown]	10.1.37.94	0	0	0	1

Table 1: Vulnerabilities in Scan Task

Vulnerabilities by Host

In this section, Discovered Vulnerabilities are grouped by host.

[Unknown] - 10.1.37.94

Vulnerabilities	Service	Level Risk
SSH Protocol Supported Versions Detected	ssh	0.0

WIM-01 - 10.0.12.25

Vulnerabilities	Service	Level Risk
JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Remote Code Execution	http	10.0
JBoss Administrative Console Security Bypass Vulnerability	http	8.0
SMB User Enumeration By Host/Domain SID	microsoft-ds	5.0
Red Hat JBoss Enterprise Application Platform Web Console Security Bypass Vulnerability I	http	5.0
JBoss JMX Console Unrestricted Access Vulnerability	http	5.0
JBoss Enterprise Application Platform Status Servlet Request Information Disclosure Vulnerability	http	4.0
JBoss Web Console Cross-Site Scripting Vulnerability (CVE-2009-2405)	http	4.0
FTP Server Found	ftp	0.0
NetBIOS Bindings Information Detected	netbios-ns	0.0
Microsoft SQL Server Authentication Mode	ms-sql-s	0.0
NetBIOS Null Session Enabled	microsoft-ds	0.0
FTP Server Detected	ftp	0.0
LDAP Server Detected	ldap	0.0
Microsoft IIS Server Detected	http	0.0
FTP Server With Clear Text Authentication Detected	ftp	0.0
SSH Protocol Supported Versions Detected	ssh	0.0
Web Server HTTP Protocol Version Detected	http	0.0
LDAP Crafted Search Request Access Allowed	ldap	0.0

Vulnerabilities	Service	Level Risk
Microsoft Windows Domain Or Workgroup Detection	microsoft-ds	0.0
LSASS RPC Interface Detected	loc-srv	0.0
LDAP Service Detected	ldap	0.0
Microsoft Remote Procedure Call Service Detected	loc-srv	0.0
LDAP Server NULL Bind Connection Allowed	ldap	0.0
Microsoft Windows Terminal Service	ms-term-service	0.0
LDAP NULL Base Search Access Allowed	ldap	0.0
Microsoft SQL TCP Listener Detected	ms-sql-s	0.0
Hidden WWW Server Name Detected	http	0.0
Microsoft Windows Active Directory Domain Controller Detected	ldap	0.0
NetBIOS NBTSTAT -A	netbios-ns	0.0
VNC Server Detected	vnc	0.0
NetBIOS Names Information Accessible	netbios-ns	0.0
VNC HTTP Console	http	0.0
DNS Server Detected	domain	0.0

Vulnerabilities In Detail

JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Remote Code Execution

Vulnerbility:		JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Remote Code Execution	
Level Risk:		10.0	
Service:	http	**CVE:**	CVE-2012-0874

Observation:

JBoss is an application server developed by Red Hat. A remote code execution vulnerability is present in some versions of JBoss. The flaw is due to how certain HTTP requests containing marshalled Java objects are handled. Successful exploitation by a remote attacker could result in the execution of arbitrary code. Note that the vulnerability also lies in some products which are internally using JBoss .

Recommendation:

The vendor has released advisories to address this issue: http://rhn.redhat.com/errata/RHSA-2013-0191.html http://rhn.redhat.com/errata/RHSA-2013-0192.html http://rhn.redhat.com/errata/RHSA-2013-0193.html http://rhn.redhat.com/errata/RHSA-2013-0194.html http://rhn.redhat.com/errata/RHSA-2013-0195.html http://rhn.redhat.com/errata/RHSA-2013-0196.html http://rhn.redhat.com/errata/RHSA-2013-0197.html http://rhn.redhat.com/errata/RHSA-2013-0198.html

Description:

A remote code execution vulnerability is present in some versions of JBoss.

JBoss Administrative Console Security Bypass Vulnerability

Vulnerbility:		JBoss Administrative Console Security Bypass Vulnerability	
Level Risk:		8.0	
Service:	http	**CVE:**	CVE-2007-1036

Observation:

JBoss is an open source application server. The default install of JBoss does not restrict access to the administrative console, which allows attackers to bypass authentication and access to the administrative interface.

Recommendation:

Enabling role based security or Restricting access to the administrative interface may mitigate this vulnerability. http://www.jboss.org/community/wiki/SecureJBoss http://www.jboss.org/community/wiki/securethejmxconsole http://www.jboss.org/community/wiki/LimitAccessToCertainClients

Description:

The JBoss Application Server may allow unauthenticated access to the administrative interface.

SMB User Enumeration By Host/Domain SID

Vulnerbility:		SMB User Enumeration By Host/Domain SID	
Level Risk:		5.0	
Service:	microsoft-ds	**CVE:**	CVE-2000-1200

Observation:

The SMB protocol is Windows core network protocol.On some systems, it is possible to create a unauthenticated SMB session. It is possible to get the host or domain Security Identifier (SID) and enumerate local users by SID via the SMB null session. While the enumerated information is not an immediate risk, much of the information can be leveraged to launch further attacks against the target system. The check enumerates only users with a Relative ID (RID) from 1000 to 1004.

Recommendation:

The following policies can be found in local group policy editor. In order to completely disable anonymous logons, you need to disable policy 1 and 4, to enable policy 2 and 3, and to specify empty lists for policy 5 and 6. 1 . Network access: Allow anonymous SID/Name translation2 . Network access: Do not allow anonymous enumeration of SAM accounts3 . Network access: Do not allow anonymous enumeration of SAM accounts and shares4. Network access: Let Everyone permissions apply to anonymous users 5. Network access: Named Pipes that can be accessed anonymously6. Network access: Shares that can be accessed anonymously

Description:

It is possible to enumerate user accounts for the target system by host/domain SID.

Red Hat JBoss Enterprise Application Platform Web Console Security Bypass Vulnerability I

Vulnerbility:		Red Hat JBoss Enterprise Application Platform Web Console Security Bypass Vulnerability I	
Level Risk:		5.0	
Service:	http	**CVE:**	CVE-2010-1428

Observation:

Red Hat JBoss Enterprise Application Platform is an open source Java applications platformA security bypass vulnerability is present in some versions of Red Hat JBoss Enterprise Application Platform. The flaw occurs due to JBoss improper check HTTP method when it received a crafted HTTP request. Successful exploitation could allow an attacker to bypass the security restriction.

Recommendation:

Download the latest version of Red Hat JBoss Enterprise Application Platform from the following location: http://www.jboss.com/ For users of JBoss Community project, download the latest version from the following location: http://www.jboss.org/

Description:

A security bypass vulnerability is present in some versions of Red Hat JBoss Enterprise Application Platform.

JBoss JMX Console Unrestricted Access Vulnerability

Vulnerbility:		JBoss JMX Console Unrestricted Access Vulnerability	
Level Risk:		5.0	
Service:	http	**CVE:**	-

Observation:

JBoss is an industry standard application server supported by Red Hat.An unrestricted access vulnerability is present in some versions of JBoss. A flaw is present in the application, which does not secure JMX Console properly. Successful exploitation could allow an attacker to obtain sensitive information.

Recommendation:

The vendor has released an advisory describing a workaround that can be applied to mitigate this issue. More information can be found at: http://community.jboss.org/wiki/SecureTheJmxConsole

Description:

An unrestricted access vulnerability is present in some versions of JBoss.

JBoss Enterprise Application Platform Status Servlet Request Information Disclosure Vulnerability

Vulnerbility:		JBoss Enterprise Application Platform Status Servlet Request Information Disclosure Vulnerability	
Level Risk:		4.0	
Service:	http	**CVE:**	CVE-2008-3273

Observation:

JBoss Enterprise Application Platform (EAP) is a platform for running Java applicationsThe flaw lies in the status servlet in JBoss EAP. Successful exploitation would allow remote attackers to obtain sensitive information via a request with a "full=true" query string.

Recommendation:

Update JBoss Enterprise Application Platform to 4.2.0.CP3 or 4.3.0.CP1

Description:

A vulnerability exists in JBoss Enterprise Application Platform (EAP) that may allow for sensitive information disclosure.

JBoss Web Console Cross-Site Scripting Vulnerability (CVE-2009-2405)

Vulnerbility:	JBoss Web Console Cross-Site Scripting Vulnerability (CVE-2009-2405)		
Level Risk:	4.0		
Service:	http	**CVE:**	CVE-2009-2405

Observation:
JBoss Enterprise Application Platform is an open-source Java EE-based application serverJBoss Enterprise Application Platform doesn't properly sanitize user input to the monitorName, objectName, attribute, or period parameters to createSnapshot.jsp, or the monitorName, objectName, attribute, threshold, period, or enabled parameters to createThresholdMonitor.jsp which allow remote attackers to inject arbitrary web script or HTML.

Recommendation:
Upgrade JBoss EAP 4.2.0 to 4.2.0.CP08, 4.3 to 4.3.0.CP07, and 5.1.0 to 5.1.0.GA.https://rhn.redhat.com/errata/RHSA-2009-1636.html https://rhn.redhat.com/errata/RHSA-2009-1637.html https://rhn.redhat.com/errata/RHSA-2009-1649.html https://rhn.redhat.com/errata/RHSA-2009-1650.html

Description:
JBoss Enterprise Application Platform is prone to multiple cross-site scripting (XSS) vulnerabilities.

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.

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.

Microsoft SQL Server Authentication Mode

Vulnerbility:		Microsoft SQL Server Authentication Mode	
Level Risk:		0.0	
Service:	ms-sql-s	**CVE:**	-

Observation:
Microsoft SQL Server is an enterprise class relational database management system.The target host is running Microsoft SQL Server with authentication enabled. Microsoft SQL Server has two types of authentication modes: "SQL Server and Windows" and "Windows only".

Recommendation:
Ensure that the Microsoft SQL Server authentication mode in use complies with your enterprise policy.

Description:
The target host is running Microsoft SQL Server with authentication enabled.

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.

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.

LDAP Server Detected

Vulnerbility: LDAP Server Detected
Level Risk: 0.0
Service: ldap **CVE:** -

Observation:
Lightweight Directory Access Protocol (LDAP) is an access protocol used for querying and manipulating data of directory services. LDAP server was detected on the host.

Recommendation:
Ensure that LDAP server complies with organizational policy.

Description:
LDAP server was detected 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.

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.

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.

LDAP Crafted Search Request Access Allowed

Vulnerbility: LDAP Crafted Search Request Access Allowed
Level Risk: 0.0
Service: ldap **CVE:** -

Observation:
Lightweight Directory Access Protocol (LDAP) is an access protocol used for querying and manipulating data of directory services. LDAP host allows search requests with objectClass=* filter. It is possible to obtain host information through such requests.

Recommendation:
Ensure that LDAP complies with organizational policy.

Description:
Lightweight Directory Access Protocol (LDAP) host allows search requests with objectClass=* filter.

Microsoft Windows Domain Or Workgroup Detection

Vulnerbility: Microsoft Windows Domain Or Workgroup Detection
Level Risk: 0.0
Service: microsoft-ds **CVE:** CVE-MAP-NOMATCH

Observation:
Microsoft Windows is an industry standard operating system. It is possible to group computers running the Windows operating system into administrative domains or workgroups. This check determines the target's primary domain name, system account domain name and whether the primary domain is a workgroup or domain. If the primary domain name has no associated security identifier (SID) then it is determined to be a workgroup name.This check requires anonymous access to the lsarpc interface. On Windows XP SP2, Windows 2003 and later systems, the default configuration may prevent this check from obtaining the domain information. For more information see: http://support.microsoft.com/default.aspx?scid=kb;en-us;179891

Recommendation:
Ensure that host's domain or workgroup membership complies with corporate policy.

Description:
The target's domain or workgroup name was 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.

SSH Protocol Supported Versions Detected

Vulnerbility: SSH Protocol Supported Versions Detected
Level Risk: 0.0
Service: ssh **CVE:** -

Observation:
SSH protocol is used to establish a secure channel for data exchange.SSH protocol supported version was detected on the host.

Recommendation:
Ensure that ssh protocol complies with organizational policy.

Description:
SSH protocol supported version was detected on the host.

LDAP Service Detected

Vulnerbility: LDAP Service Detected
Level Risk: 0.0
Service: ldap **CVE:** -

Observation:
Provides Lightweight Directory Access Protocol (LDAP) connectivity.

Recommendation:
Disable this service unless the functionality provided is required and permitted by your enterprise security policy. Removing unnecessary services reduces the security risk, exposure and overall digital footprint of hosts in an environment, thereby increasing the overall security posture of your organization.

Description:
The LDAP service is running on the host.

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.

LDAP Server NULL Bind Connection Allowed

Vulnerbility: LDAP Server NULL Bind Connection Allowed
Level Risk: 0.0
Service: ldap **CVE:** -

Observation:
Lightweight Directory Access Protocol (LDAP) is an access protocol used for querying and manipulating data of directory services. LDAP server allows null bind connection.

Recommendation:
Ensure that LDAP server complies with organizational policy.

Description:
Lightweight Directory Access Protocol (LDAP) server allows null bind connection.

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.

LDAP NULL Base Search Access Allowed

Vulnerbility: LDAP NULL Base Search Access Allowed
Level Risk: 0.0
Service: ldap **CVE:** -

Observation:
Lightweight Directory Access Protocol (LDAP) is an access protocol used for querying and manipulating data of directory services. LDAP null base search access is allowed.

Recommendation:
Ensure that LDAP complies with organizational policy.

Description:
Lightweight Directory Access Protocol (LDAP) null base search access is allowed.

Microsoft SQL TCP Listener Detected

Vulnerbility: Microsoft SQL TCP Listener Detected
Level Risk: 0.0
Service: ms-sql-s **CVE:** -

Observation:
Microsoft SQL Server is an industry standard database server.MS SQL uses TCP port 1433 for communication between a database and other application servers. Some malware, such as the SQL Slammer/Sapphire Worm, has spread using communication on port 1433. Systems: Microsoft SQL - any

Recommendation:
Ensure that access controls restrict network traffic on port 1433 to essential hosts only. Block access to the port on border devices such as firewalls and routers.

Description:
A Microsoft SQL Server TCP listener was detected.

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.

Microsoft Windows Active Directory Domain Controller Detected

Vulnerbility:		Microsoft Windows Active Directory Domain Controller Detected	
Level Risk:		0.0	
Service:	ldap	**CVE:**	-

Observation:
Microsoft Active Directory is a directory structure used to store information about the Windows domain.Microsoft Windows Active Directory/Domain Controller was detected on the host and the domain controller name was obtained.

Recommendation:
Ensure Microsoft Windows Active Directory/Domain Controller complies with organizational policy.

Description:
Microsoft Windows Active Directory/Domain Controller was detected on the host.

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.

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.

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.

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.

DNS Server Detected

Vulnerbility:		DNS Server Detected	
Level Risk:		0.0	
Service:	domain	**CVE:**	-

Observation:
Domain Name System (DNS) servers are used to manage the naming system for computers and services in a network.DNS Server was detected on the host.

Recommendation:
Ensure that DNS Server complies with organizational policy.

Description:
DNS Server was detected on the host.