Vulnerabilities
MANAGEMENT

Host Vulnerabilities Report

Hostname:	HO-CNTT-TT2-037
IP Address:	10.1.171.157
Submit by:	admin
Generated Time:	Oct. 1, 2018, 3:46 p.m.

Table Of Contents

Table Of Contents 2
Host Detailed Information 3
Information 3
Running Service 3
Vulnerabilities 4
Overview 4
Scan History 5
Current Vulnerabilities In Detail 6
NetBIOS Sessions Using Any Username And Password Are Allowed 6
Microsoft IIS Server Detected 6
VNC Server Detected 7
Microsoft Terminal Service Has Not Been Configured Network Level Authentication 7
VNC HTTP Console 8
Web Server HTTP Protocol Version Detected 8
Microsoft Remote Procedure Call Service Detected 8
Microsoft Windows NETBIOS Anonymous Accessible Shares Detected 9
Microsoft Windows Anonymous Remote Registry Pipe Access Detected 9
Microsoft Windows Anonymous Remote Registry Key Access Detected 9
NetBIOS Null Session Enabled 10
Hidden WWW Server Name Detected 10
Microsoft IIS Basic Authentication Scheme Disabled 11
LSASS RPC Interface Detected 11
Microsoft IIS NTLM Authentication Disabled 11
Microsoft Windows Terminal Service 12

Host Detailed Information

Information

Submit by:		admin	
Created Date:		Sept. 10, 2018, 3:30 a.m.	
Updated Date:		Sept. 10, 2018, 3:30 a.m.	
Hostname:	HO-CNTT-TT2-037	**Ip Address:**	10.1.171.157
OS:	Windows 7 Professional (Service Pack 1)	**Version:**	NA#

Description:
NA#

Running Service

Service	Network Port	Description
http	5800	
loc-srv	135	
netbios-ssn	139	
microsoft-ds	445	
ms-term-service	3389	
vnc	5900	
unknown	49153	
unknown	49154	
http	80	

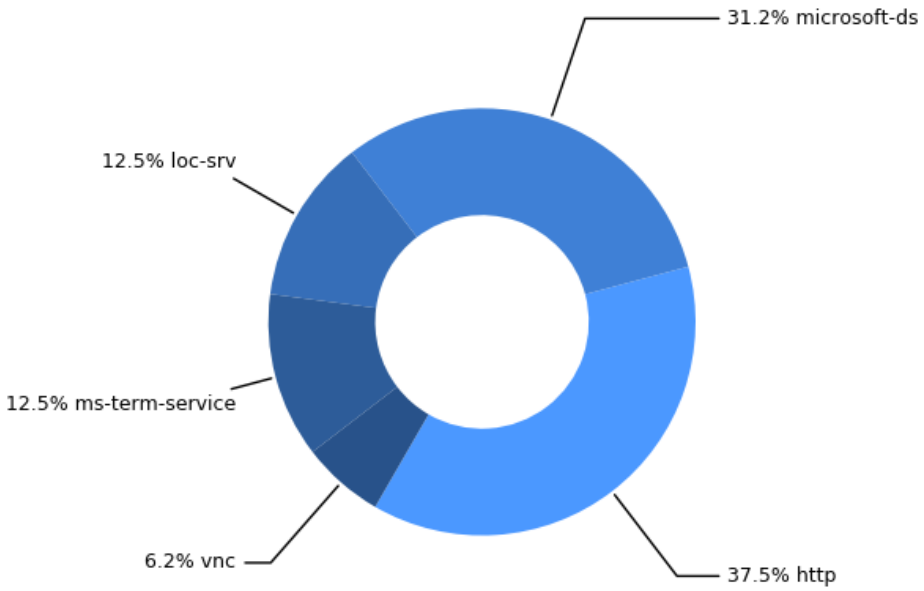
Table 1: Running Services of Host

Vulnerabilities

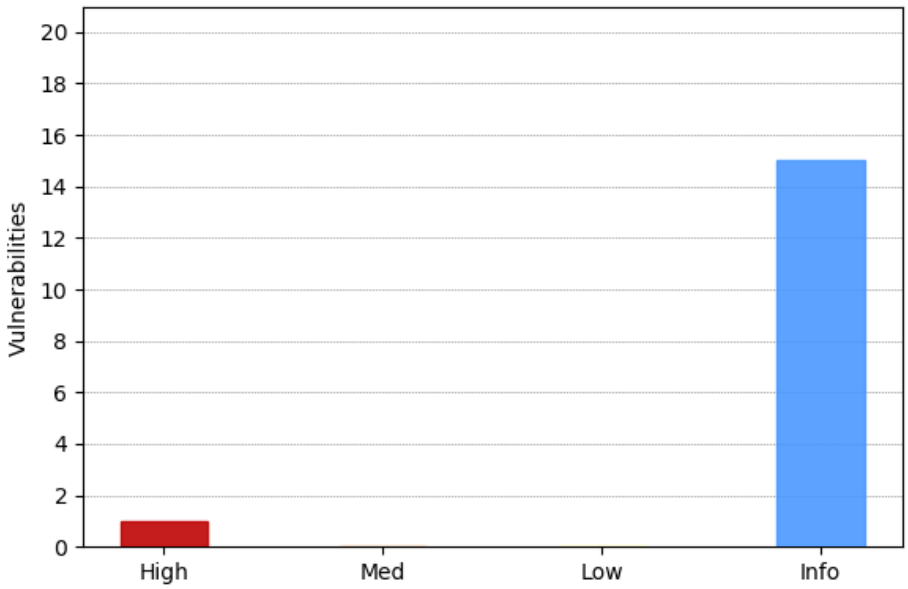
Overview

In this section, this report contains overview information that includes statistics by running services (in graph-1) and current categorized vulnerabilities (in graph-2) 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.



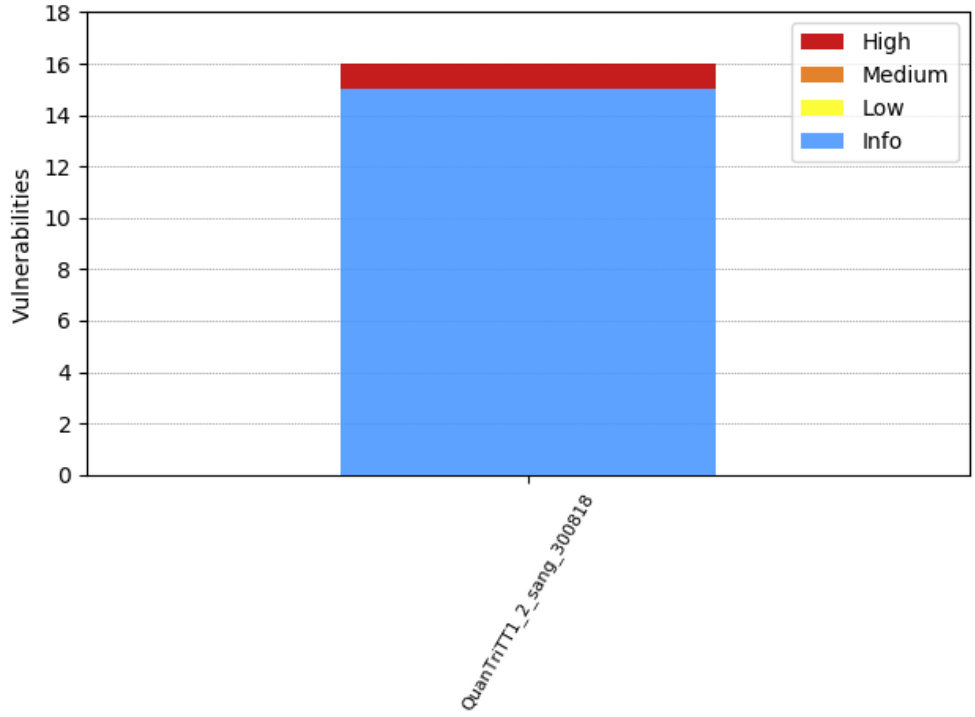
Graph 1: Vulnerabilities statistic by services



Graph 2: Current Vulnerabilities of Host

Scan History

In this section, the report contains scan history of host. It includes scan frequency and brief information of involved scan tasks.



Graph 3: Scan History Statistic of Host

Scan History:

Scan Task	Start Time	Finished Time	Vulnerabilities			
			High	Med	Low	Info
QuanTriTT1_2_sang_300818	Aug. 30, 2018, 4:30 a.m.	Aug. 30, 2018, 4:57 a.m.	1	0	0	15

Table 2: Scan History of Host

Current Vulnerabilities In Detail

NetBIOS Sessions Using Any Username And Password Are Allowed

Vulnerbility:		NetBIOS Sessions Using Any Username And Password Are Allowed	
Level Risk:		7.0	
Service:	microsoft-ds	**CVE:**	CVE-1999-0519

Observation:
The Network Basic Input/Output System (NetBIOS) is an Application Programming Interface (API) that allows computers to communicate over a network. The host allows remote computers to establish a NetBIOS session using any username and password. On a Microsoft Windows machine, this indicates that the Guest account has a blank password.

Recommendation:
On Windows systems, disable the Guest account or at least set a non-blank password for the account.For Samba on Linux, set the following in the smb.conf file: guest account = NO_SUCH_USER restrict anonymous = yeswhere NO_SUCH_USER is not a valid user in the password file. For other Unix based operating systems, refer the vendor specific documentation and restrict Samba guest account and anonymous login by making necessary changes in the Samba configuration file.

Description:
The host allows remote computers to establish a NetBIOS session using any username and password.

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.

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.

Microsoft Terminal Service Has Not Been Configured Network Level Authentication

Vulnerbility:		Microsoft Terminal Service Has Not Been Configured Network Level Authentication	
Level Risk:		0.0	
Service:	ms-term-service	**CVE:**	-

Observation:
The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication. Network Level Authentication provides better security than previous authentication approach.

Recommendation:
Consider to configure the Terminal Service to use Network Level Authentication if possible.More details could be found at: http://technet.microsoft.com/en-us/library/cc732713.aspx

Description:
The target is running Microsoft Terminal Service and the Terminal Service has not been configured Network Level Authentication.

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.

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.

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.

Microsoft Windows NETBIOS Anonymous Accessible Shares Detected

Vulnerbility:		Microsoft Windows NETBIOS Anonymous Accessible Shares Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
Microsoft Windows is an industry standard operating system. SMB shares can be accessed anonymously on the Windows host.

Recommendation:
Ensure that Microsoft Windows complies with organizational policy.

Description:
SMB shares can be accessed anonymously on the Windows host.

Microsoft Windows Anonymous Remote Registry Pipe Access Detected

Vulnerbility:		Microsoft Windows Anonymous Remote Registry Pipe Access Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
Microsoft Windows is an industry standard operating system. Anonymous remote registry access was detected on the Windows host.

Recommendation:
Ensure that Microsoft Windows host complies with organizational policy.

Description:
Anonymous remote registry access was detected on the Windows host.

Microsoft Windows Anonymous Remote Registry Key Access Detected

Vulnerbility:		Microsoft Windows Anonymous Remote Registry Key Access Detected	
Level Risk:		0.0	
Service:	microsoft-ds	**CVE:**	-

Observation:
Microsoft Windows is an industry standard operating system. Anonymous remote registry key access was detected on the Windows host.

Recommendation:
Ensure that Microsoft Windows host complies with organizational policy.

Description:
Anonymous remote registry key access was detected on the Windows host.

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.

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 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.

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.

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.

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.