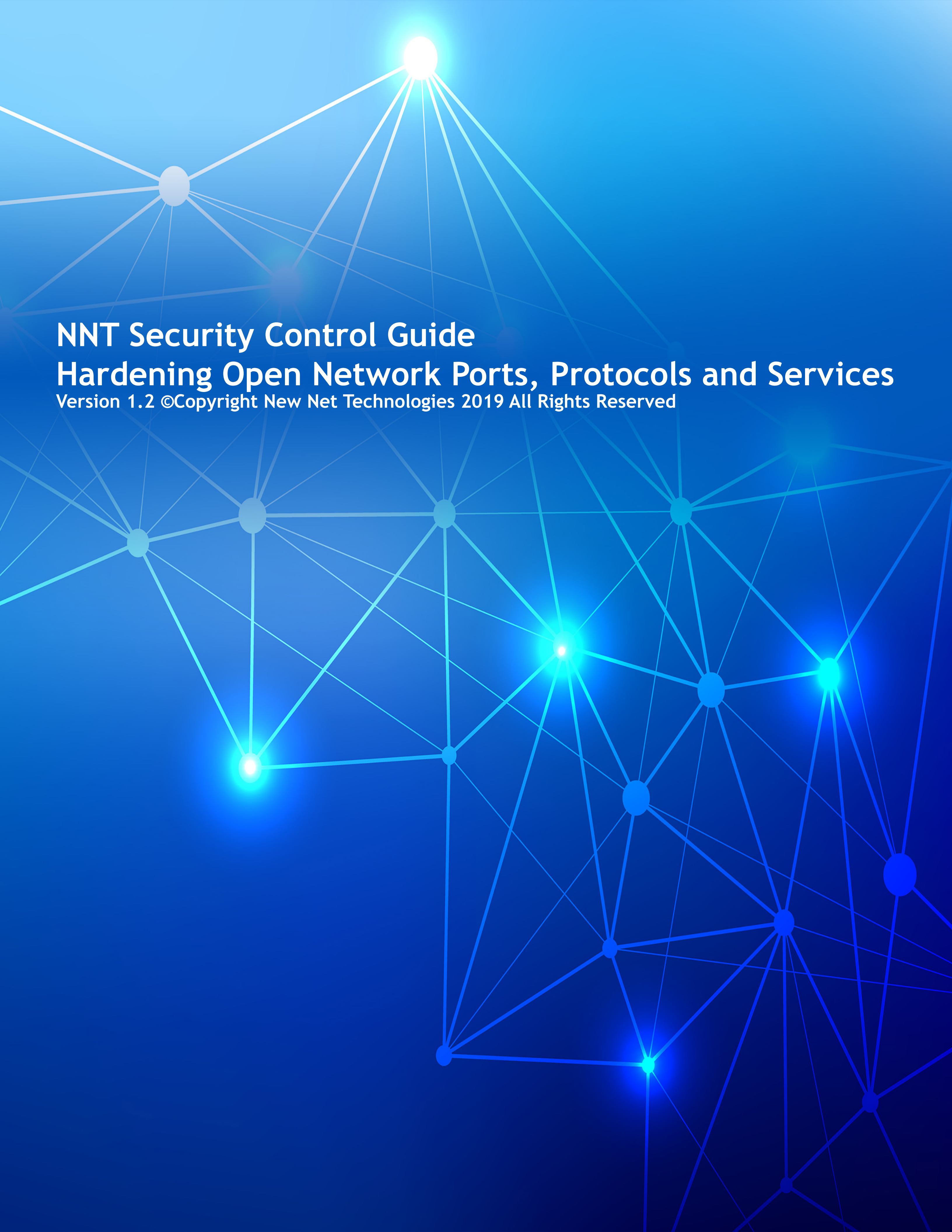


NNT Security Control Guide
Hardening Open Network Ports, Protocols and Services

Version 1.2 ©Copyright New Net Technologies 2019 All Rights Reserved

Introduction

This guide will help the reader to understand:

- Why the control of open ports, protocols and services is an essential cyber security control
- Which open ports and protocols are viewed as safe for any network, and which are considered unsafe?
- How do you detect open ports and protocols on your network?
- How to identify which services/applications are using which ports/protocols?
- What to do if you need to remove open ports, protocols and/or services from your systems

Background

In summary, every source of security control guidance (see following examples) recommends the same thing: any network ports, protocols and running services increases the opportunity for a system to be compromised.

As an analogy, think of the Star Wars® 'Death Star': It was designed to be impregnable, seemingly impossible to attack. But it still needed an engine, which in turn needed an exhaust port, which ultimately left it prone to a fatal strike.

Therefore in any scenario, be it for IT systems or planet-busting, intergalactic weapons of mass destruction, reducing the 'attack surface' is a critical security control.

To provide a typical example, configuration services for a host or appliance will be presented via a Web interface or command line. Interaction with the service via the network must use the assigned protocol to connect to the designated port, in this example, the HTTPS protocol via port 443 and the SSH protocol via port 22.

From this example you can see that each protocol has a default port assigned. Appendix A provides a useful guide to 'Well-Known and Registered Ports'. The port number is just another level of addressing so that connections to an IP Address can be paired up with the underlying service.

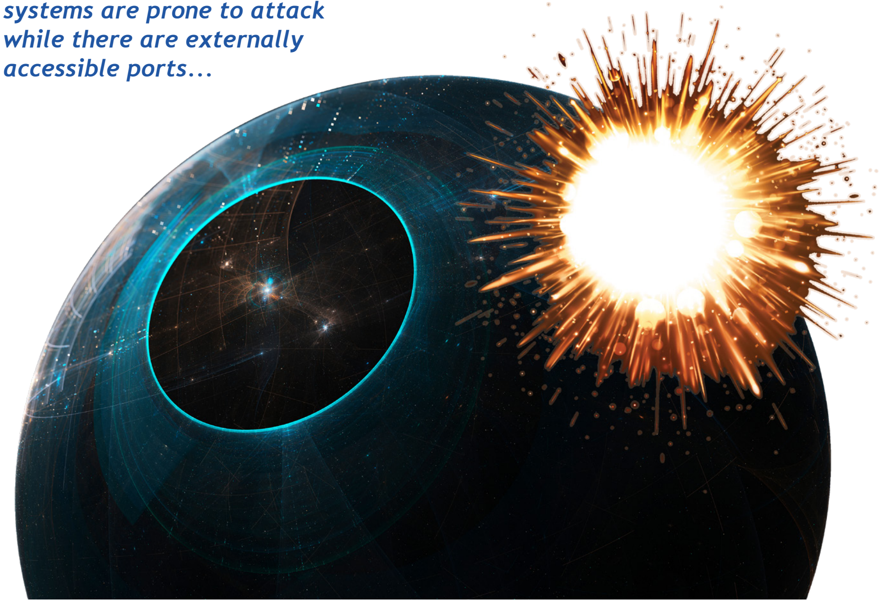


Figure 1: Even the most secure systems are prone to attack while there are externally accessible ports...

While the protocol must always match the service, you can usually go freestyle and assign your own choice of port number. Indeed, this is a standard security best practice intended to throw hackers off the scent. Using the default port for the service removes any need to guess which protocol to use, so using a non-standard port number serves as interference.

In summary, this entwined relationship between service, protocol and port is important to understand – you can't have one without the others.

In other words, remove the service, you eliminate the protocol and close the port. In this way, the opportunities for an attacker are diminished.

Why is control of open ports and protocols a critical security control?

The main reasons why monitoring open ports is ordained a key security control:

- The more open/accessible we make a system, the greater the attack surface (even for the Death Star). With new exploits being discovered every day, anything that reduces the potential for attack, the better
- Where a service is needed, and there is a choice of ports/protocols offered i.e. HTTP or HTTPS using TLS 1.2+, we want to use the secured variant
- By extension, we also want to ensure that the non-encrypted channel is never used and disable it

The Center for Internet Security provides this rationale for CIS Control 9:

"Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of different device types, often without a business need for the given service.

Many software packages automatically install services and turn them on as part of the installation of the main software package without informing the user. Attackers scan for such services and attempt to exploit these services, often attempting to exploit default user IDs and passwords or widely available exploitation code"

Similarly, the **NERC CIP** standard calls for

*"**Standard CIP-007-3** requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3"*

And for **NIST 800-53**

*"**CM-6 CONFIGURATION SETTINGS - Control:** The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures*

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system… Security-related parameters are those parameters impacting the security state of information systems including… (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline"

And finally for **PCI DSS V3.2.1**

*"**Requirement 2.2:** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards…Enabling only necessary services, protocols, daemons, etc., as required for the function of the system, Implementing additional security features for any required services, protocols or daemons that are considered to be insecure"*

Examples of Detailed Controls related to Open Ports

To provide a more detailed example, the NERC CIP standard calls for:

CIP-007-3	Cyber Security — Systems Security Management:
R1-1.2, R2-R2.3, R3.1-R3.3, R4.1-R4.4, R5.1-R5.7	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

Table 1: NERC CIP requires control of ports and services

While the CIS Critical Security Control 9 defines the following sub-controls:

CIS Control9: Limitation and Control of Network Ports, Protocols, and Services				
Sub-Control	*Asset Type*	*Security Function*	*Control Title*	*Control Description*
9.1	Devices	Identify	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.
9.4	Devices	Protect	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.

Table 2: The Center for Internet Security (CIS) place control of ports, protocols and services in their Top Ten of Critical Security Controls

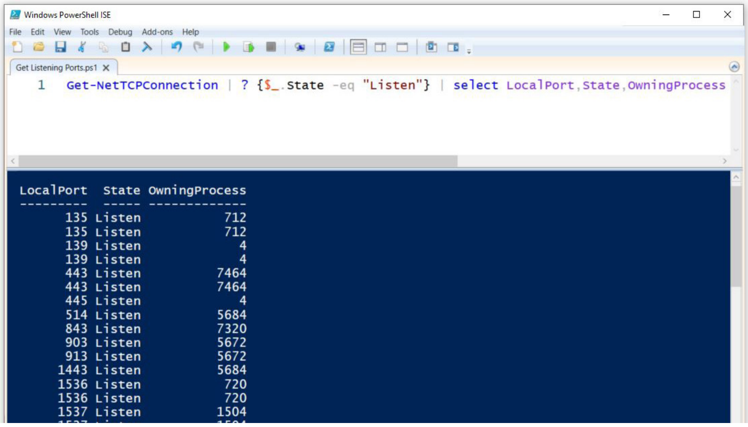
How do you detect open ports and protocols on your network?

There are two main approaches to consider, each with pros and cons. Call them External and Direct.

Figure 2: Is there anybody out there? A network scan looks for open ports on a network by sending test connections and waiting for a response

The External Option to discover ports and protocols presented by your systems uses a network-based port-scan. It's like a sonar scan via the network, with test connections sprayed out to all IP addresses while listening for any positive responses returned. This builds a picture of which IP addresses are in use and by virtue of responses from devices that respond, it can be determined which ports are available and which protocols and therefore services are likely to be in use.

This is actually Step 1, Chapter 1 of the Hacking 101 course notes and as such, Port Scanning has very negative connotations in firewall terms. Since this is often used for bad, it is a network activity that firewalls are designed to prevent/alert on. As such, this is an important consideration when running a discovery scan.



```
Get-NetTCPConnection | ? {$_.State -eq "Listen"} | select LocalPort,State,OwningProcess
```

```
LocalPort  State OwningProcess
---------  ----- -------------
      135 Listen           712
      135 Listen           712
      139 Listen             4
      139 Listen             4
      443 Listen          7464
      443 Listen          7464
      445 Listen             4
      514 Listen          5684
      843 Listen          7320
      903 Listen          5672
      913 Listen          5672
     1443 Listen          5684
     1536 Listen           720
     1536 Listen           720
     1537 Listen          1504
```

Figure 3: Most platforms provide commands to report all listening ports - but should these ports be available when they could render the system more prone to attack?

By contrast, the Direct Approach involves interrogating the system directly at a command-line level, querying the device with specific commands designed to list out ports in use, for example netstat. This sounds like a good solution but isn't without a few drawbacks, not least that it requires direct access to each device, the right commands for each environment and a degree of interpretation of the results to get a clear answer for the security control.

Both these options are explored further later, with some useful commands to use and some suggestions on automated options.

The summary is that measuring open ports in a way that is consistent and reliable is actually way more difficult than it sounds.

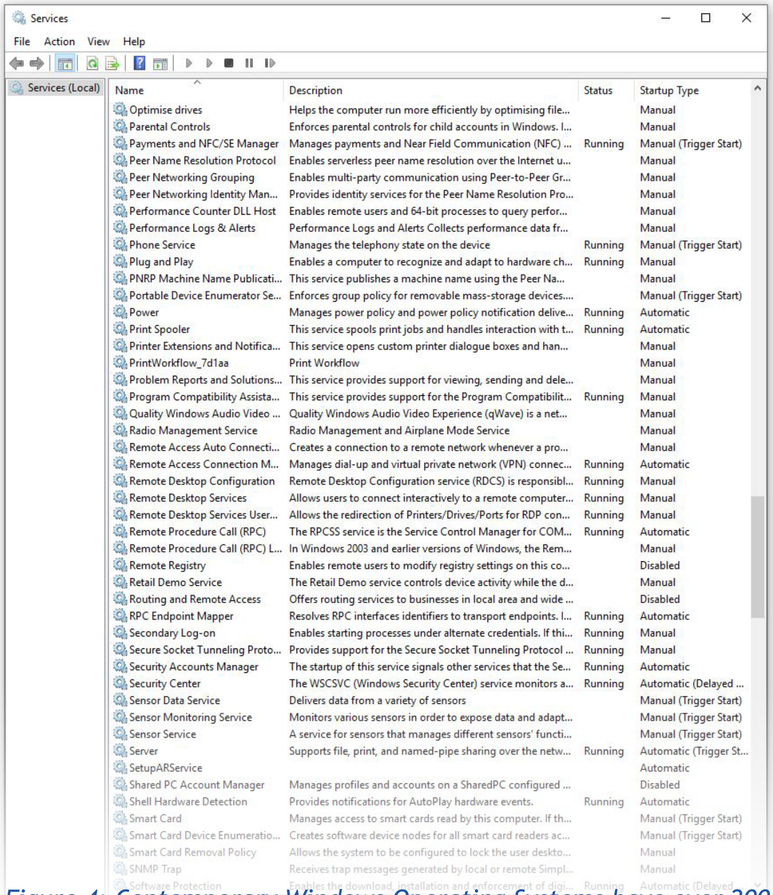
For instance, in no particular order, problems are presented by:

- Protocols that use random or Ephemeral Ports
- Ports that open and close as manual or on-demand services start/stop
- and of course, Firewalls that are designed to control/block traffic

And all this is before you start trying to test the existence of UDP ports, more challenging because, unlike their TCP cousins, UDP services are notoriously reluctant to respond when tested during a scan.

Remember - it's 'Ports, Protocols *AND* Services'

One other option is to flip the control around and instead focus on the services dimension first. This is something that the best vulnerability scanners can deliver, reporting on services using a credentialed scan, but because it significantly extends scan durations, it is seldom used.



Name	Description	Status	Startup Type
Optimise drives	Helps the computer run more efficiently by optimising file...		Manual
Parental Controls	Enforces parental controls for child accounts in Windows. I...		Manual
Payments and NFC/SE Manager	Manages payments and Near Field Communication (NFC) ...	Running	Manual (Trigger Start)
Peer Name Resolution Protocol	Enables serverless peer name resolution over the Internet u...		Manual
Peer Networking Grouping	Enables multi-party communication using Peer-to-Peer Gr...		Manual
Peer Networking Identity Man...	Provides identity services for the Peer Name Resolution Pro...		Manual
Performance Counter DLL Host	Enables remote users and 64-bit processes to query perfor...		Manual
Performance Logs & Alerts	Performance Logs and Alerts Collects performance data fr...		Manual
Phone Service	Manages the telephony state on the device	Running	Manual (Trigger Start)
Plug and Play	Enables a computer to recognize and adapt to hardware ch...	Running	Manual
PNRP Machine Name Publicati...	This service publishes a machine name using the Peer Na...		Manual
Portable Device Enumerator Se...	Enforces group policy for removable mass-storage devices....		Manual (Trigger Start)
Power	Manages power policy and power policy notification delive...	Running	Automatic
Print Spooler	This service spools print jobs and handles interaction with t...	Running	Automatic
Printer Extensions and Notifica...	This service opens custom printer dialogue boxes and han...		Manual
PrintWorkflow_7d1aa	Print Workflow		Manual
Problem Reports and Solutions...	This service provides support for viewing, sending and dele...		Manual
Program Compatibility Assista...	This service provides support for the Program Compatibilit...	Running	Manual
Quality Windows Audio Video ...	Quality Windows Audio Video Experience (qWave) is a net...		Manual
Radio Management Service	Radio Management and Airplane Mode Service		Manual
Remote Access Auto Connecti...	Creates a connection to a remote network whenever a pro...		Manual
Remote Access Connection M...	Manages dial-up and virtual private network (VPN) connec...	Running	Automatic
Remote Desktop Configuration	Remote Desktop Configuration service (RDCS) is responsibl...	Running	Manual
Remote Desktop Services	Allows users to connect interactively to a remote computer...	Running	Manual
Remote Desktop Services User...	Allows the redirection of Printers/Drives/Ports for RDP con...	Running	Manual
Remote Procedure Call (RPC)	The RPCSS service is the Service Control Manager for COM...	Running	Automatic
Remote Procedure Call (RPC) L...	In Windows 2003 and earlier versions of Windows, the Rem...		Manual
Remote Registry	Enables remote users to modify registry settings on this co...		Disabled
Retail Demo Service	The Retail Demo service controls device activity while the d...		Manual
Routing and Remote Access	Offers routing services to businesses in local area and wide ...		Disabled
RPC Endpoint Mapper	Resolves RPC interfaces identifiers to transport endpoints. I...	Running	Automatic
Secondary Log-on	Enables starting processes under alternate credentials. If thi...	Running	Manual
Secure Socket Tunneling Proto...	Provides support for the Secure Socket Tunneling Protocol ...	Running	Manual
Security Accounts Manager	The startup of this service signals other services that the Se...	Running	Automatic
Security Center	The WSCSVC (Windows Security Center) service monitors a...	Running	Automatic (Delayed ...
Sensor Data Service	Delivers data from a variety of sensors		Manual (Trigger Start)
Sensor Monitoring Service	Monitors various sensors in order to expose data and adapt...		Manual (Trigger Start)
Sensor Service	A service for sensors that manages different sensors' functi...		Manual (Trigger Start)
Server	Supports file, print, and named-pipe sharing over the netw...	Running	Automatic (Trigger St...
SetupARService			Automatic
Shared PC Account Manager	Manages profiles and accounts on a SharedPC configured ...		Disabled
Shell Hardware Detection	Provides notifications for AutoPlay hardware events.	Running	Automatic
Smart Card	Manages access to smart cards read by this computer. If th...		Manual (Trigger Start)
Smart Card Device Enumeratio...	Creates software device nodes for all smart card readers ac...		Manual (Trigger Start)
Smart Card Removal Policy	Allows the system to be configured to lock the user deskto...		Manual
SNMP Trap	Receives trap messages generated by local or remote Simpl...		Manual
Software Protection	Enables the download, installation and enforcement of digi...	Running	Automatic (Delayed ...

Figure 4: Contemporary Windows Operating Systems have over 200 services installed. Deciding which of these can be safely disabled without affecting required functionality is far from straightforward.

For this services-lead approach, host-resident, system integrity monitoring technology delivers a superior solution. This option not only gathers details of installed services with their running and startup states, but by being host-resident, also has the advantage of being able to continuously track changes to service configuration settings.

For example, NNT Change Tracker™ Gen 7 R2 uses distributed agents covering each device so unlike a Vulnerability Scanner, the collection of services data is performed in a massively parallel manner with each device being queried simultaneously.

This means that both for

- Change Control (reporting any drift from the baseline configuration build), and
- Breach Detection (reporting unexpected new services and processes)

So the true intent of the security control is being delivered.

Ultimately, both the port and service dimensions should be tested and baselined with changes tracked, but the argument to reverse the priority of the security control, focusing more on services than open ports, makes a lot of sense.

Security controls are subject to a 'bang-for-buck' rating like anything else, and one that is easier to operate, with easier to interpret results, will always be more effective than a more technically challenging parallel. And while the incidence of breaches continues to increase, anything that makes security best practices easier to implement and us more secure should be welcomed. Any port in storm...

See Step One - Discovery for detailed guidance on options for exposing open ports on systems using both External Options and Direct Options, including commands to use.

Implementing a Hardened Port and Protocol Standard

So far we have looked at why open ports are a security consideration, and discussed the concepts available for building a picture of the open ports and protocols in use within our network, finally exploring a services-lead approach to dealing with control of services/protocols and ports.

But once you have your scan results listing out all the devices on the network and showing which ports are open, how do you then determine which service is behind the port, and crucially, whether it needs to remain in place or not?

Port Numbers and their assigned usage

The Internet Assigned Numbers Authority (IANA) is the official body responsible for allocating port numbers to protocols.

As such, there is a globally agreed listing of both TCP and UDP port numbers and their assigned usage.

There are three categories of ports:

- ***Well-Known Ports***, covering the most commonly used system ports in the range 0 – 1023
- ***Registered Ports***, covering ports that have been assigned to manufacturers and applications within the range of 1024 – 49151
- ***Ephemeral Ports***, covering a pool of dynamically allocated private ports used on a session by session basis for any services not included within the Well Known and Registered ranges

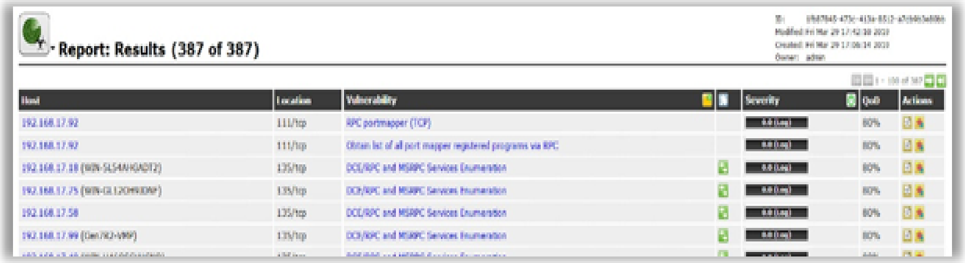
See Appendix A for a table detailing the services associated with any port number in Appendix A.

How do I determine which service is associated with which port number?

We now have either our scan results or the netstat-equivalent command output from the device(s) being assessed. It is likely there will be a long list of open ports, both TCP and UDP - so what's the next move? Remember the goal is to minimize open ports and protocols in order to reduce the attack surface presented.

Fortunately the association between ports, protocols and services is globally agreed and adhered to. This assignment of an officially designated port number to a protocol and service is overseen by the Internet Assigned Numbers Authority - see the side panel for more information.

A good automated scanning solution such as NNT Vulnerability Tracker™ or NNT Change Tracker™ will provide this association for you as standard following a scan.



Report: Results (387 of 387)

Host	Location	Vulnerability		Severity	QoD	Actions
192.168.17.92	111/tcp	RPC portmapper (TCP)		0.0 (Log)	80%	
192.168.17.92	111/tcp	Obtain list of all port mapper registered programs via RPC		0.0 (Log)	80%	
192.168.17.18 (WIN-SL54AHGADT2)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.75 (WIN-GL12OHN3DNP)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.58	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.99 (Dan782-VMP)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	

Figure 5: NNT Vulnerability Tracker™ provides scan results listing devices with their open ports and the service registered to the port

As a helpful reference you can see a table detailing the services associated with any port number in Appendix A. The table is a comprehensive list of all relevant, contemporary Well Known and Registered ports most likely to appear on your network and, in turn, the service behind the port.

NNT have taken the list a step further in indicating those ports/services that are considered to be ***'Expected and Acceptable'***, plus those that are ***'Not Acceptable'*** and where there is a preferable alternative port to use (usually the secure/encrypted variant of the protocol in question).

See ***Step 2 – Correlate Open Ports to Services/Applications*** for detailed guidance on determining which port is backed by which service/application, including commands to use.

What to do if you need to remove open ports, protocols and/or services from your systems?

Once you have a list of open ports accessible on your systems, for each one listed it will be necessary to pass the test of 'Is the service behind this port essential for our business services?'. In some cases there may be overlapping parallel ports/protocols for the same fucntion, for example a web server that offers both HTTP and HTTPS.

For other ports, it may be that there are simply default services or unwanted extras installed on the platform that are not needed for your environment, for example, software update services or remote management capabilities. In this case, either look to remove the package/program in question, or stop and disable the services under review. Commands are provided in "*Step 3 – Harden Systems to Eliminate Unwanted/Unnecessary Open Ports*"

How do I decide which open ports, protocols and services should be removed?

Ultimately, as with any configuration hardening project, only you can decide which services - and therefore which ports and protocols - are essential for your organizations' business services.

CIS Control 9 *"Ensure that only network ports, protocols, and services listening on a system with* ***validated business needs****, are running on each system"*

Just as there is no such thing as '100% secure', there are no truly 'safe' ports, but the more you can minimize functionality, the more you can reduce the attack surface presented.

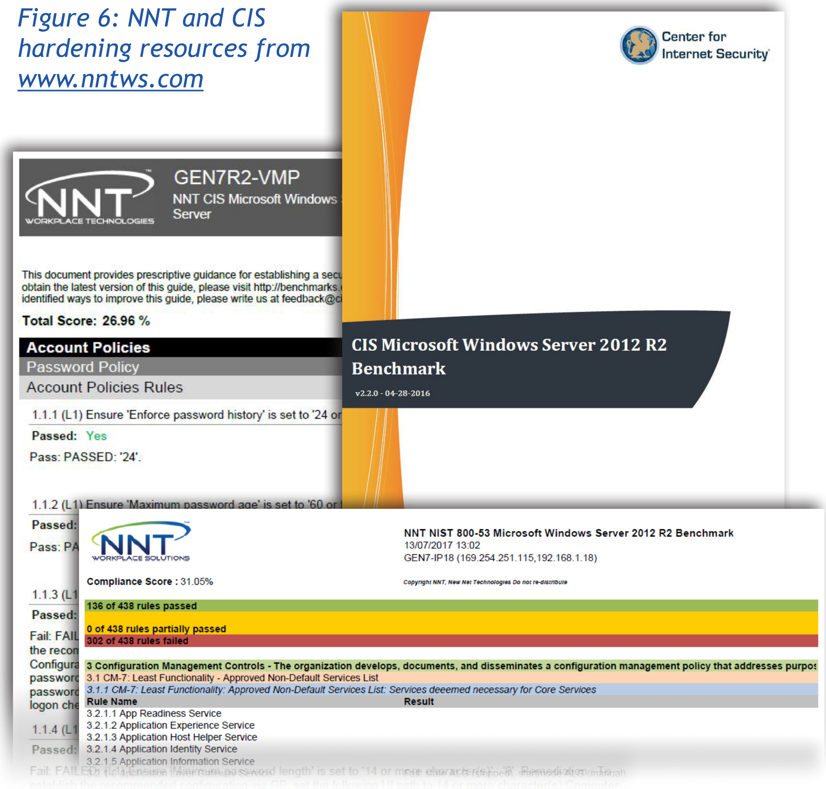


Figure 6: NNT and CIS hardening resources from www.nntws.com

GEN7R2-VMP
NNT CIS Microsoft Windows
Server

This document provides prescriptive guidance for establishing a secu
obtain the latest version of this guide, please visit http://benchmarks.
identified ways to improve this guide, please write us at feedback@ci

Total Score: 26.96 %

Account Policies
Password Policy
Account Policies Rules

1.1.1 (L1) Ensure 'Enforce password history' is set to '24 or

Passed: Yes

Pass: PASSED: '24'.

1.1.2 (L1) Ensure 'Maximum password age' is set to '60 or

Passed:

Pass: PA

1.1.3 (L1

Passed:

Fail: FAIL
the recom
Configura
passwor
passwor
logon che

1.1.4 (L1

Passed:

Fail: FAILED: (L1) Ensure 'Minimum password length' is set to '14 or more character(s)' : '0'. Remediation : To
establish the recommended configuration via GP, set the following UI path to 14 or more character(s):Computer

Center for Internet Security

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.2.0 - 04-28-2016

NNT NIST 800-53 Microsoft Windows Server 2012 R2 Benchmark
13/07/2017 13:02
GEN7-IP18 (169.254.251.115,192.168.1.18)

Copyright NNT, New Net Technologies Do not re-distribute

Compliance Score : 31.05%

136 of 438 rules passed

0 of 438 rules partially passed

302 of 438 rules failed

3 Configuration Management Controls - The organization develops, documents, and disseminates a configuration management policy that addresses purpos
3.1 CM-7: Least Functionality - Approved Non-Default Services List
3.1.1 CM-7: Least Functionality: Approved Non-Default Services List: Services deeemed necessary for Core Services

Rule Name	Result
3.2.1.1 App Readiness Service	
3.2.1.2 Application Experience Service	
3.2.1.3 Application Host Helper Service	
3.2.1.4 Application Identity Service	
3.2.1.5 Application Information Service	
3.2.1.6 Application Layer Gateway Service	Fail: State ALG (stopped), startmode ALG (manual).

Help is at hand: NNT publish expert guidance on service hardening, with detailed Hardened Services Lists available free of charge from the NNT website. These have been developed as a '*one size fits all*' hardened services profile that will suit any base Enterprise Server build.

In addition, NNT in conjunction with the Center for Internet Security provide extensive resources to help you with wider configuration hardening. The CIS Benchmark secure configuration guides specify a huge range of configuration settings recommended to improve security, including which default services should be disabled on a platform.

You can download CIS Benchmarks for all platforms and applications here and there are separate 'Recommended Hardened Services Lists' for most Windows and Linux platforms to help further. Finally NNT also provide a number of 'Remediation Kits' which can be used to automatically apply hardened configuration settings in line with the CIS Benchmarks. The Remediation Kit takes the form of either a Windows Group Policy Object template or a Shell Script for Linux.

See Step 3 – Harden Systems to Eliminate Unwanted/Unnecessary Open Ports for detailed guidance on disabling services/protocols/ports, including commands to use.

How can I meet the audit requirement for removing Open Ports and Protocols if I need specific ports for essential business services?

Again, CIS Control 9 and indeed any Security Auditor acknowledge that business services do need to network accessible and there will always be open ports within any network, hence the supplementary guidance

> *"Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed"*, and
>
> *"Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged"*

Open Port Hardening Guide

Step One- Discovery

List Open Ports on Windows

Run PowerShell (Run as Administrator)

```
Get-NetTCPConnection | ? {$_.State -eq “Listen”} | select LocalPort,State,OwningProcess |
Sort-Object LocalPort
```

And to get the associated Process and Path for the executable, use

```
Get-Process -PID <PID_of_Interest> | Select-Object ID,Name,Path
```

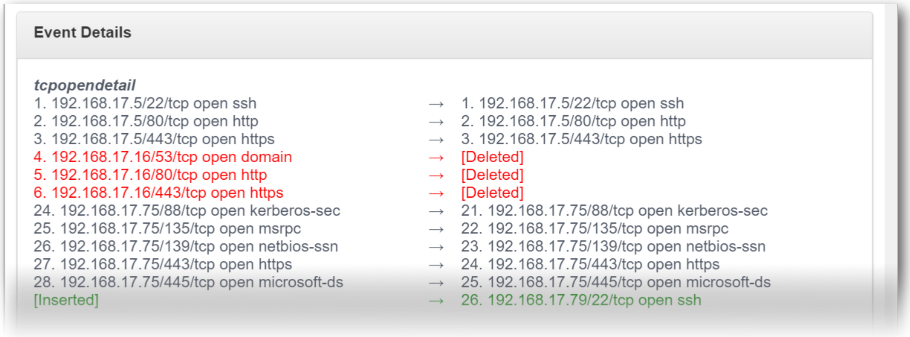
This will help determine which ports are used by which services/applications.

List Open Ports on Linux

```
ss -tulpn | egrep “LISTEN” | awk ‘{print “IP-Port “ $4 “ PID/Name “ $7}’
```

Automated Solutions

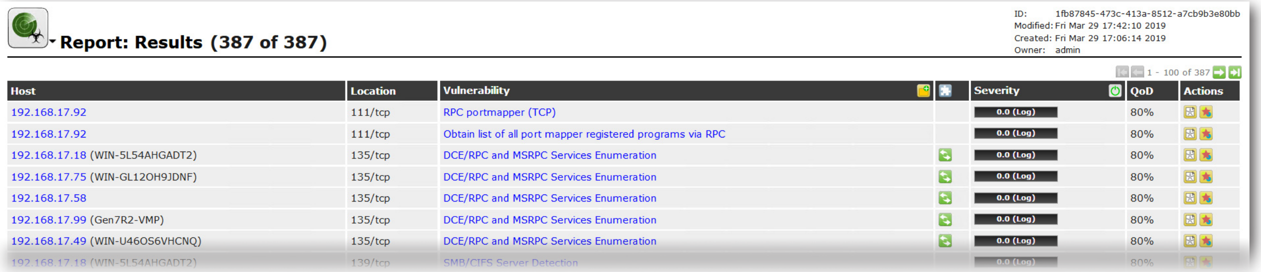
Best options are to use an automated solution that continuously operates and also covers more security controls than just the CIS ‘Limitation and control of Network Ports, Protocols and Services’
NNT Change Tracker™ Gen 7 R2 provides an integrated Network Port scanner to discover open ports across all devices within your network estate. Better still is that Change Tracker™ will repeatedly re-scan the network and clearly highlight any adds, changes or moves, see below.



Event Details

```
tcpopendetail
1. 192.168.17.5/22/tcp open ssh                 →  1. 192.168.17.5/22/tcp open ssh
2. 192.168.17.5/80/tcp open http                →  2. 192.168.17.5/80/tcp open http
3. 192.168.17.5/443/tcp open https              →  3. 192.168.17.5/443/tcp open https
4. 192.168.17.16/53/tcp open domain             →  [Deleted]
5. 192.168.17.16/80/tcp open http               →  [Deleted]
6. 192.168.17.16/443/tcp open https             →  [Deleted]
24. 192.168.17.75/88/tcp open kerberos-sec      →  21. 192.168.17.75/88/tcp open kerberos-sec
25. 192.168.17.75/135/tcp open msrpc            →  22. 192.168.17.75/135/tcp open msrpc
26. 192.168.17.75/139/tcp open netbios-ssn      →  23. 192.168.17.75/139/tcp open netbios-ssn
27. 192.168.17.75/443/tcp open https            →  24. 192.168.17.75/443/tcp open https
28. 192.168.17.75/445/tcp open microsoft-ds     →  25. 192.168.17.75/445/tcp open microsoft-ds
[Inserted]                                      →  26. 192.168.17.79/22/tcp open ssh
```

Change Tracker™ Gen 7 R2 also automates a whole bunch of other vital security controls too so should be an essential part of any organizations cyber security strategy.
NNT Vulnerability Tracker™ also provides an option for open port discovery on an automated basis and equally delivers other essential security controls relating to vulnerability management.



Report: Results (387 of 387)

ID: 1fb87845-473c-413a-8512-a7cb9b3e80bb
Modified: Fri Mar 29 17:42:10 2019
Created: Fri Mar 29 17:06:14 2019
Owner: admin

1 - 100 of 387

Host	Location	Vulnerability		Severity	QoD	Actions
192.168.17.92	111/tcp	RPC portmapper (TCP)		0.0 (Log)	80%	
192.168.17.92	111/tcp	Obtain list of all port mapper registered programs via RPC		0.0 (Log)	80%	
192.168.17.18 (WIN-5L54AHGADT2)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.75 (WIN-GL12OH9JDNF)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.58	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.99 (Gen7R2-VMP)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.49 (WIN-U46OS6VHCNQ)	135/tcp	DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	
192.168.17.18 (WIN-5L54AHGADT2)	139/tcp	SMB/CIFS Server Detection		0.0 (Log)	80%	

Other Options Downloads for both NMAP and OpenVAS (Greenbone Community Edition) provide options for a network-wide port scan.

Step 2 – Correlate Open Ports to Services/Applications

If you determine that you have unwanted or unnecessary services in use, you can then use the next steps to first identify details of the services concerned and then either stop and/or disable the service from running in the future. For example, telnet should never be used on any system where the alternative SSH option is available.

List services on Windows

Use run -> services.msc and use the Services Console to stop and/or disable services.

Use Windows PowerShell (RunAs Administrator) to list all services

```
Get-Service -Name *
```

List services on Linux

From a terminal/putty session,

```
service --status-all
chkconfig --list
systemctl -a
```

Step 3 – Harden Systems to Eliminate Unwanted/Unnecessary Open Ports

Control services on Windows

Use Windows PowerShell (RunAs Administrator)

To stop a service, use

```
Stop-Service -Name <Service_Name_of_Interest>
```

To disable a service

```
Set-Service -Name <Service_Name_of_Interest> -StartupType Disabled
```

Control services on Linux

From a terminal/putty session,

To stop a service use

```
Service <Service-Name> stop
Chkconfig <Service-Name>
Systemctl stop <Service-Name>
```

To disable a service use

```
Systemctl disable <Service-Name>
Chkconfig <Service-Name> off
```

Also inspect the `/etc/init.d/` path for any service control scripts, run an `ls /etc/init.d/` to expose all startup scripts and rename/remove any that are to be disabled.

Well-Known/System Port Numbers

Key:

- 🟦 Expected on most Networks
- 🟧 Consider reconfiguration to use alternative protocol
- ⬜ Review whether functionality is necessary

Port	TCP	UDP	Description
20, 21	TCP	Assigned	File Transfer Protocol (FTP)
22	TCP	Assigned	Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding
23	TCP	Assigned	Telnet protocol—unencrypted text communications
25	TCP	Assigned	Simple Mail Transfer Protocol (SMTP), used for email sending from a client and for routing between mail servers
37	TCP	UDP	Time Protocol
42	Assigned	UDP	Host Name Server Protocol
43	TCP	Assigned	WHOIS protocol
49	TCP	UDP	TACACS Login Host protocol
53	TCP	UDP	Domain Name System (DNS)
67, 68	Assigned	UDP	Dynamic Host Configuration Protocol (DHCP) a.k.a Bootstrap Protocol (BOOTP): server port 67, client port 68
69	Assigned	UDP	Trivial File Transfer Protocol (TFTP)
79	TCP	Assigned	Finger protocol
80	TCP	Assigned	Web Services Hypertext Transfer Protocol (HTTP), regular web browing and web services traffic
88	TCP	Assigned	Kerberos authentication system
104	TCP	UDP	Digital Imaging and Communications in Medicine (DICOM; also port 11112)
107	TCP	UDP	Remote User Telnet Service (RTelnet)
108	TCP	UDP	IBM Systems Network Architecture (SNA) gateway access server
110	TCP	Assigned	Post Office Protocol, version 3 (POP3), basic email protocol for collection of email
115	TCP	Assigned	Simple File Transfer Protocol
117	TCP	UDP	UUCP Mapping Project (path service)
123	Assigned	UDP	Network Time Protocol (NTP), used for time synchronization
135	TCP	UDP	Microsoft End Point Mapper/RPC Locator service, remote management for DHCP server, DNS server, WINS & DCOM
137	TCP	UDP	NetBIOS Name Service, used for name registration and resolution
138	Assigned	UDP	NetBIOS Datagram Service
139	TCP	Assigned	NetBIOS Session Service
143	TCP	Assigned	Internet Message Access Protocol (IMAP), advanced email operation protocol
153	TCP	UDP	Simple Gateway Monitoring Protocol (SGMP)
161	Assigned	UDP	Simple Network Management Protocol (SNMP)
162	TCP	UDP	Simple Network Management Protocol Trap (SNMPTRAP)
177	TCP	UDP	X Display Manager Control Protocol (XDMCP), used for remote logins to an X Display Manager server
179	TCP	Assigned	Border Gateway Protocol (BGP), used to exchange routing and reachability information
194	TCP	UDP	Internet Relay Chat (IRC)
220	TCP	UDP	Internet Message Access Protocol (IMAP), version 3 ***(Note: See ports 143 and 993)***
264	TCP	UDP	Border Gateway Multicast Protocol (BGMP)
389	TCP	Assigned	Lightweight Directory Access Protocol (LDAP) ***(Note: See Port 636 LDAP over SSL)***
399	TCP	UDP	Digital Equipment Corporation DECnet (Phase V+) over TCP/IP
401	TCP	UDP	Uninterruptible power supply (UPS)
427	TCP	UDP	Service Location Protocol (SLP)
433	TCP	UDP	NNSP, part of Network News Transfer Protocol
443	TCP	Assigned	Web Services Hypertext Transfer Protocol over TLS/SSL (HTTPS)
445	TCP	Assigned	Microsoft SMB file sharing, also used by Active Directory services
464	TCP	UDP	Kerberos Change/Set password
465	TCP		Authenticated SMTP over TLS/SSL (SMTPS)
500	Assigned	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)
502	TCP	UDP	Modbus Protocol
512	TCP		Rexec, Remote Process Execution
513	TCP		rlogin
514		UDP	Syslog, used for system logging ***(See note on port 601 Rsyslog)***
520		UDP	Routing Information Protocol (RIP)
521		UDP	Routing Information Protocol Next Generation (RIPng)
530	TCP	UDP	Remote procedure call (RPC)
540	TCP		Unix-to-Unix Copy Protocol (UUCP)
542	TCP	UDP	commerce (Commerce Applications)
543	TCP		klogin, Kerberos login
544	TCP		kshell, Kerberos Remote shell
546, 547	TCP	UDP	DHCPv6: client uses Port 546, server uses Port 547
554	TCP	UDP	Real Time Streaming Protocol (RTSP)
593	TCP	UDP	RPC over HTTP, often used by DCOM services and MS Exchange Server
601	TCP		Reliable Syslog Service, used for system logging (***Note: More usually on port 514)***
636	TCP	Assigned	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
646	TCP	UDP	Label Distribution Protocol (LDP), a routing protocol used in MPLS networks
647	TCP		DHCP Failover protocol
657	TCP	UDP	IBM RMC (Remote Monitoring & Control) used by System p5 AIX Integrated Virtualization Manager
660	TCP	Assigned	Mac OS X Server administration, version 10.4 and earlier

Well-Known/System Port Numbers contd.

Port	TCP	UDP	Description
691	TCP		Microsoft Exchange Routing Engine (RESvc) listens for routing link state information on TCP port 691
694	TCP	UDP	Linux-HA high-availability heartbeat
698		UDP	Optimized Link State Routing (OLSR)
711	TCP		Cisco Tag Distribution Protocol—being replaced by the MPLS Label Distribution Protocol
829	TCP	Assigned	Certificate Management Protocol
830-833	TCP	UDP	NETCONF: SSH Port 830, BEEP Port 831, SOAP/HTTPS Port 832, SOAP/HTTP Port 833
847	TCP		DHCP Failover protocol
848	TCP	UDP	Group Domain Of Interpretation (GDOI) protocol
853	TCP	UDP	DNS over TLS (RFC 7858)
860	TCP		iSCSI (RFC 3720)
873	TCP		rsync file synchronization protocol
953	TCP	Reserved	BIND remote name daemon control (RNDC)
989-990	TCP	UDP	FTP over TLS/SSL: Data Port uses 989, Control Port uses 990
993	TCP	UDP	Internet Message Access Protocol (IMAP) over SSL
995	TCP	UDP	Post Office Protocol 3 over TLS/SSL (POP3S)

Registered Ports

Port	TCP	UDP	Description
1027		UDP	Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment (6a44)
1058, 1059	TCP	UDP	IBM AIX Network Installation Manager (NIM)
1080	TCP	UDP	SOCKS proxy
1085	TCP	UDP	WebObjects
1098, 1099	TCP	UDP	Java remote method invocation (RMI): Activation uses Port 1098, Registry uses Port 1099
1167	TCP and SCTP	UDP	Cisco IP SLA (Service Assurance Agent)
1194	TCP	UDP	OpenVPN
1198	TCP	UDP	The cajo project Free dynamic transparent distributed computing in Java
1220	TCP	Assigned	QuickTime Streaming Server administration
1234	TCP	UDP	Infoseek search agent
1270	TCP	UDP	Microsoft System Center Operations Manager (SCOM) (formerly MS Operations Manager (MOM)) agent
1293	TCP	UDP	Internet Protocol Security (IPSec)
1311	TCP	UDP	Windows RxMon.exe
1341	TCP	UDP	Qubes (Manufacturing Execution System)
1344	TCP	UDP	Internet Content Adaptation Protocol
1352	TCP	UDP	IBM Lotus Notes/Domino (RPC) protocol
1414	TCP	UDP	IBM WebSphere MQ (formerly known as MQSeries)
1431	TCP		Reverse Gossip Transport Protocol (RGTP)
1433, 1444	TCP	UDP	Microsoft SQL Server database management system (MSSQL): Server uses Port 1433, Monitor uses Port 1434
1512	TCP	UDP	Microsoft's Windows Internet Name Service (WINS)
1524	TCP	UDP	ingreslock, ingres
1527	TCP	UDP	Oracle Net Services, formerly known as SQL*Net
1533	TCP	UDP	IBM Sametime Virtual Places Chat
1701	TCP	UDP	Layer 2 Forwarding Protocol (L2F)
1701	Assigned	UDP	Layer 2 Tunneling Protocol (L2TP)
1719-1720	TCP	UDP	H.323 registration and call signaling
1723	TCP	Assigned	Point-to-Point Tunneling Protocol (PPTP)
1755	TCP	UDP	Microsoft Media Services (MMS, ms-streaming)
1801	TCP	UDP	Microsoft Message Queuing
1812-1813	TCP	UDP	RADIUS: Authentication protocol Port 1812, Accounting protocl Port 1813
1863	TCP	UDP	Microsoft Notification Protocol (MSNP), used by Microsoft Messenger service and other IM clients
1883	TCP	UDP	MQTT (formerly MQ Telemetry Transport)
1900	Assigned	UDP	Simple Service Discovery Protocol (SSDP), discovery of UPnP devices
1985	Assigned	UDP	Cisco Hot Standby Router Protocol (HSRP)
2049	TCP and SCTP	UDP	Network File System (NFS)
2080	TCP	UDP	Autodesk NLM (FLEXlm)
2083	TCP	UDP	Secure RADIUS Service (radsec)
2095	TCP		cPanel default web mail
2222, 2223	TCP		ESET Remote administrator
2375, 2376	TCP	Reserved	Docker REST API
2377	TCP	Reserved	Docker Swarm cluster management communications
2379, 2380	TCP	Reserved	CoreOS etcd: Client communication Port 2379, Server communication Port 2380
2401	TCP	UDP	CVS version control system password-based server
2427	TCP	UDP	Media Gateway Control Protocol (MGCP) media gateway
2483, 2484	TCP	UDP	Oracle database listener
2535	TCP	UDP	Multicast Address Dynamic Client Allocation Protocol (MADCAP). All standard messages are UDP
2546, 2548	TCP	UDP	EVault data protection services
2638	TCP	UDP	SQL Anywhere database server
2727	TCP	UDP	Media Gateway Control Protocol (MGCP) media gateway controller (call agent)

Well-Known/System Port Numbers contd.

Port	TCP	UDP	Description
2967	TCP	UDP	Symantec System Center agent (SSC-AGENT)
3020	TCP	UDP	Common Internet File System (CIFS), see also port 445 for Server Message Block, a dialect of CIFS
3050	TCP	UDP	gds-db (Interbase/Firebird databases)
3052	TCP	UDP	APC PowerChute Network
3225	TCP	UDP	Fibre Channel over IP (FCIP)
3233	TCP	UDP	WhiskerControl research control protocol
3260	TCP	UDP	iSCSI
3306	TCP	Assigned	MySQL database system
3389	TCP	UDP	Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT)
3412	TCP	UDP	xmlBlaster
3455	TCP	UDP	Resource Reservation Protocol (RSVP)
3478	TCP	UDP	STUN, a protocol for NAT traversal
3493	TCP	UDP	Network UPS Tools (NUT)
3516	TCP	UDP	Smartcard Port
3527		UDP	Microsoft Message Queuing
3544		UDP	Teredo tunneling
3632	TCP	Assigned	Distcc, distributed compiler
3690	TCP	UDP	Subversion (SVN) version control system
3872	TCP		Oracle Enterprise Manager Remote Agent
4739	TCP	UDP	IP Flow Information Export
4789		UDP	Virtual eXtensible Local Area Network (VXLAN)
5004, 5005	TCP	UDP	Real-time Transport Protocol: Media data (RTP) (RFC 3551, RFC 4571) Port 5004, Control Protocol Port 5005
5060, 5061	TCP	UDP	Session Initiation Protocol (SIP)
5093, 5099	TCP	UDP	SafeNet, Inc Sentinel LM/Sentinel RMS/License Manager: Client comms Port 5093, Server comms Port 5099
5222	TCP	Reserved	Extensible Messaging and Presence Protocol (XMPP) client connection
5405	TCP	UDP	NetSupport Manager Tutor Console uses port 5405 (TCP and UDP) to Browse and connect to Students
5412	TCP	UDP	IBM Rational Synergy (Telelogic Synergy) (Continuus CM) Message Router
5413	TCP	UDP	Wonderware SuiteLink service
5421	TCP	UDP	NetSupport Manager Tutor Console uses port 5421 for the Multicast\Broadcast Show and File Distribution features
5514	TCP		NNT Log Tracker remote agent configuration channel
5432	TCP	Assigned	PostgreSQL database system
5631-5632	TCP	UDP	pcANYWHEREdata, Symantec pcAnywhere (version 7.52 and later)
5671-5672	TCP	Assigned	Advanced Message Queuing Protocol (AMQP)
5722	TCP	UDP	Microsoft RPC, DFSR (SYSVOL) Replication Service[citation needed]
5985-5986	TCP		HTTP/HTTPSWindows PowerShell Default psSession
6000–6063	TCP	UDP	X11—used between an X client and server over the network
6343		UDP	SFlow, sFlow traffic monitoring
6379	TCP		Redis key-value data store
6513	TCP		NETCONF over TLS
6514	TCP		Syslog over TLS
6515	TCP	UDP	Elipse RPC Protocol (REC)
6566	TCP		SANE (Scanner Access Now Easy)—SANE network scanner daemon
6600	TCP		Microsoft Hyper-V Live
6601	TCP		Microsoft Forefront Threat Management Gateway
6602	TCP		Microsoft Windows WSS Communication
6665-6669	TCP		Internet Relay Chat (IRC) uses ports 6665, 6666, 6667, 6668 & 6669
6679, 6697	TCP		IRC SSL (Secure Internet Relay Chat)—often used
7400-7402	TCP	UDP	RTPS (Real Time Publish Subscribe) DDS uses ports 7400, 7401 & 7402
8140	TCP		Puppet (software) Master server
8243, 8280	TCP	UDP	Apache Synapse
11112	TCP	UDP	ACR/NEMA Digital Imaging and Communications in Medicine (DICOM)
11371	TCP	UDP	OpenPGP HTTP key server
12222-12223		UDP	Light Weight Access Point Protocol (LWAPP) LWAPP data (RFC 5412)
13075	TCP		Default for BMC Software Control-M/Enterprise Manager Corba communication
13724	TCP	UDP	Symantec Veritas NetBackup master server
20000		UDP	Google Voice via OBiTalk ATA devices, also MagicJack & Vonage ATA devices
27000–27009	TCP	UDP	FlexNet Publisher's License server default ports 27000,27001,27002,27003,27004,27005,27006,27007,27008,27009
27017	TCP		MongoDB daemon process (mongod) and routing service (mongos)
33434	TCP	UDP	traceroute
35357	TCP		OpenStack Identity (Keystone) administration
40000	TCP	UDP	SafetyNET p – a real-time Industrial Ethernet protocol
44818	TCP	UDP	EtherNet/IP explicit messaging
47001	TCP		Windows Remote Management Service (WinRM)

Dynamic/Ephemeral ports

The range 49152–65535 contains dynamic or private ports used for private or customized services, for temporary purposes, and for automatic allocation of ephemeral ports.

Conclusion - The NNT View

Security hardening is always a balance between maximizing security and delivering the required functions for a platform. Put simply, the more functions provided by a platform, the greater the opportunity for attack, because any functionality has the potential to be misused and abused.

Open ports are significant within this because any network-based attack must utilize network-accessible services, so its a logical way to measure the attack surface of a platform.

But the risk of such a linear interpretation of this objective is that other more straightforward hardening practices may be overlooked. NNT technology will provide you with not just simple to use tools for identifying and tracking changes to open ports, but as a matter of course encompass visibility of all other key vulnerability considerations.

This includes the analysis of

- running services and their startup states
- installed software and related known vulnerabilities
- security-related configuration settings
- any new and changed system files

NNT Secure Ops® automates these functions for you within the context of your day-to-day IT Service Operations to maintain security and expose breach activity. Even in a dynamic enterprise where security threats would otherwise remain hidden, NNT can cut out the change noise to clearly identify security issues.

About New Net Technologies (NNT)

New Net Technologies (NNT) is the leading provider of Secure Ops®, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance.

NNT delivers its Secure Ops® suite by combining:

- System Configuration Hardening
- Closed Loop Change Control
- Vulnerability Management and
- Event Log Management

These core security disciplines are defined by the Center for Internet Security and the SANS Institute as the essential Critical Security Controls for any cyber security initiative. For more information, visit www.newnettechnologies.com

TO REQUEST A FREE TRIAL OR DISCUSS ANY AREA COVERED IN THIS WHITEPAPER, PLEASE CONTACT US AT info@nntws.com