NetCertScanner

Universal Network Based SSL Certificate Scanner Software

NetCertScanner Feature Guide

Contents

- About NetCertScanner
- Benefits of NetCertScanner
- Features of NetCertScanner
- Special Features of Console Version
- Screenshots of NetCertScanner
- System Requirements
- Contact Information

About NetCertScanner

Website: http://xenarmor.com/network-ssl-certificate-scanner.php

Short line: Universal Network Based SSL Certificate Scanner

Description:

NetCertScanner is the enterprise software to scan & manage expired SSL Certificates on your local network or internet. Its swift SSL Certificate scan powered by 'Host-Port Multiplexed Multithreading' technique helps you to scan the entire network in just few minutes.

Along with this, it also boasts of other special features like Smarter SSL Cert Analysis, Hidden SSL Port Scan, Color based Display, Database Integration, Console Version, HTML/CSV Scan Report etc. making it a unique product in the universe.

Benefits of NetCertScanner

NetCertScanner helps you to instantly find expired SSL Certificates on your local Intranet or Internet with just one click. It is very useful to keep track of SSL certificates which are about to expire and then replace them before hosted services are disrupted causing potential embarrassment & financial losses to the organization.

Here are the major benefits of NetCertScanner

- **Save Precious Time:** Quickly scan all your SSL Servers on Intranet or Internet with just One Click.
- **Stay on the Job:** Find the Expired or Self-Signed SSL Certificates well in advance
- **Stay Alert:** Find out any Rogue/Unauthorized/Dummy SSL servers in your Network
- **Be Smarter than Attacker:** Detect the sophisticated 'Man in the Middle' (MITM) Attacks happening right under your nose. Any Server with self signed/rogue SSL Certificate is indication of possible MITM attack
- **Stay Secure:** Make sure your 'Secure Online Transaction' is really secure beforehand. Quickly verify the web server using NetCertScanner to make sure it's SSL certificate is VALID and not Self-Signed or Expired.

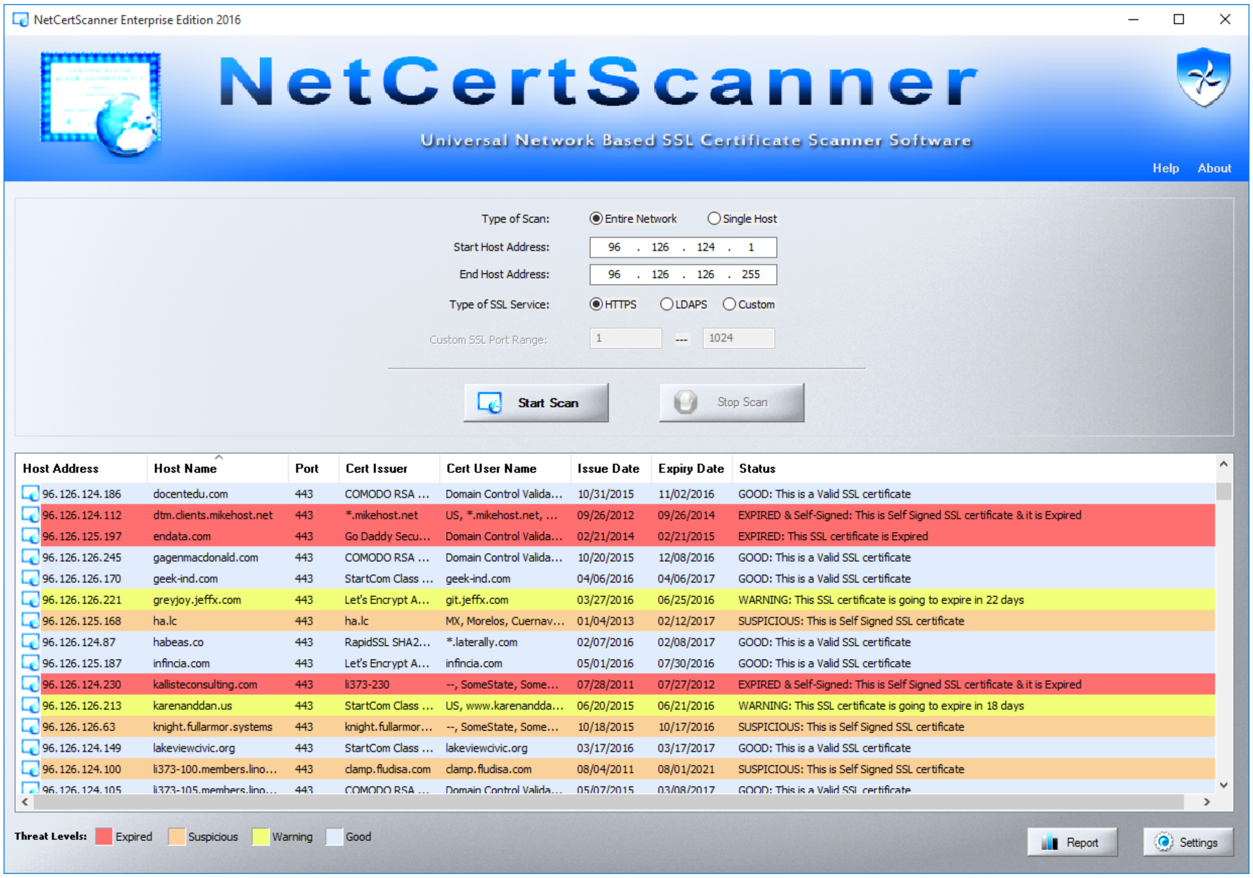
Key Features of NetCertScanner

- ✓ Swift SSL Scanning Operation using 'Host-Port Multiplexed Multithreading' Technique
- ✓ 'Universal SSL Scanner' based unique method of retrieving SSL Certificate from Remote Host
- ✓ Supports both HTTP-SSL (443) and LDAP-SSL (636) Services on Local Network or Internet
- ✓ Scan entire Local Network (*.*.0.0/16) or 256x256 Hosts in one go
- ✓ Hidden SSL Port Scanning feature using Brute-force method
- ✓ Smart SSL Certificate Analysis (Expired/Self-signed Certs)
- ✓ Special 'Warning Note' for the SSL Certificates that are about to Expire in a month
- ✓ Color based Display of SSL Certificate Results (warning/expired/self-signed etc)
- ✓ Console/Command-Line version for Automation of SSL Scanning operation
- ✓ File based IP List Scanning [Console Version]
- ✓ Generate SSL Certificate Scan Report in both HTML/CSV format
- ✓ Database integration with Microsoft SQL Server to Auto-store Certificate Scan results
- ✓ View complete SSL Certificate [requires Database integration]
- ✓ Fully Portable, does not require Java, .NET or any other Components

Special Features of NetCertScanner Console Version

- ✓ Facilitate automation of entire SSL Certificate scanning operation.
- ✓ Support for Scanning of specific IP addresses from input ‘IP List File’ - making it faster & efficient.
- ✓ Automatically takes settings configured through NetCertScanner GUI version.
- ✓ Complete support for database integration as in NetCertScanner GUI version.

Screenshots of NetCertScanner

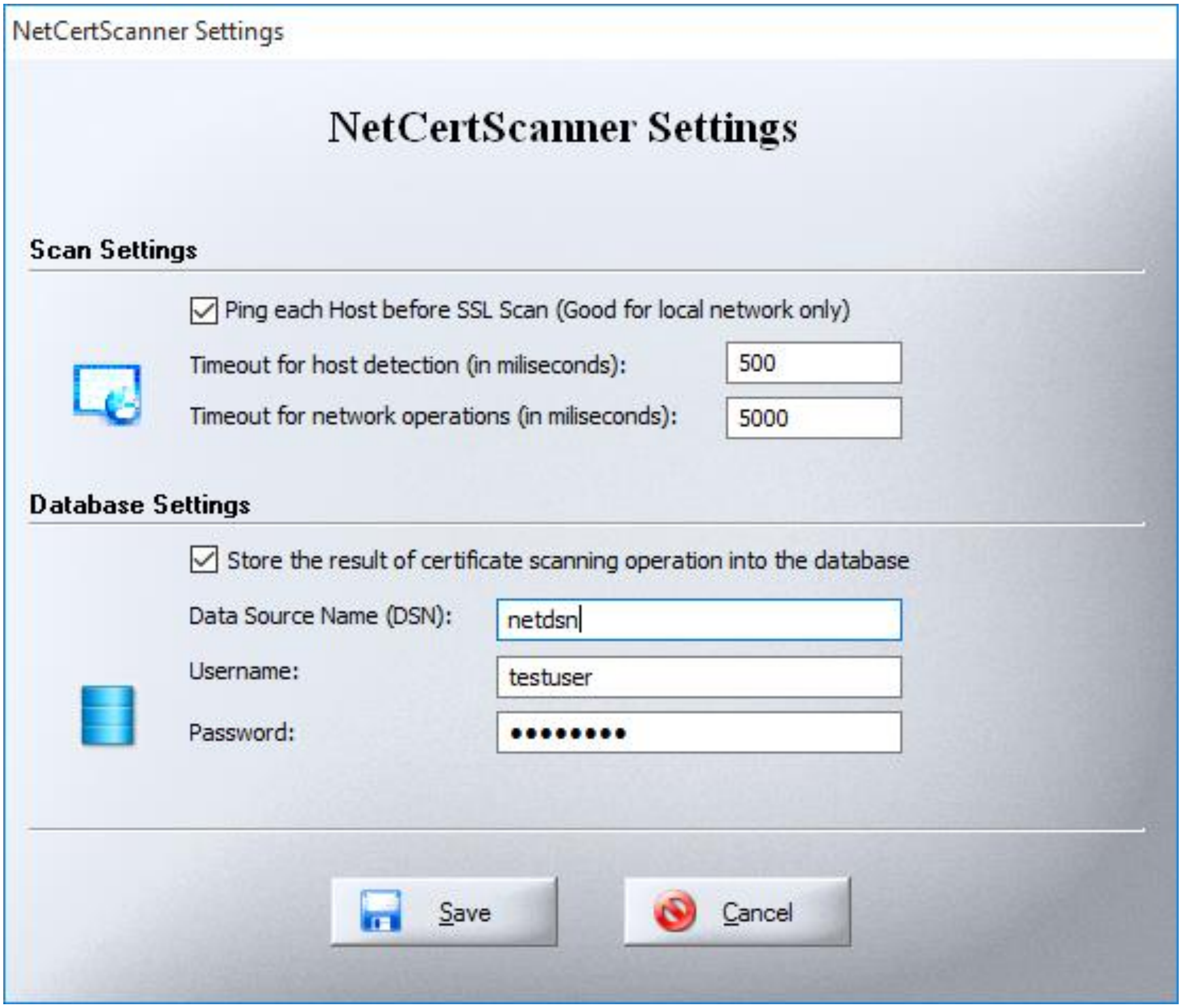

NetCertScanner Enterprise Edition 2016
NetCertScanner
Universal Network Based SSL Certificate Scanner Software
Help
About
Start Scan
Stop Scan
Report
Settings

Type of Scan: ● Entire Network ○ Single Host
Start Host Address: 96 . 126 . 124 . 1
End Host Address: 96 . 126 . 126 . 255
Type of SSL Service: ● HTTPS ○ LDAPS ○ Custom
Custom SSL Port Range: 1 --- 1024

Host Address	Host Name	Port	Cert Issuer	Cert User Name	Issue Date	Expiry Date	Status
96.126.124.186	docentedu.com	443	COMODO RSA ...	Domain Control Valida...	10/31/2015	11/02/2016	GOOD: This is a Valid SSL certificate
96.126.124.112	dtm.clients.mikehost.net	443	*.mikehost.net	US, *.mikehost.net, ...	09/26/2012	09/26/2014	EXPIRED & Self-Signed: This is Self Signed SSL certificate & it is Expired
96.126.125.197	endata.com	443	Go Daddy Secu...	Domain Control Valida...	02/21/2014	02/21/2015	EXPIRED: This SSL certificate is Expired
96.126.126.245	gagenmacdonald.com	443	COMODO RSA ...	Domain Control Valida...	10/20/2015	12/08/2016	GOOD: This is a Valid SSL certificate
96.126.126.170	geek-ind.com	443	StartCom Class ...	geek-ind.com	04/06/2016	04/06/2017	GOOD: This is a Valid SSL certificate
96.126.126.221	greyjoy.jeffx.com	443	Let's Encrypt A...	git.jeffx.com	03/27/2016	06/25/2016	WARNING: This SSL certificate is going to expire in 22 days
96.126.125.168	ha.lc	443	ha.lc	MX, Morelos, Cuernav...	01/04/2013	02/12/2017	SUSPICIOUS: This is Self Signed SSL certificate
96.126.124.87	habeas.co	443	RapidSSL SHA2...	*.laterally.com	02/07/2016	02/08/2017	GOOD: This is a Valid SSL certificate
96.126.125.187	infincia.com	443	Let's Encrypt A...	infincia.com	05/01/2016	07/30/2016	GOOD: This is a Valid SSL certificate
96.126.124.230	kallisteconsulting.com	443	li373-230	--, SomeState, Some...	07/28/2011	07/27/2012	EXPIRED & Self-Signed: This is Self Signed SSL certificate & it is Expired
96.126.126.213	karenanddan.us	443	StartCom Class ...	US, www.karenandda...	06/20/2015	06/21/2016	WARNING: This SSL certificate is going to expire in 18 days
96.126.126.63	knight.fullarmor.systems	443	knight.fullarmor...	--, SomeState, Some...	10/18/2015	10/17/2016	SUSPICIOUS: This is Self Signed SSL certificate
96.126.124.149	lakeviewcivic.org	443	StartCom Class ...	lakeviewcivic.org	03/17/2016	03/17/2017	GOOD: This is a Valid SSL certificate
96.126.124.100	li373-100.members.lino...	443	clamp.fludisa.com	clamp.fludisa.com	08/04/2011	08/01/2021	SUSPICIOUS: This is Self Signed SSL certificate
96.126.124.105	li373-105.members.lino...	443	COMODO RSA ...	Domain Control Valida...	05/07/2015	03/08/2017	GOOD: This is a Valid SSL certificate

Threat Levels: 🟥 Expired 🟧 Suspicious 🟨 Warning ⬜ Good

Figure 1: NetCertScanner Scanning for HTTP SSL certificates on the Internet. As you can see Valid SSL certificates are shown in BLUE while Expired/Self-Signed certificates are shown in RED/Saffron color for easier and quicker identification. SSL Certificates that are going to expire in a month are shown in YELLOW color.



NetCertScanner Settings

NetCertScanner Settings

Scan Settings

☑ Ping each Host before SSL Scan (Good for local network only)

Timeout for host detection (in miliseconds): 500

Timeout for network operations (in miliseconds): 5000

Database Settings

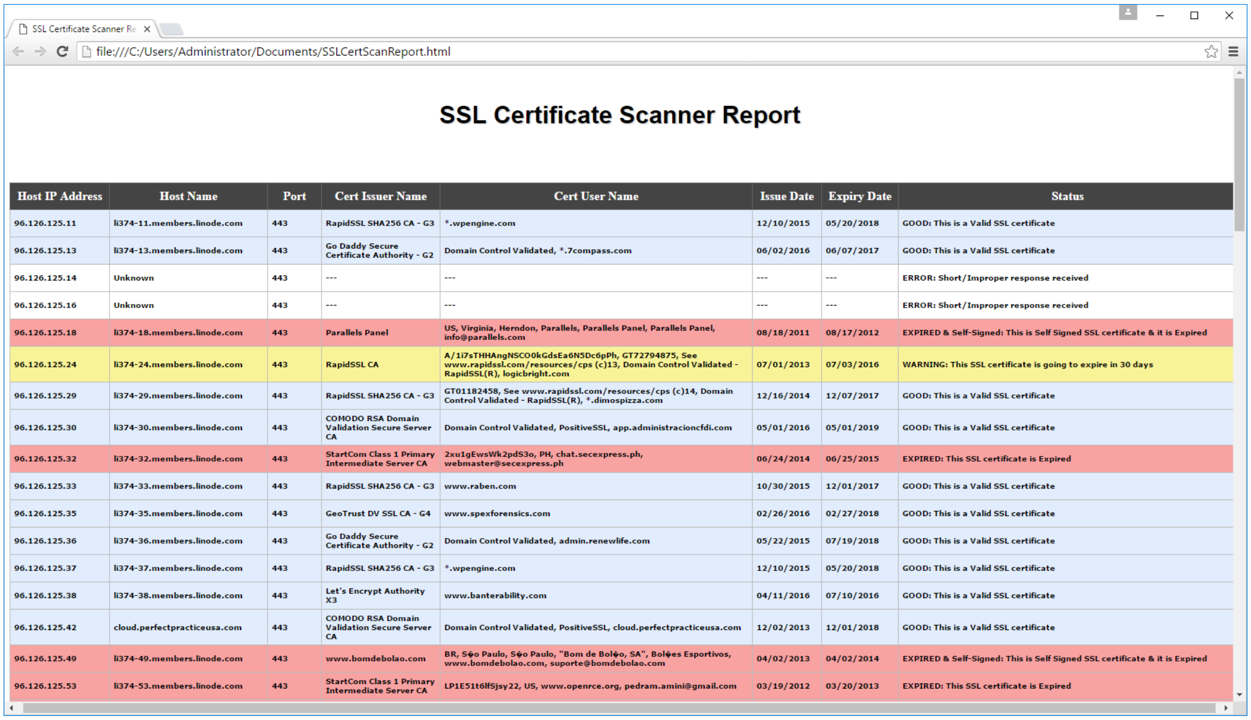
☑ Store the result of certificate scanning operation into the database

Data Source Name (DSN): netdsn

Username: testuser

Password: ●●●●●●●●●

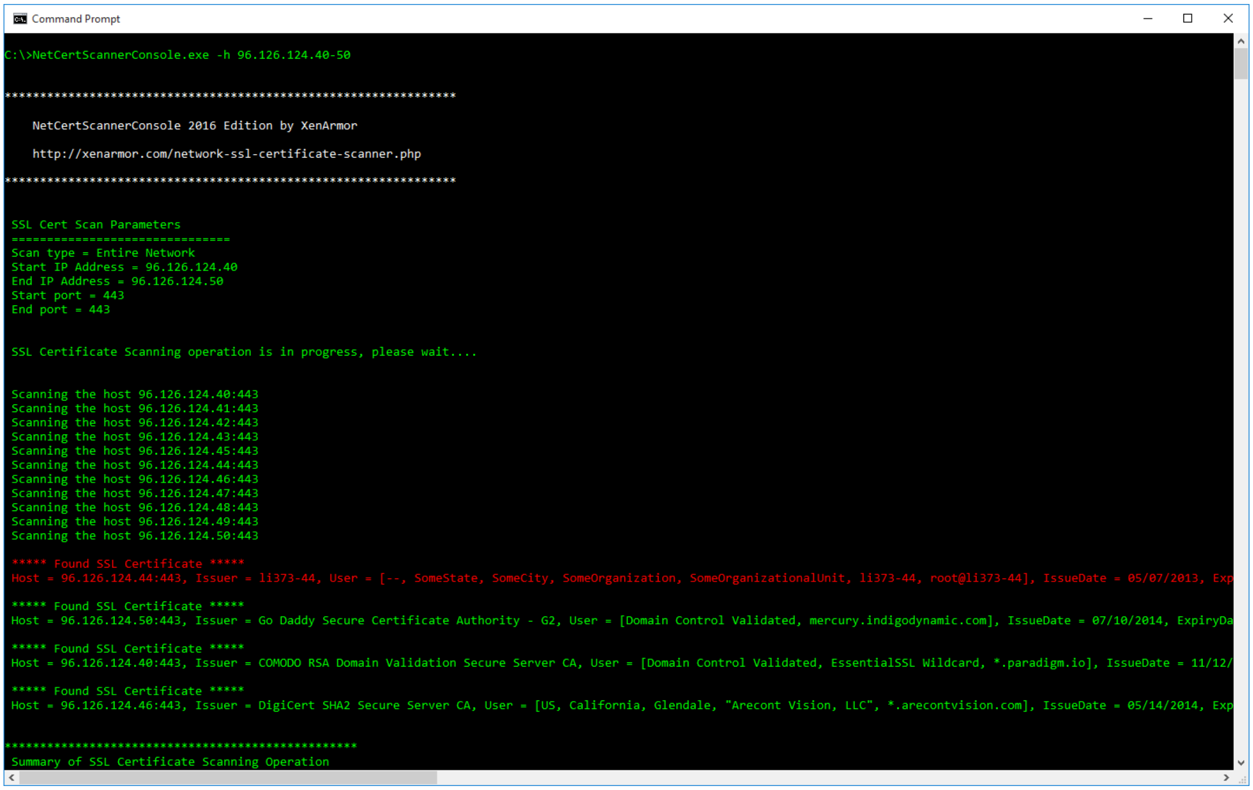
Figure 2: NetCertScanner's Settings Wizard to help you in fine tuning the Scanning performance, & Database related configuration.


SSL Certificate Scanner Re
file:///C:/Users/Administrator/Documents/SSLCertScanReport.html

SSL Certificate Scanner Report

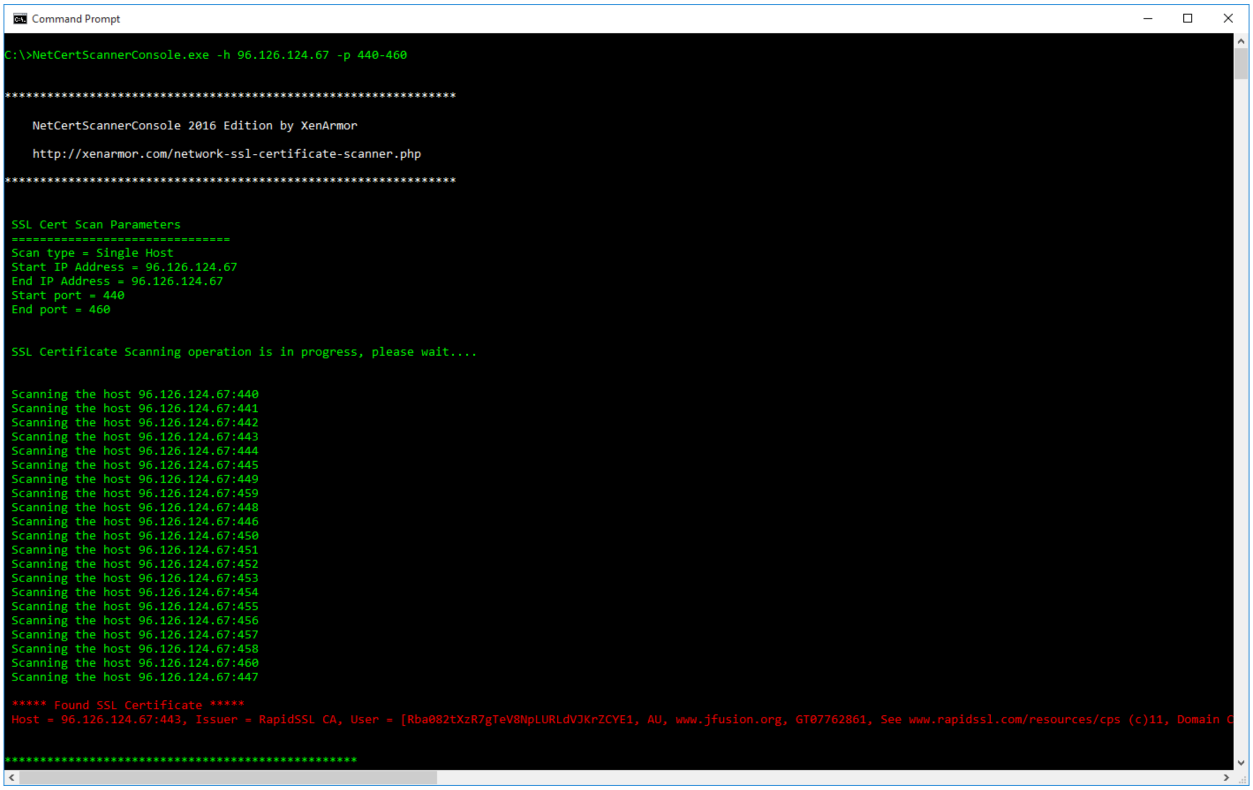
Host IP Address	Host Name	Port	Cert Issuer Name	Cert User Name	Issue Date	Expiry Date	Status
96.126.125.11	li374-11.members.linode.com	443	RapidSSL SHA256 CA - G3	*.wpengine.com	12/10/2015	05/20/2018	GOOD: This is a Valid SSL certificate
96.126.125.13	li374-13.members.linode.com	443	Go Daddy Secure Certificate Authority - G2	Domain Control Validated, *.7compass.com	06/02/2016	06/07/2017	GOOD: This is a Valid SSL certificate
96.126.125.14	Unknown	443	---	---	---	---	ERROR: Short/Improper response received
96.126.125.16	Unknown	443	---	---	---	---	ERROR: Short/Improper response received
96.126.125.18	li374-18.members.linode.com	443	Parallels Panel	US, Virginia, Herndon, Parallels, Parallels Panel, Parallels Panel, info@parallels.com	08/18/2011	08/17/2012	EXPIRED & Self-Signed: This is Self Signed SSL certificate & it is Expired
96.126.125.24	li374-24.members.linode.com	443	RapidSSL CA	A/1i7sTHHAngNSCO0kGdsEa6N5Dc6pPh, GT72794875, See www.rapidssl.com/resources/cps (c)13, Domain Control Validated - RapidSSL(R), logicbright.com	07/01/2013	07/03/2016	WARNING: This SSL certificate is going to expire in 30 days
96.126.125.29	li374-29.members.linode.com	443	RapidSSL SHA256 CA - G3	GT01182458, See www.rapidssl.com/resources/cps (c)14, Domain Control Validated - RapidSSL(R), *.dimospizza.com	12/16/2014	12/07/2017	GOOD: This is a Valid SSL certificate
96.126.125.30	li374-30.members.linode.com	443	COMODO RSA Domain Validation Secure Server CA	Domain Control Validated, PositiveSSL, app.administracioncfdi.com	05/01/2016	05/01/2019	GOOD: This is a Valid SSL certificate
96.126.125.32	li374-32.members.linode.com	443	StartCom Class 1 Primary Intermediate Server CA	2xu1gEwsWk2pdS3o, PH, chat.secexpress.ph, webmaster@secexpress.ph	06/24/2014	06/25/2015	EXPIRED: This SSL certificate is Expired
96.126.125.33	li374-33.members.linode.com	443	RapidSSL SHA256 CA - G3	www.raben.com	10/30/2015	12/01/2017	GOOD: This is a Valid SSL certificate
96.126.125.35	li374-35.members.linode.com	443	GeoTrust DV SSL CA - G4	www.spexforensics.com	02/26/2016	02/27/2018	GOOD: This is a Valid SSL certificate
96.126.125.36	li374-36.members.linode.com	443	Go Daddy Secure Certificate Authority - G2	Domain Control Validated, admin.renewlife.com	05/22/2015	07/19/2018	GOOD: This is a Valid SSL certificate
96.126.125.37	li374-37.members.linode.com	443	RapidSSL SHA256 CA - G3	*.wpengine.com	12/10/2015	05/20/2018	GOOD: This is a Valid SSL certificate
96.126.125.38	li374-38.members.linode.com	443	Let's Encrypt Authority X3	www.banterability.com	04/11/2016	07/10/2016	GOOD: This is a Valid SSL certificate
96.126.125.42	cloud.perfectpracticeusa.com	443	COMODO RSA Domain Validation Secure Server CA	Domain Control Validated, PositiveSSL, cloud.perfectpracticeusa.com	12/02/2013	12/01/2018	GOOD: This is a Valid SSL certificate
96.126.125.49	li374-49.members.linode.com	443	www.bomdebolao.com	BR, S�o Paulo, S�o Paulo, "Bom de Bol�o, SA", Bol�es Esportivos, www.bomdebolao.com, suporte@bomdebolao.com	04/02/2013	04/02/2014	EXPIRED & Self-Signed: This is Self Signed SSL certificate & it is Expired
96.126.125.53	li374-53.members.linode.com	443	StartCom Class 1 Primary Intermediate Server CA	LP1E51t6lfSjsy22, US, www.openrce.org, pedram.amini@gmail.com	03/19/2012	03/20/2013	EXPIRED: This SSL certificate is Expired

Figure 3: HTML based SSL Certificate Scanning Report generated by NetCertScanner.



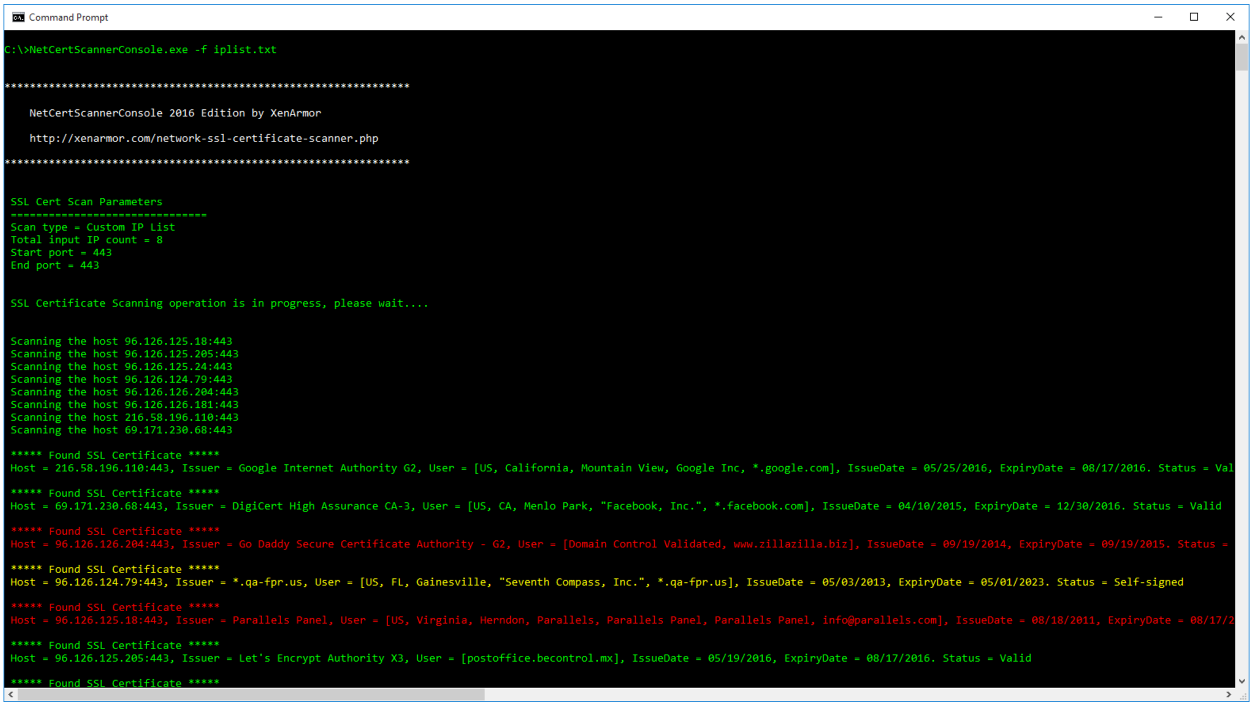
```
C:\>NetCertScannerConsole.exe -h 96.126.124.40-50


****************************************************************

    NetCertScannerConsole 2016 Edition by XenArmor

    http://xenarmor.com/network-ssl-certificate-scanner.php

****************************************************************


 SSL Cert Scan Parameters
 ===============================
 Scan type = Entire Network
 Start IP Address = 96.126.124.40
 End IP Address = 96.126.124.50
 Start port = 443
 End port = 443


 SSL Certificate Scanning operation is in progress, please wait....


 Scanning the host 96.126.124.40:443
 Scanning the host 96.126.124.41:443
 Scanning the host 96.126.124.42:443
 Scanning the host 96.126.124.43:443
 Scanning the host 96.126.124.45:443
 Scanning the host 96.126.124.44:443
 Scanning the host 96.126.124.46:443
 Scanning the host 96.126.124.47:443
 Scanning the host 96.126.124.48:443
 Scanning the host 96.126.124.49:443
 Scanning the host 96.126.124.50:443

 ***** Found SSL Certificate *****
 Host = 96.126.124.44:443, Issuer = li373-44, User = [--, SomeState, SomeCity, SomeOrganization, SomeOrganizationalUnit, li373-44, root@li373-44], IssueDate = 05/07/2013, Exp

 ***** Found SSL Certificate *****
 Host = 96.126.124.50:443, Issuer = Go Daddy Secure Certificate Authority - G2, User = [Domain Control Validated, mercury.indigodynamic.com], IssueDate = 07/10/2014, ExpiryDa

 ***** Found SSL Certificate *****
 Host = 96.126.124.40:443, Issuer = COMODO RSA Domain Validation Secure Server CA, User = [Domain Control Validated, EssentialSSL Wildcard, *.paradigm.io], IssueDate = 11/12/

 ***** Found SSL Certificate *****
 Host = 96.126.124.46:443, Issuer = DigiCert SHA2 Secure Server CA, User = [US, California, Glendale, "Arecont Vision, LLC", *.arecontvision.com], IssueDate = 05/14/2014, Exp


**************************************************
 Summary of SSL Certificate Scanning Operation
```

Figure 4: SSL Certificate scanning on the network from NetCertScanner Console version.



```
C:\>NetCertScannerConsole.exe -h 96.126.124.67 -p 440-460


****************************************************************

    NetCertScannerConsole 2016 Edition by XenArmor

    http://xenarmor.com/network-ssl-certificate-scanner.php

****************************************************************


 SSL Cert Scan Parameters
 ===============================
 Scan type = Single Host
 Start IP Address = 96.126.124.67
 End IP Address = 96.126.124.67
 Start port = 440
 End port = 460


 SSL Certificate Scanning operation is in progress, please wait....


 Scanning the host 96.126.124.67:440
 Scanning the host 96.126.124.67:441
 Scanning the host 96.126.124.67:442
 Scanning the host 96.126.124.67:443
 Scanning the host 96.126.124.67:444
 Scanning the host 96.126.124.67:445
 Scanning the host 96.126.124.67:449
 Scanning the host 96.126.124.67:459
 Scanning the host 96.126.124.67:448
 Scanning the host 96.126.124.67:446
 Scanning the host 96.126.124.67:450
 Scanning the host 96.126.124.67:451
 Scanning the host 96.126.124.67:452
 Scanning the host 96.126.124.67:453
 Scanning the host 96.126.124.67:454
 Scanning the host 96.126.124.67:455
 Scanning the host 96.126.124.67:456
 Scanning the host 96.126.124.67:457
 Scanning the host 96.126.124.67:458
 Scanning the host 96.126.124.67:460
 Scanning the host 96.126.124.67:447

 ***** Found SSL Certificate *****
 Host = 96.126.124.67:443, Issuer = RapidSSL CA, User = [Rba082tXzR7gTeV8NpLURLdVJKrZCYE1, AU, www.jfusion.org, GT07762861, See www.rapidssl.com/resources/cps (c)11, Domain C


**************************************************
```

Figure 5: Custom SSL Port Scanning from NetCertScanner Console Version.



```
C:\>NetCertScannerConsole.exe -f iplist.txt


****************************************************************

    NetCertScannerConsole 2016 Edition by XenArmor

    http://xenarmor.com/network-ssl-certificate-scanner.php

****************************************************************


 SSL Cert Scan Parameters
 ===============================
 Scan type = Custom IP List
 Total input IP count = 8
 Start port = 443
 End port = 443


 SSL Certificate Scanning operation is in progress, please wait....


 Scanning the host 96.126.125.18:443
 Scanning the host 96.126.125.205:443
 Scanning the host 96.126.125.24:443
 Scanning the host 96.126.124.79:443
 Scanning the host 96.126.126.204:443
 Scanning the host 96.126.126.181:443
 Scanning the host 216.58.196.110:443
 Scanning the host 69.171.230.68:443

 ***** Found SSL Certificate *****
 Host = 216.58.196.110:443, Issuer = Google Internet Authority G2, User = [US, California, Mountain View, Google Inc, *.google.com], IssueDate = 05/25/2016, ExpiryDate = 08/17/2016. Status = Val

 ***** Found SSL Certificate *****
 Host = 69.171.230.68:443, Issuer = DigiCert High Assurance CA-3, User = [US, CA, Menlo Park, "Facebook, Inc.", *.facebook.com], IssueDate = 04/10/2015, ExpiryDate = 12/30/2016. Status = Valid

 ***** Found SSL Certificate *****
 Host = 96.126.126.204:443, Issuer = Go Daddy Secure Certificate Authority - G2, User = [Domain Control Validated, www.zillazilla.biz], IssueDate = 09/19/2014, ExpiryDate = 09/19/2015. Status =

 ***** Found SSL Certificate *****
 Host = 96.126.124.79:443, Issuer = *.qa-fpr.us, User = [US, FL, Gainesville, "Seventh Compass, Inc.", *.qa-fpr.us], IssueDate = 05/03/2013, ExpiryDate = 05/01/2023. Status = Self-signed

 ***** Found SSL Certificate *****
 Host = 96.126.125.18:443, Issuer = Parallels Panel, User = [US, Virginia, Herndon, Parallels, Parallels Panel, Parallels Panel, info@parallels.com], IssueDate = 08/18/2011, ExpiryDate = 08/17/2

 ***** Found SSL Certificate *****
 Host = 96.126.125.205:443, Issuer = Let's Encrypt Authority X3, User = [postoffice.becontrol.mx], IssueDate = 05/19/2016, ExpiryDate = 08/17/2016. Status = Valid

 ***** Found SSL Certificate *****
```

Figure 6: Scanning of Custom IP Address List from input file by NetCertScanner Console version.

System Requirements

Operating System: Windows XP, Vista, Windows 7, Windows 8, Windows 10 (32-bit/64-bit)
Physical Memory: 1 GB
HARD Disk Capacity: 100 MB
Database: MS SQL Server (optional)

Note: We have successfully tested with MS SQL Server 2000/2005 version. It may work well with newer versions as well as other Database Software as we use standard database interface. In such case we highly encourage you to use the Demo version for verification using our easy to follow 'Database Integration Guide'.

Contact Information

We are just email away for any of your queries or support help.

Sales Enquiries/Orders:	sales [at] xenarmor.com
Support Issues/Updates:	support [at] xenarmor.com
General Info/Queries:	contact [at] xenarmor.com

For latest information, please visit online [product page of NetCertScanner]