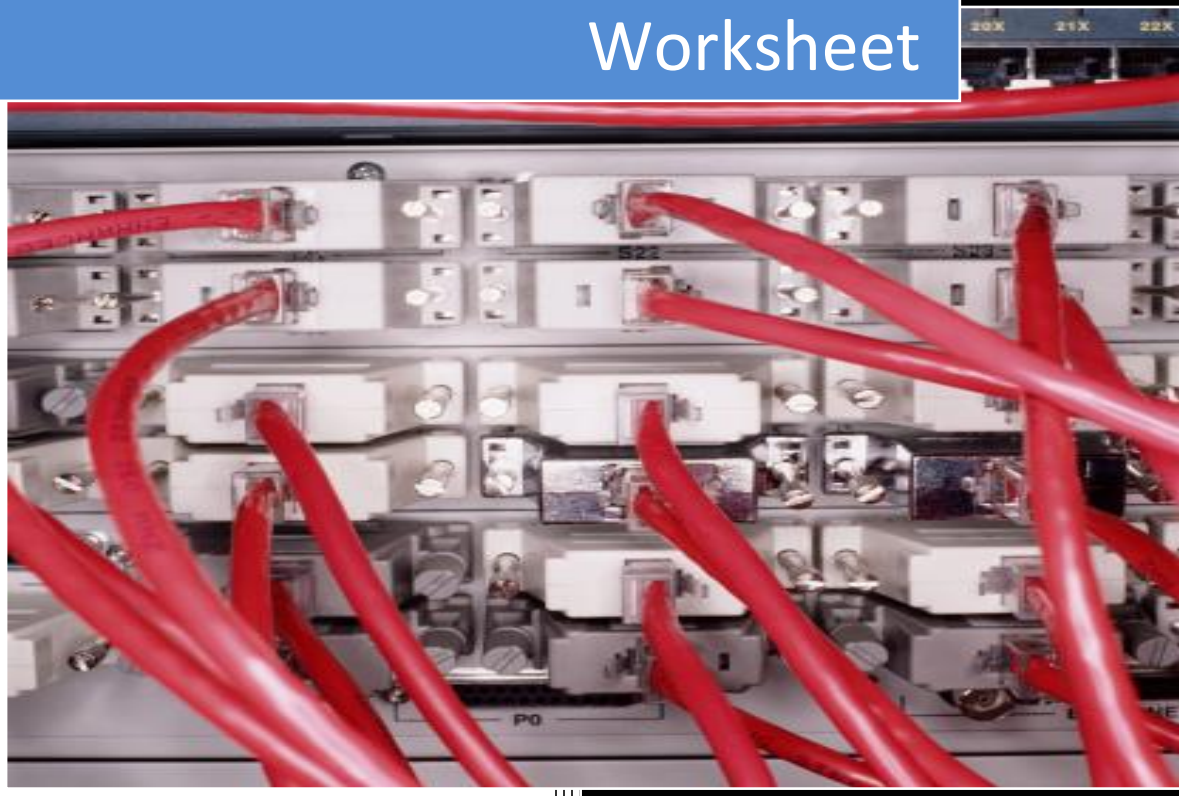
YourIT!
Your Logo Goes Here

PCI Assessment

Response Report - Compensating Controls Worksheet



Prepared for:
Prospect or Customer
Prepared by:
Your Company Name

Table of Contents

PCI DSS Requirement 1.1.4

Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

Topic	Response	Responded By
One or more Internet connections are not secured as required to protect the Cardholder Data Environment from malicious attacks.		
The current network diagram is not consistent with the firewall configuration standards.		

PCI DSS Requirement 1.2.1

Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

Topic	Response	Responded By
fw1 - Missing Explicit Deny Outbound Rule		

PCI DSS Requirement 1.3.5

Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

Topic	Response	Responded By
Web access to potentially harmful sites		
	http://espn.go.com http://gmail.google.com http://isohunt.to http://mail.yahoo.com http://thepiratebay.se http://www.cnet.com http://www.facebook.com http://www.myspace.com http://www.playboy.com http://www.tucows.com http://www.youporn.com http://www.youtube.com https://plus.google.com	

PCI DSS Requirements 2.2.5

Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

Topic	Response	Responded By
Unnecessary functionality found on STORAGE01 (fe80::7862:940f:f35b:ee35%24,fe80::2421:204a:f5ff:feba%21,10.0.1.69,2001:0:9d38:6abd:2421:204a:f5ff:feba)		
	Driver WAN Miniport (SSTP)	
Unnecessary functionality found on STORAGE01 (fe80::7862:940f:f35b:ee35%24,fe80::2421:204a:f5ff:feba%21,10.0.1.69,2001:0:9d38:6abd:2421:204a:f5ff:feba)		
	Driver WAN Miniport (PPTP)	
Unnecessary functionality found on STORAGE01 (fe80::7862:940f:f35b:ee35%24,fe80::2421:204a:f5ff:feba%21,10.0.1.69,2001:0:9d38:6abd:2421:204a:f5ff:feba)		
	Driver WAN Miniport (PPPOE)	
Unnecessary functionality found on STORAGE01 (fe80::7862:940f:f35b:ee35%24,fe80::2421:204a:f5ff:feba%21,10.0.1.69,2001:0		

:9d38:6abd:2421:204a:f5ff:feba)		
	Driver WAN Miniport (IPv6)	
Unnecessary functionality found on STORAGE01 (fe80::7862:940f:f35b:ee35%24,fe80::2421:204a:f5ff:feba%21,10.0.1.69,2001:0:9d38:6abd:2421:204a:f5ff:feba)		
	Feature Common HTTP Features	

PCI DSS Requirements 2.3a

Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.

Topic	Response	Responded By
Based upon observing administrator log on procedures and the further examination of system configurations, it has been determined that a strong encryption method is not invoked before the administrator's password is requested.		

PCI DSS Requirements 2.3.b

Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.

Topic	Response	Responded By
Telnet (23/TCP) on (10.0.0.1)		
HTTP (80/TCP) on (10.0.0.1)		
HTTP (80/TCP) on (10.0.0.21)		
Telnet (23/TCP) on (10.0.1.1)		
HTTP (80/TCP) on (10.0.1.1)		
HTTP (80/TCP) on VPNGW (10.0.1.5)	VPN server secure protocol transmission	
Telnet (23/TCP) on ISA1 (10.0.1.6)		
HTTP (80/TCP) on ISA1 (10.0.1.6)	Use as tunnel only. Traffic locked to specific external IP.	
HTTP (8080/TCP) on ISA1 (10.0.1.6)		
HTTP (80/TCP) on UTIL12 (10.0.1.15)		
HTTP (80/TCP) on DEVTFS (10.0.1.16)		
HTTP (8080/TCP) on DEVTFS (10.0.1.16)		
HTTP (80/TCP) on FILE2012-1 (10.0.1.41)		

HTTP (80/TCP) on MYCO-DATTO (10.0.1.50)		
VNC (5900/TCP) on MYCO-DATTO (10.0.1.50)		
Telnet (23/TCP) on (10.0.1.51)		
HTTP (80/TCP) on (10.0.1.51)		
Telnet (23/TCP) on (10.0.1.52)		
HTTP (80/TCP) on (10.0.1.52)		
HTTP (80/TCP) on STORAGE01 (10.0.1.69)		
HTTP (80/TCP) on FINANCE (10.0.1.81)		
HTTP (80/TCP) on HV02 (10.0.1.120)		
HTTP (80/TCP) on HV02 (10.0.1.121)		
HTTP (80/TCP) on (10.0.1.201)		
HTTP (80/TCP) on (10.0.1.202)		
HTTP (80/TCP) on (10.0.1.203)		
HTTP (80/TCP) on (10.0.1.204)		
HTTP (80/TCP) on (10.0.1.205)		

VNC (5900/TCP) on (10.0.1.205)		
HTTP (80/TCP) on (10.0.1.240)		
Telnet (23/TCP) on BRN30055C36B0DA (10.0.1.244)		
HTTP (80/TCP) on BRN30055C36B0DA (10.0.1.244)		
Telnet (23/TCP) on BRN001BA921EFB7 (10.0.1.245)		
HTTP (80/TCP) on BRN001BA921EFB7 (10.0.1.245)		
HTTP (80/TCP) on AMAZONROUTER (10.0.3.2)		
Telnet (23/TCP) on (10.0.5.1)		
HTTP (80/TCP) on (10.0.5.1)		
HTTP (80/TCP) on SVR74QG-U (10.0.6.2)		
HTTP (80/TCP) on NEWBUILD (10.0.6.8)		
HTTP (80/TCP) on SVRTEST1 (10.0.6.12)		
HTTP (80/TCP) on SVRDEV3 (10.0.6.20)		

HTTP (8080/TCP) on (10.0.6.23)		
HTTP (80/TCP) on (10.0.6.49)		
Telnet (23/TCP) on ISA1 (10.0.6.69)		
HTTP (80/TCP) on ISA1 (10.0.6.69)		
HTTP (80/TCP) on SVRDEMO1 (10.0.6.76)		
VNC (5900/TCP) on PITMACMINI (10.0.6.77)		
HTTP (80/TCP) on PS01 (10.0.6.80)		
HTTP (80/TCP) on SVRDEV2-U (10.0.6.84)		
HTTP (80/TCP) on SVRRFT1 (10.0.6.86)		
HTTP (80/TCP) on JRAWIN8K1QA3 (10.0.6.88)		
HTTP (80/TCP) on RANCOR (10.0.6.97)		
HTTP (80/TCP) on VPNGW (10.0.6.107)		
HTTP (80/TCP) on IDRAC-FTJMPQ1 (10.0.6.122)		
VNC (5900/TCP) on IDRAC-FTJMPQ1 (10.0.6.122)		

HTTP (80/TCP) on THAYDEN-DT (10.0.7.45)		
HTTP (80/TCP) on MYCO30DEV (10.0.7.65)		
HTTP (8080/TCP) on MYCO30DEV (10.0.7.65)		
HTTP (80/TCP) on SPA112 (10.0.7.89)		

PCI DSS Requirements 2.3.c

Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.

Topic	Response	Responded By
Observed insecure login to: http://webconsole01		

PCI DSS Requirements 3.2

Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

Topic	Response	Responded By
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\creditcardfiles\122000000000003.docx)		
	5555********4444 5019********3742 3670******0000 3614******7913 6011********0000 3528********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\creditcardfiles\Diners_creditcard.xlsx)		
	3670******0000 3614******7913	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\creditcardfiles\Discover_creditcard.xlsx)		
	6011********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\creditcardfiles\Visa_creditcard.xlsx)		
	4911*****0000 4917********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\credit		

cardfiles\creditcardstxtfile.txt)		
	5555********4444 5019********3742 3670******0000 3614******7913 6011********0000 3528********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\QA_Files\creditcardfiles\visadebit_creditcard.xlsx)		
	4462********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\Users\jsmith\AppData\Roaming\Microsoft\Windows\Cookies\C57IJUF1.txt)		
	5124********0258	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\Users\jsmith\Documents\Diners_creditcard.xlsx)		
	3670******0000 3614******7913	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\Users\jsmith\Documents\Discover_creditcard.xlsx)		
	6011********0000	
Personal Account Numbers found: QA-PC (10.0.6.41) (C:\Users\jsmith\Documents\Visa_creditcard.xlsx)		
	4911*****0000 4917********0000	

Personal Account Numbers found: QA-PC (10.0.6.41) (C:\Users\jsmith\Documents\visadebit_creditcard.xlsx)		
	4462********0000	

PCI DSS Requirements 4

Encrypt transmission of cardholder data across open, public networks

Topic	Response	Responded By
Insecure Company Wireless: ObjectNet		

PCI DSS Requirements 5.1.1

Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

Topic	Response	Responded By
The listed anti-virus applications were found to not meet the minimum requirements		
	Microsoft Security Essentials Windows Defender	

PCI DSS Requirements 6.2

Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Topic	Response	Responded By
Missing patches on: PIT\DC03 (10.0.1.3)		
Missing patches on: PIT\DC03 (10.0.1.4)		
Missing patches on: PIT\VPNGW (10.0.1.5)		
Missing patches on: PIT\ISA1 (10.0.1.6)		
Missing patches on: PIT\UTIL12 (10.0.1.15)		
Missing patches on: PIT\DEVTFS (10.0.1.16)		
Missing patches on: PIT\RDGATEWAY (10.0.1.21)		
Missing patches on: PIT\DC03 (10.0.1.23)		
Missing patches on: PIT\FILE2012-1 (10.0.1.41)		
Missing patches on: PIT\STORAGE01 (10.0.1.69)		
Missing patches on: PIT\HV01 (10.0.1.111)		

Missing patches on: PIT\HV02 (10.0.1.120)		
Missing patches on: PIT\HV02 (10.0.1.121)		
Missing patches on: PIT\TTREX (10.0.6.1)		
Missing patches on: PIT\CCPROC01 (10.0.6.4)		
Missing patches on: PIT\CONFERENCEROOM (10.0.6.33)		
Missing patches on: PIT\BROWND (10.0.6.35)		
Missing patches on: PIT\JACOB-WIN7 (10.0.6.44)		
Missing patches on: PIT\CONFERENCEROOM (10.0.6.55)		
Missing patches on: PIT\DEVTFSBUILD (10.0.6.67)		
Missing patches on: PIT\ISA1 (10.0.6.69)		
Missing patches on: PIT\PS01 (10.0.6.80)		
Missing patches on: PIT\RANCOR (10.0.6.97)		

Missing patches on: PIT\VPNGW (10.0.6.107)		
Missing patches on: PIT\PITMARCUSUS-PC (10.0.6.133)		
Missing patches on: PIT\JACOB-WIN8 (10.0.7.44)		
Missing patches on: DC03 (10.0.1.23, 10.0.1.4, 10.0.1.3)		
Missing patches on: HV02 (192.168.1.12, 10.0.1.121, 10.0.1.120)		
Missing patches on: PS01 (10.0.6.80, 192.168.159.1, 192.168.85.1)		
Missing patches on: VPNGW (10.0.1.5, 10.0.6.107)		

PCI DSS Requirement 8.1.1/8.5

Assign all users a unique ID before allowing them to access system components or cardholder data. Do not use group, shared, or generic IDs, passwords, or other authentication methods. The following contains a list of potential generic users.

Topic	Response	Responded By
Corp.myco.com\admin		
	First Name: admin Last Name: admin	
Corp.myco.com\Administrator		
	First Name: Last Name:	
Corp.myco.com\ASPNET		
	First Name: Last Name:	
Corp.myco.com\CORE$		
	First Name: Last Name:	
Corp.myco.com\DEV$		
	First Name: Last Name:	
Corp.myco.com\helper		
	First Name: Last Name: helper	
Corp.myco.com\HQ$		
	First Name: Last Name:	
Corp.myco.com\IUSR_DC02		
	First Name: Last Name:	
Corp.myco.com\IUSR_STEINBRENNER		
	First Name: Last Name:	

Corp.myco.com\IWAM_DC02		
	First Name: Last Name:	
Corp.myco.com\IWAM_STEINBRENNER		
	First Name: Last Name:	
Corp.myco.com\netvendor		
	First Name: Last Name:	
Corp.myco.com\supportguy		
	First Name: supportguy Last Name: supportguy	
Corp.myco.com\Tester		
	First Name: Tester Last Name:	

PCI DSS Requirement 8.1.3

Manage IDs used by employees to access, support, or maintain system components. The following contains a list of potential former employees.

Topic	Response	Responded By
Corp.myco.com\admin		
	Name: admin admin Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\adminonly		
	Name: admin only Last Login: 7/2/2014 12:26:48 PM	
Corp.myco.com\ASPNET	Service Account	
	Name: ASPNET Last Login: <Unknown>	
Corp.myco.com\BackupUser		
	Name: Backup User Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\bvinings		
	Name: Bob vinings Last Login: 2/28/2014 10:03:14 PM	
Corp.myco.com\bgelding		
	Name: beth gelding Last Login: <Unknown>	
Corp.myco.com\CORE$		
	Name: CORE$ Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\DEV$		
	Name: DEV$ Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\helper		
	Name: helper Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\HQ$		
	Name: HQ$ Last Login: 1/1/1601 12:00:00 AM	

Corp.myco.com\IUSR_DC02		
	Name: IUSR_DC02 Last Login: 10/12/2009 2:53:59 PM	
Corp.myco.com\IUSR_STEINBRENNER		
	Name: IUSR_STEINBRENNER Last Login: 4/11/2012 3:58:18 PM	
Corp.myco.com\IWAM_DC02		
	Name: IWAM_DC02 Last Login: 4/30/2009 8:16:41 PM	
Corp.myco.com\IWAM_STEINBRENNER		
	Name: IWAM_STEINBRENNER Last Login: <Unknown>	
Corp.myco.com\jcraig		
	Name: Joe craig Last Login: 1/14/2014 11:03:14 AM	
Corp.myco.com\kmayhem1		
	Name: k mayhem1 Last Login: <Unknown>	
Corp.myco.com\mwest		
	Name: mary west Last Login: 1/19/2015 3:19:30 PM	
Corp.myco.com\msummer		
	Name: Mark summer Last Login: 3/20/2015 8:16:53 PM	
Corp.myco.com\NetScanner		
	Name: Net Scanner - myco Last Login: 7/20/2012 9:35:23 PM	
Corp.myco.com\netvendor		
	Name: netvendor Last Login: <Unknown>	
Corp.myco.com\hr		
	Name: internal IT HR Last Login: <Unknown>	
Corp.myco.com\info		
	Name: internal IT PR Last Login: <Unknown>	

Corp.myco.com\prsales		
	Name: internal IT Sales Last Login: <Unknown>	
Corp.myco.com\support		
	Name: internal IT Support Team Last Login: 11/5/2011 11:22:27 PM	
Corp.myco.com\PGKTest1		
	Name: PGK Test1 Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\PurchaseUser		
	Name: Purchase User Last Login: 1/29/2015 8:47:28 PM	
Corp.myco.com\srammond		
	Name: Sam rammond. Last Login: 5/2/2014 2:31:33 PM	
Corp.myco.com\smurray		
	Name: sam murray Last Login: 12/16/2013 2:43:36 PM	
Corp.myco.com\SharePointSQL		
	Name: SharePoint SQL Last Login: 7/4/2014 4:49:32 AM	
Corp.myco.com\slowe		
	Name: sherry Lowe Last Login: 7/24/2014 5:54:22 PM	
Corp.myco.com\supportguy		
	Name: supportguy supportguy Last Login: 1/1/1601 12:00:00 AM	
Corp.myco.com\nonadminuser		
	Name: test non-admin Last Login: 7/15/2014 1:32:10 PM	
Corp.myco.com\marcusustest		
	Name: Test User Last Login: 12/11/2012 2:39:17 PM	

PCI DSS Requirement 8.1.5

Manage IDs used by vendors to access, support, or maintain system components. The following contains a list of potential former employees.

Topic	Response	Responded By
Corp.myco.com\partners		
	Name: internal IT Managed Services Partners Last Login: <None>	

PCI DSS Requirements 8.1.6

Limit repeated access attempts by locking out the user ID after not more than six attempts.

Topic	Response	Responded By
Account lockout threshold disabled		
	All Sampled	

PCI DSS Requirements 8.1.7

Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

Topic	Response	Responded By
Account lockout duration disabled		
	All Sampled	

PCI DSS Requirements 8.2.3

Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

Topic	Response	Responded By
Minimum password length disabled		
	trex RJOHNSON-PC Sdavis-LT STORAGE01 Thayden-DT thanos-PC UTIL12 VPNGW	
Password must meet complexity requirements (Disabled)		
	ccproc01 BROWND CONFERENCEROOM DC03 DEVTFS DEVTFSBUILD FILE2012-1 FT-LENOVO HV01 HV02 jacob-WIN8 Mmayhemon-HP Mwest-PC Mwest-WIN864 PITmarcusus-PC PS01 Psimpson-PC Psimpson-WIN7TEST QA-PC RANCOR RDGATEWAY trex trex RJOHNSON-PC RJOHNSON-PC Sdavis-LT Sdavis-LT STORAGE01	

	STORAGE01 Thayden-DT Thayden-DT thanos-PC thanos-PC UTIL12 UTIL12 VPNGW VPNGW	
Store passwords using reversible encryption (Disabled)		
	All Sampled	

PCI DSS Requirements 8.2.5

Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

Topic	Response	Responded By
Enforce password history disabled		
	All Sampled	

PCI DSS Requirements 10

Track and monitor all access to network resources and cardholder data

Topic	Response	Responded By
All actions taken by any individual with root or administrative privileges are not automatically audited using Group Policy		
Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges are not automatically audited using Group Policy		

PCI DSS Requirements 11.2.3 External Vulnerabilities

Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

Topic	Response	Responded By
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)		
	199.38.223.84	

PCI DSS Requirements 11.2.3 Internal Vulnerabilities

Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.

Topic	Response	Responded By
NVT: Discard port open (OID: 1.3.6.1.4.1.25623.1.0.11367)	False positive	
	10.0.6.69	
NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)		
	10.0.6.69 10.0.7.65 10.0.1.6	
NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)		
	10.0.6.69 10.0.1.5 10.0.1.15 10.0.1.21 10.0.1.69 10.0.1.81 10.0.6.12 10.0.6.20 10.0.6.76 10.0.6.86 10.0.6.107 10.0.6.109 10.0.7.45 10.0.7.65 10.0.6.103 10.0.1.16 10.0.6.80 10.0.1.6 10.0.1.3 10.0.1.4 10.0.1.23 10.0.1.41	

	10.0.1.100 10.0.1.104 10.0.1.120 10.0.1.121 10.0.6.0 10.0.6.1 10.0.6.4 10.0.6.14 10.0.6.33 10.0.6.35 10.0.6.40 10.0.6.41 10.0.6.44 10.0.6.47 10.0.6.53 10.0.6.55 10.0.6.67 10.0.6.88 10.0.6.96 10.0.6.97 10.0.6.106 10.0.6.133 10.0.7.18 10.0.7.44 10.0.7.74 10.0.7.95 10.0.7.123	
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)		
	10.0.1.5 10.0.1.15 10.0.1.21 10.0.1.69 10.0.1.81 10.0.6.12 10.0.6.20 10.0.6.76 10.0.6.86 10.0.6.107 10.0.6.109 10.0.6.50	

NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)		
	10.0.1.5 10.0.1.15 10.0.1.21 10.0.1.69 10.0.1.81 10.0.6.107 10.0.6.50 10.0.1.201 10.0.1.202 10.0.1.203 10.0.1.204 10.0.1.205 10.0.6.122 10.0.1.240 10.0.6.49	
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)		
	10.0.1.5 10.0.1.15 10.0.1.21 10.0.1.69 10.0.1.81 10.0.6.107 10.0.6.50 10.0.1.240 10.0.6.49	
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)		
	10.0.1.5 10.0.1.15 10.0.1.21 10.0.1.69 10.0.1.81 10.0.6.107	

	10.0.6.50 10.0.1.202 10.0.1.1 10.0.5.1 10.0.1.240 10.0.6.103 10.0.0.1 10.0.6.49	
NVT: SSL Certification Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)		
	10.0.1.15 10.0.1.69 10.0.1.81	
NVT: PHP _php_stream_scandir() Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803317)		
	10.0.7.45	
NVT: PHP Multiple Vulnerabilities - March 2013 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803337)		
	10.0.7.45	
NVT: PHP phar/tar.c Heap Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803342)		
	10.0.7.45	
NVT: PHP Remote Code Execution and Denail of Service Vulnerabilities Dec13 (OID: 1.3.6.1.4.1.25623.1.0.804174)		
	10.0.7.45	

NVT: PHP Multiple Double Free Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805412)		
	10.0.7.45 10.0.6.103	
NVT: PHP Multiple Vulnerabilities-02 - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805413)		
	10.0.7.45 10.0.6.103	
NVT: PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805414)		
	10.0.7.45 10.0.6.103	
NVT: PHP XML Handling Heap Buffer Overflow Vulnerability July13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803729)		
	10.0.7.45	
NVT: PHP Sessions Subsystem Session Fixation Vulnerability-Aug13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803737)		
	10.0.7.45	
NVT: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213)		
	10.0.7.45 10.0.7.65 10.0.6.103	

NVT: PHP Multiple Vulnerabilities -01 March13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803341)		
	10.0.7.45	
NVT: Apache HTTP Server mod_proxy_ajp Process Timeout DoS Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.802683)		
	10.0.7.45	
NVT: PHP open_basedir Secuirity Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803318)		
	10.0.7.45	
NVT: PHP Multiple Vulnerabilities - June13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803678)		
	10.0.7.45	
NVT: PHP open_basedir Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.804241)		
	10.0.7.45	
NVT: PHP CDF File Parsing Denial of Service Vulnerabilities -01 Jun14 (OID: 1.3.6.1.4.1.25623.1.0.804639)		
	10.0.7.45	

NVT: PHP SSL Certificate Validation Security Bypass Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803739)		
	10.0.7.45	
NVT: PHP SOAP Parser Multiple Information Disclosure Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.803764)		
	10.0.7.45	
NVT: PHP LibGD Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.804292)		
	10.0.7.45	
NVT: Apache HTTP Server httpOnly Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)		
	10.0.7.45	
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (OID: 1.3.6.1.4.1.25623.1.0.902269)	False positive	
	10.0.7.68	
NVT: Microsoft Windows SMTP Server DNS spoofing vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100624)		

	10.0.7.68	
NVT: Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100596)		
	10.0.7.68	
NVT: IPMI Cipher Zero Authentication Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103840)		
	10.0.1.201 10.0.1.202 10.0.1.203 10.0.1.204 10.0.1.205 10.0.6.122	
NVT: IPMI MD2 Auth Type Support Enabled (OID: 1.3.6.1.4.1.25623.1.0.103839)		
	10.0.1.201 10.0.1.202 10.0.1.203 10.0.1.204 10.0.1.205 10.0.6.122	
NVT: OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)		
	10.0.1.202	
NVT: Dell iDRAC6 and iDRAC7 ErrorMsg Parameter Cross Site Scripting Vulnerability (OID:		

1.3.6.1.4.1.25623.1.0.103808)		
	10.0.1.205	
NVT: SSH Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.103239)		
	10.0.6.122 10.0.1.1 10.0.5.1	
NVT: IPMI Default Password Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105923)		
	10.0.6.122	
NVT: NFS export (OID: 1.3.6.1.4.1.25623.1.0.102014)		
	10.0.1.50	
NVT: X Server (OID: 1.3.6.1.4.1.25623.1.0.10407)		
	10.0.1.50	
NVT: Microsoft IIS FTPd NLST stack overflow (OID: 1.3.6.1.4.1.25623.1.0.100952)		
	10.0.7.65	
NVT: Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387) (OID: 1.3.6.1.4.1.25623.1.0.902818)	False positive	
	10.0.7.65	
NVT: Windows Administrator NULL FTP password (OID: 1.3.6.1.4.1.25623.1.0.11160)		

	10.0.7.65	
NVT: Apache Tomcat servlet/JSP container default files (OID: 1.3.6.1.4.1.25623.1.0.12085)		
	10.0.7.65	
NVT: Apache Tomcat Multiple Vulnerabilities - 01 Mar14 (OID: 1.3.6.1.4.1.25623.1.0.804519)		
	10.0.7.65	
NVT: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)		
	10.0.7.65 10.0.1.1 10.0.5.1	
NVT: IIS Service Pack - 404 (OID: 1.3.6.1.4.1.25623.1.0.11874)		
	10.0.7.65	
NVT: Microsoft ASP.NET Information Disclosure Vulnerability (2418042) (OID: 1.3.6.1.4.1.25623.1.0.901161)		
	10.0.7.65	
NVT: Microsoft IIS IP Address/Internal Network Name Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902796)		
	10.0.7.65	
NVT: Apache Tomcat Multiple		

Vulnerabilities June-09 (OID: 1.3.6.1.4.1.25623.1.0.800813)		
	10.0.7.65	
NVT: Apache Tomcat Cross-Site Scripting and Security Bypass Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.900021)		
	10.0.7.65	
NVT: Microsoft IIS Default Welcome Page Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802806)		
	10.0.7.65	
NVT: Apache Tomcat JSP Example Web Applications Cross Site Scripting Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.111014)		
	10.0.7.65	
NVT: Apache Tomcat RemoteFilterValve Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800024)		
	10.0.7.65	
NVT: Apache Tomcat Multiple Vulnerabilities - 02 Mar14 (OID: 1.3.6.1.4.1.25623.1.0.804520)		
	10.0.7.65	
NVT: Missing Secure Attribute		

SSL Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902661)		
	10.0.1.1 10.0.5.1	
NVT: Multiple NetGear ProSafe Switches Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103773)		
	10.0.0.21	
NVT: Report default community names of the SNMP Agent (OID: 1.3.6.1.4.1.25623.1.0.10264)		
	10.0.0.21 10.0.0.1 10.0.0.11 10.0.1.51	
NVT: Lighttpd Multiple vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.802072)		
	10.0.1.240	
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)		
	10.0.1.240 10.0.0.1 10.0.6.49	
NVT: Dropbear SSH Server Multiple Security Vulnerabilities (OID:		

1.3.6.1.4.1.25623.1.0.105114)		
	10.0.1.240	
NVT: PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805411)		
	10.0.6.103	
NVT: SNMP GETBULK Reflected DrDoS (OID: 1.3.6.1.4.1.25623.1.0.105062)		
	10.0.0.1 10.0.1.52	
NVT: Web Server Cross Site Scripting (OID: 1.3.6.1.4.1.25623.1.0.10815)		
	10.0.0.11	
NVT: Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote (OID: 1.3.6.1.4.1.25623.1.0.805110)		
	10.0.1.16 10.0.6.80	
NVT: LDAP allows null bases (OID: 1.3.6.1.4.1.25623.1.0.10722)		
	10.0.1.3 10.0.1.4 10.0.1.23	
NVT: Use LDAP search request to retrieve information from NT Directory Services (OID:		

1.3.6.1.4.1.25623.1.0.12105)		
	10.0.1.3 10.0.1.4 10.0.1.23	