RAPID7

Metasploit Pro

Detailed Audit Report

Report generated:

Fri, 5 Mar 2021 14:19:28 +0530

Total Pages: 35

Executive Summary

This report represents a security audit performed using Metasploit Pro from Rapid7, Inc. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

During this test, 79 hosts with a total of 176 exposed services were discovered. No modules were successfully run and no login credentials were obtained.

Major Findings

Discovered Operating Systems

Operating System	Hosts	Services	Vulnerabilities
IOS	31	59	0
Unknown	43	41	0
Windows	1	17	1
Windows 2008 R2	1	15	0
Windows 2012 R2	3	49	0

Discovered Hosts

Discovered	IP Address	Hostname	OS	Services	Vulns
3/5/21 8:09 AM	124.4.164.223	GCPWUSCIN1ADC01	Windows	17	1
3/5/21 8:09 AM	119.43.99.66	119.43.99.66	Unknown	1	0
3/5/21 8:09 AM	58.2.58.22	ind-hyd-gsd-int-pa-02.	Unknown	0	0
3/5/21 8:09 AM	10.70.244.192	ind-con-gsd-int-fw-01.	Unknown	2	0
3/5/21 8:09 AM	58.2.241.17	loopback0-ind-dlf-bus-rt-02*	IOS	2	0
3/5/21 8:09 AM	58.2.64.5	58.2.64.5	IOS	2	0
3/5/21 8:09 AM	58.2.38.30	ind-dlf-gsd-il2-sw-03.	IOS	2	0
3/5/21 8:09 AM	10.75.178.157	10.75.178.157	Unknown	0	0
3/5/21 8:09 AM	182.94.220.19	ind-hyr-gsd-bus-rt-01.	IOS	2	0
3/5/21 8:09 AM	58.2.47.148	58.2.47.148	Unknown	2	0
3/5/21 8:09 AM	10.100.252.6	ind-cos-gsd-int-fw-02.	Unknown	2	0
3/5/21 8:09 AM	182.94.138.76	182.94.138.76	IOS	2	0
3/5/21 8:09 AM	58.2.57.3	ind-hyd-gsd-cor-sw-02.	IOS	2	0
3/5/21 8:09 AM	10.70.244.193	ind-con-gsd-int-fw-02.	Unknown	2	0
3/5/21 8:09 AM	58.2.57.2	ind-hyd-gsd-cor-sw-01.	IOS	2	0
3/5/21 8:09 AM	182.94.138.119	ind-hyr-gsd-dps-sw-02.	IOS	2	0
3/5/21 8:09 AM	182.94.129.25	182.94.129.25	Unknown	1	0
3/5/21 8:09 AM	58.2.37.2	ind-dlf-gsd-cor-sw-01.	IOS	2	0
3/5/21 8:09 AM	58.2.243.172	ind-dlf-gsd-dps-sw-01.	IOS	2	0
3/5/21 8:09 AM	10.70.244.60	ind-con-gsd-int-rt-01.	IOS	2	0
3/5/21 8:09 AM	58.2.37.3	ind-dlf-gsd-cor-sw-02.	IOS	2	0
3/5/21 8:09 AM	58.2.40.6	58.2.40.6	Unknown	0	0
3/5/21 8:09 AM	124.4.164.242	GCPWUSCIN1SEP01	Windows 2008 R2	15	0
3/5/21 8:09 AM	10.75.178.123	10.75.178.123	Unknown	0	0
3/5/21 8:09 AM	58.2.47.116	ind-dlf-acs-01.ind.corp.ad	Unknown	10	0
3/5/21 8:09 AM	58.2.64.4	58.2.64.4	Unknown	1	0
3/5/21 8:09 AM	182.94.220.15	ind-hyd-nbs-dps-rt-01.	Unknown	0	0

Discovered	IP Address	Hostname	OS	Services	Vulns
3/5/21 8:09 AM	10.100.254.193	ind-cos-gsd-int-rt-01.	Unknown	0	0
3/5/21 8:09 AM	10.75.178.253	10.75.178.253	Unknown	0	0
3/5/21 8:09 AM	10.75.178.60	10.75.178.60	Unknown	0	0
3/5/21 8:09 AM	58.2.40.5	ind-dlf-gsd-int-rt-02.genpact.	Unknown	1	0
3/5/21 8:09 AM	182.94.152.116	GCPWINDEL2OKT02	Windows 2012 R2	14	0
3/5/21 8:09 AM	58.2.38.29	58.2.38.29	Unknown	0	0
3/5/21 8:09 AM	182.94.152.5	182.94.152.5	Unknown	1	0
3/5/21 8:09 AM	58.2.243.173	ind-dlf-gsd-dps-sw-02.	IOS	2	0
3/5/21 8:09 AM	10.75.162.93	10.75.162.93	Unknown	1	0
3/5/21 8:09 AM	182.94.220.20	ind-hyr-gsd-bus-rt-02.	IOS	2	0
3/5/21 8:09 AM	58.2.241.16	loopback0-ind-dlf-bus-rt-01	IOS	2	0
3/5/21 8:09 AM	58.2.40.4	ind-dlf-gsd-int-rt-01.genpact.	Unknown	1	0
3/5/21 8:09 AM	10.70.244.51	ind-con-gsd-bus-rt-01.	IOS	1	0
3/5/21 8:09 AM	58.2.69.60	ind-hyd-gsd-bus-02.	Unknown	0	0
3/5/21 8:09 AM	10.75.178.179	10.75.178.179	Unknown	0	0
3/5/21 8:09 AM	58.2.64.6	ind-hyd-gsd-il2-sw-52.	IOS	2	0
3/5/21 8:09 AM	124.4.225.74	GCPWGTGUA1SCCM1	Windows 2012 R2	20	0
3/5/21 8:09 AM	182.94.138.18	ind-hyr-gsd-bus-fw-02.	Unknown	0	0
3/5/21 8:09 AM	182.94.96.226	182.94.96.226	Unknown	0	0
3/5/21 8:09 AM	58.2.58.33	ind-hyd-gsd-il2-sw-61.	IOS	2	0
3/5/21 8:09 AM	119.43.85.150	119.43.85.150	Unknown	3	0
3/5/21 8:09 AM	182.94.138.118	ind-hyr-gsd-dps-sw-01.	IOS	2	0
3/5/21 8:09 AM	10.75.162.76	10.75.162.76	Unknown	1	0
3/5/21 8:09 AM	58.2.40.3	ind-dlf-gsd-il2-sw-01.	Unknown	1	0
3/5/21 8:09 AM	58.2.38.25	58.2.38.25	Unknown	0	0
3/5/21 8:09 AM	10.100.254.195	ind-cos-gsd-bus-rt-01.	IOS	2	0
3/5/21 8:09 AM	58.2.243.180	ind-hyd-gsd-dps-sw-01.	IOS	2	0
3/5/21 8:09 AM	10.74.243.52	10.74.243.52	Unknown	0	0
3/5/21 8:09 AM	58.2.37.54	ind-dlf-gsd-bus-fw-02.	Unknown	0	0
3/5/21 8:09 AM	10.75.178.181	10.75.178.181	Unknown	0	0
3/5/21 8:09 AM	58.2.64.3	ind-hyd-gsd-il2-sw-51.	IOS	2	0
3/5/21 8:09 AM	10.75.178.63	10.75.178.63	Unknown	0	0
3/5/21 8:09 AM	58.2.241.2	loopback0-ind-upl-bus-rt-02	IOS	2	0
3/5/21 8:09 AM	10.100.250.53	10.100.250.53	Unknown	0	0
3/5/21 8:09 AM	10.70.244.52	ind-con-gsd-bus-rt-02.	IOS	1	0
3/5/21 8:09 AM	10.70.244.59	ind-con-gsd-int-rt-02.	IOS	2	0
3/5/21 8:09 AM	58.2.58.21	ind-hyd-gsd-int-pa-01.	Unknown	0	0
3/5/21 8:09 AM	58.2.241.1	loopback0-ind-upl-bus-rt-01	IOS	2	0
3/5/21 8:09 AM	58.2.37.53	ind-dlf-gsd-bus-fw-01.	Unknown	0	0
3/5/21 8:09 AM	10.100.252.5	ind-cos-gsd-int-fw-01.	Unknown	2	0
3/5/21 8:09 AM	58.2.243.181	ind-hyd-gsd-dps-sw-02.	IOS	2	0
3/5/21 8:09 AM	119.43.85.227	GCPWINHYD2OKT01	Windows 2012 R2	15	0
3/5/21 8:09 AM	182.94.128.1	ind-hyr-gsd-cor-sw.genpact.	IOS	1	0
3/5/21 8:09 AM	58.2.69.59	ind-hyd-gsd-bus-01.	Unknown	0	0

Discovered	IP Address	Hostname	OS	Services	Vulns
3/5/21 8:09 AM	182.94.138.77	182.94.138.77	IOS	2	0
3/5/21 8:09 AM	58.2.58.181	ind-upl-acs-01.ind.corp.ad	Unknown	7	0
3/5/21 8:09 AM	10.100.254.196	ind-cos-gsd-bus-rt-02.	IOS	2	0
3/5/21 8:09 AM	58.2.38.26	58.2.38.26	Unknown	0	0
3/5/21 8:09 AM	119.43.12.30	119.43.12.30	Unknown	0	0
3/5/21 8:09 AM	182.94.138.17	182.94.138.17	Unknown	2	0
3/5/21 8:09 AM	58.2.58.34	ind-hyd-gsd-il2-sw-62.	IOS	2	0
3/5/21 8:09 AM	10.100.254.194	ind-cos-gsd-int-rt-02.	Unknown	0	0

Detailed Findings

124.4.164.223 - GCPWUSCIN1ADC01

Discovered: 2021-03-05 08:09:32.078101

Operating System: Windows

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
53	tcp	dns	
80	tcp	http	Microsoft-HTTPAPI/2.0
135	tcp	dcerpc	Endpoint Mapper (613 services)
139	tcp	smb	
389	tcp	ldap	
445	tcp	smb	
3389	tcp	ms-wbt-server	
17000	tcp	dcerpc	51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 Ngc Pop Key Service
49664	tcp	dcerpc	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0
49665	tcp	dcerpc	f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 Event log TCPIP
50000	tcp	dcerpc	897e2e5f-93f3-4376-9c9c-fd2277495c27 v1.0 Frs2 Service
54004	tcp	dcerpc	50abc2a4-574d-40b3-9d66-ee4fd5fba076 v5.0
57186	tcp	dcerpc	367abb81-9844-35f1-ad32-98f038001003 v2.0
61447	tcp	dcerpc	51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 Ngc Pop Key Service
61450	tcp	dcerpc	d09bdeb5-6171-4a34-bfe2-06fa82652568 v1.0
61452	tcp	dcerpc	6b5bdd1e-528c-422c-af8c-a4079be4fe48 v1.0 Remote Fw APIs
61458	tcp	dcerpc	51a227ae-825b-41f2-b4a9-1ac9557a1018 v1.0 Ngc Pop Key Service

Web Vulnerabilities

Disclosed Vulnerabilities

Vulnerability	Description
SMB Signing Is Not Required	

119.43.99.66 - 119.43.99.66

Discovered: 2021-03-05 08:09:31.262545

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
514	tcp	shell	

Web Vulnerabilities

58.2.58.22 - ind-hyd-gsd-int-pa-02.genpact.com

Discovered: 2021-03-05 08:09:31.308507

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.70.244.192 - ind-con-gsd-int-fw-01.genpact.com

Discovered: 2021-03-05 08:09:31.329143

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_12.1
443	tcp	https	(302-/php/login.php)

Web Vulnerabilities

58.2.241.17 - loopback0-ind-dlf-bus-rt-02*

Discovered: 2021-03-05 08:09:31.39071

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f600001da800001f423a022f94e3ec5a5b0353f7d8c54f234b71b152f3e3ec65c6d645a418e3ec65c6d645a418

Web Vulnerabilities

58.2.64.5 - 58.2.64.5

Discovered: 2021-03-05 08:09:31.431505

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000270c00001acf3a022f94e3ec61d1edd2f438c54f234b71b152f3e3ec65c6122d0e88e3ec65c6122d0e88

Web Vulnerabilities

58.2.38.30 - ind-dlf-gsd-il2-sw-03.genpact.com

Discovered: 2021-03-05 08:09:31.476742

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f600001e2100002a413a022f94e3ec4e503ef9dbd0c54f234b71b152f3e3ec65c444189430e3ec65c444189430

Web Vulnerabilities

10.75.178.157 - 10.75.178.157

Discovered: 2021-03-05 08:09:31.515506

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

182.94.220.19 - ind-hyr-gsd-bus-rt-01.genpact.com

Discovered: 2021-03-05 08:09:31.53337

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000270d00001a9e3a022f94e3ec62514b851f88c54f234b71b152f3e3ec65c9228f5c88e3ec65c9228f5c88

Web Vulnerabilities

58.2.47.148 - 58.2.47.148

Discovered: 2021-03-05 08:09:31.574271

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_7.4
123	udp	ntp	240404e700001dd9000019973a0228a9e3ec5d81d8b5bcbfc54f234b71b152f3e3ec65c4da6dfb3de3ec65c4da71c864

Web Vulnerabilities

10.100.252.6 - ind-cos-gsd-int-fw-02.genpact.com

Discovered: 2021-03-05 08:09:31.615583

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_12.1
443	tcp	https	(302-/php/login.php)

Web Vulnerabilities

182.94.138.76 - 182.94.138.76

Discovered: 2021-03-05 08:09:31.67436

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000274f00001b623a022f94e3ec5e6493f7d070c54f234b71b152f3e3ec65c85c28f6c0e3ec65c85c28f6c0

Web Vulnerabilities

58.2.57.3 - ind-hyd-gsd-cor-sw-02.genpact.com

Discovered: 2021-03-05 08:09:31.712948

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504ea000026bc00002be33a022f94e3ec5261c6de2939c54f234b71b152f3e3ec65c51555589ee3ec65c515564b53

Web Vulnerabilities

10.70.244.193 - ind-con-gsd-int-fw-02.genpact.com

Discovered: 2021-03-05 08:09:31.753575

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_12.1
443	tcp	https	(302-/php/login.php)

Web Vulnerabilities

58.2.57.2 - ind-hyd-gsd-cor-sw-01.genpact.com

Discovered: 2021-03-05 08:09:31.814818

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504ea000027d9000044c03a022f94e3ec365c3d8b31dec54f234b71b152f3e3ec65c5139152c8e3ec65c513923c52

Web Vulnerabilities

182.94.138.119 - ind-hyr-gsd-dps-sw-02.genpact.com

Discovered: 2021-03-05 08:09:31.855941

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000270c00001ad53a022f94e3ec613e5645a2b8c54f234b71b152f3e3ec65c8a28f5de8e3ec65c8a28f5de8

Web Vulnerabilities

182.94.129.25 - 182.94.129.25

Discovered: 2021-03-05 08:09:31.895784

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
514	tcp	shell	

Web Vulnerabilities

58.2.37.2 - ind-dlf-gsd-cor-sw-01.genpact.com

Discovered: 2021-03-05 08:09:31.936442

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504ea00001e6800002a653a022f94e3ec4d1d93cf1ae6c54f234b71b152f3e3ec65c3a78ef4c8e3ec65c3a78fe4ce

Web Vulnerabilities

58.2.243.172 - ind-dlf-gsd-dps-sw-01.genpact.com

Discovered: 2021-03-05 08:09:31.97595

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f600001e1500001a3d3a022f94e3ec63f920c49c00c54f234b71b152f3e3ec65c6d9db2528e3ec65c6d9db2528

Web Vulnerabilities

10.70.244.60 - ind-con-gsd-int-rt-01.genpact.com

Discovered: 2021-03-05 08:09:32.015128

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25

Web Vulnerabilities

58.2.37.3 - ind-dlf-gsd-cor-sw-02.genpact.com

Discovered: 2021-03-05 08:09:32.255339

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504ea00001eed000040973a022f94e3ec3b6ec800a39dc54f234b71b152f3e3ec65c3ad939396e3ec65c3ad946ccb

Web Vulnerabilities

58.2.40.6 - 58.2.40.6

Discovered: 2021-03-05 08:09:32.294384

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

124.4.164.242 - GCPWUSCIN1SEP01

Discovered: 2021-03-05 08:09:32.312582

Operating System: Windows 2008 R2

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
80	tcp	http	Microsoft-IIS/7.5 (Powered by ASP.NET)
135	tcp	dcerpc	Endpoint Mapper (131 services)
139	tcp	smb	
443	tcp	https	Symantec Endpoint Protection Manager
445	tcp	smb	Windows 2008 R2 Standard SP1 (build:7601) (name:GCPWUSCIN1SEP01) (domain:USACORP)
1025	tcp	dcerpc	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0
1026	tcp	dcerpc	30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 NRP server endpoint
1027	tcp	dcerpc	30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0
1029	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v1.0 KeyIso

Port	Protocol	Name	Info
1058	tcp	dcerpc	367abb81-9844-35f1-ad32-98f038001003 v2.0
3389	tcp	ms-wbt-server	
8014	tcp	unknown	
8443	tcp	https	SEPM
8445	tcp	copy	
9090	tcp	http	SEPM

Web Vulnerabilities

10.75.178.123 - 10.75.178.123

Discovered: 2021-03-05 08:09:32.530392

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.47.116 - ind-dlf-acs-01.ind.corp.ad

Discovered: 2021-03-05 08:09:32.550918

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_7.6 PKIX[11.0]
49	tcp	tacacs	
80	tcp	http	(302-https://58.2.47.116:443/admin/)
443	tcp	https	(302-https://58.2.47.116:443/admin/)
8443	tcp	https	server (302-https://58.2.47.116:8443/portal/)
8444	tcp	https	server (302-https://58.2.47.116:8444/portal/)
8445	tcp	copy	
9002	tcp	dynamid	
9090	tcp	http	(302-https://58.2.47.116:9090/portal/)

Web Vulnerabilities

58.2.64.4 - 58.2.64.4

Discovered: 2021-03-05 08:09:32.805372

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
123	udp	ntp	240504f60000269700001e4b3a022f94e3ec5c1903d70a48c54f234b71b152f3e3ec65c5d374beb0e3ec65c5d374beb0

Web Vulnerabilities

182.94.220.15 - ind-hyd-nbs-dps-rt-01.genpact.com

Discovered: 2021-03-05 08:09:32.827039

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.100.254.193 - ind-cos-gsd-int-rt-01.genpact.com

Discovered: 2021-03-05 08:09:32.847447

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.75.178.253 - 10.75.178.253

Discovered: 2021-03-05 08:09:32.868197

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.75.178.60 - 10.75.178.60

Discovered: 2021-03-05 08:09:32.889492

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.40.5 - ind-dlf-gsd-int-rt-02.genpact.com

Discovered: 2021-03-05 08:09:32.910581

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
123	udp	ntp	NTP v4 (unsynchronized)

Web Vulnerabilities

182.94.152.116 - GCPWINDEL2OKT02

Discovered: 2021-03-05 08:09:32.932407

Operating System: Windows 2012 R2

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
135	tcp	dcerpc	Endpoint Mapper (270 services)
139	tcp	smb	
445	tcp	smb	Windows 2012 R2 Standard (build:9600) (name:GCPWINDEL2OKT02) (domain:INDCORP)
1025	tcp	dcerpc	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0
1026	tcp	dcerpc	3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 DHCP Client LRPC Endpoint
1027	tcp	dcerpc	58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 AppInfo
3389	tcp	ms-wbt-server	
5986	tcp	winrm	Microsoft-HTTPAPI/2.0 Authentication Methods: ["Negotiate", "Kerberos"]
30792	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
30812	tcp	dcerpc	367abb81-9844-35f1-ad32-98f038001003 v2.0
39705	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
39709	tcp	dcerpc	76f03f96-cdfd-44fc-a22c-64950a001209 v1.0
39745	tcp	dcerpc	6b5bdd1e-528c-422c-af8c-a4079be4fe48 v1.0 Remote Fw APIs
47001	tcp	winrm	

Web Vulnerabilities

58.2.38.29 - 58.2.38.29

Discovered: 2021-03-05 08:09:33.094157

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

182.94.152.5 - 182.94.152.5

Discovered: 2021-03-05 08:09:33.115568

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
514	tcp	shell	

Web Vulnerabilities

58.2.243.173 - ind-dlf-gsd-dps-sw-02.genpact.com

Discovered: 2021-03-05 08:09:33.16315

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f600001de400001e023a022f94e3ec56b574395950c54f234b71b152f3e3ec65c70f5c2920e3ec65c70f5c2920

Web Vulnerabilities

10.75.162.93 - 10.75.162.93

Discovered: 2021-03-05 08:09:33.208729

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
443	tcp	https	

Web Vulnerabilities

182.94.220.20 - ind-hyr-gsd-bus-rt-02.genpact.com

Discovered: 2021-03-05 08:09:33.257053

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000270b00001af43a022f94e3ec63c7be354188c54f234b71b152f3e3ec65c958106340e3ec65c958106340

Web Vulnerabilities

58.2.241.16 - loopback0-ind-dlf-bus-rt-01

Discovered: 2021-03-05 08:09:33.303805

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f600001ddb00001f313a022f94e3ec60d22bc6a868c54f234b71b152f3e3ec65c6a1062698e3ec65c6a1062698

Web Vulnerabilities

58.2.40.4 - ind-dlf-gsd-int-rt-01.genpact.com

Discovered: 2021-03-05 08:09:33.351727

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
123	udp	ntp	240504f600001da3000029d63a022f94e3ec50384ccccda0c54f234b71b152f3e3ec65c48353f938e3ec65c48353f938

Web Vulnerabilities

10.70.244.51 - ind-con-gsd-bus-rt-01.genpact.com

Discovered: 2021-03-05 08:09:33.374011

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25

Web Vulnerabilities

58.2.69.60 - ind-hyd-gsd-bus-02.genpact.com

Discovered: 2021-03-05 08:09:33.422995

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.75.178.179 - 10.75.178.179

Discovered: 2021-03-05 08:09:33.444183

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.64.6 - ind-hyd-gsd-il2-sw-52.genpact.com

Discovered: 2021-03-05 08:09:33.464826

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000269b00001e953a022f94e3ec57e3d374beb0c54f234b71b152f3e3ec65c618937500e3ec65c618937500

Web Vulnerabilities

124.4.225.74 - GCPWGTGUA1SCCM1

Discovered: 2021-03-05 08:09:33.511712

Operating System: Windows 2012 R2

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
53	tcp	dns	
80	tcp	http	Microsoft-IIS/8.5 (Powered by ASP.NET)
135	tcp	dcerpc	Endpoint Mapper (289 services)
139	tcp	smb	
443	tcp	https	Microsoft-IIS/8.5 (Powered by ASP.NET)
445	tcp	smb	Windows 2012 R2 Standard (build:9600) (name:GCPWGTGUA1SCCM1) (domain:MEXCORP)
1025	tcp	dcerpc	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0
1026	tcp	dcerpc	3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 DHCP Client LRPC Endpoint
1027	tcp	dcerpc	58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 AppInfo
1028	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
1036	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
1433	tcp	mssql	
3389	tcp	ms-wbt-server	
5040	tcp	dcerpc	1a927394-352e-4553-ae3f-7cf4aafca620 v1.0
5985	tcp	winrm	Microsoft-HTTPAPI/2.0 Authentication Methods: ["Negotiate", "Kerberos"]
22094	tcp	dcerpc	367abb81-9844-35f1-ad32-98f038001003 v2.0
44808	tcp	dcerpc	50abc2a4-574d-40b3-9d66-ee4fd5fba076 v5.0
44821	tcp	dcerpc	5b821720-f63b-11d0-aad2-00c04fc324db v1.0
44829	tcp	dcerpc	6b5bdd1e-528c-422c-af8c-a4079be4fe48 v1.0 Remote Fw APIs
47001	tcp	winrm	

Web Vulnerabilities

182.94.138.18 - ind-hyr-gsd-bus-fw-02.genpact.com

Discovered: 2021-03-05 08:09:33.76555

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

182.94.96.226 - 182.94.96.226

Discovered: 2021-03-05 08:09:33.789035

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.58.33 - ind-hyd-gsd-il2-sw-61.genpact.com

Discovered: 2021-03-05 08:09:33.81075

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000268900001e483a022f94e3ec6125b8d4fff0c54f234b71b152f3e3ec65c57f7ceef0e3ec65c57f7ceef0

Web Vulnerabilities

119.43.85.150 - 119.43.85.150

Discovered: 2021-03-05 08:09:33.858315

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_7.4
443	tcp	https	Apache

Web Vulnerabilities

182.94.138.118 - ind-hyr-gsd-dps-sw-01.genpact.com

Discovered: 2021-03-05 08:09:33.959533

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f6000028690000199ab65eb0c5e3ec634f0ac08330c54f234b71b152f3e3ec65c89b22d290e3ec65c89b22d290

Web Vulnerabilities

10.75.162.76 - 10.75.162.76

Discovered: 2021-03-05 08:09:34.005393

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
443	tcp	https	

Web Vulnerabilities

58.2.40.3 - ind-dlf-gsd-il2-sw-01.genpact.com

Discovered: 2021-03-05 08:09:34.052799

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
123	udp	ntp	240504f600001e2000002a2e3a022f94e3ec520ca0c49d60c54f234b71b152f3e3ec65c44b020d18e3ec65c44b020d18

Web Vulnerabilities

58.2.38.25 - 58.2.38.25

Discovered: 2021-03-05 08:09:34.074375

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.100.254.195 - ind-cos-gsd-bus-rt-01.genpact.com

Discovered: 2021-03-05 08:09:34.096009

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	NTP v4 (unsynchronized)

Web Vulnerabilities

58.2.243.180 - ind-hyd-gsd-dps-sw-01.genpact.com

Discovered: 2021-03-05 08:09:34.143119

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000268a00001a493a022f94e3ec5eea2978d570c54f234b71b152f3e3ec65c71b22d130e3ec65c71b22d130

Web Vulnerabilities

10.74.243.52 - 10.74.243.52

Discovered: 2021-03-05 08:09:34.191105

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.37.54 - ind-dlf-gsd-bus-fw-02.genpact.com

Discovered: 2021-03-05 08:09:34.212017

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.75.178.181 - 10.75.178.181

Discovered: 2021-03-05 08:09:34.231905

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.64.3 - ind-hyd-gsd-il2-sw-51.genpact.com

Discovered: 2021-03-05 08:09:34.253316

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000268900001afa3a022f94e3ec5f2091eb86b0c54f234b71b152f3e3ec65c5cc49bc90e3ec65c5cc49bc90

Web Vulnerabilities

10.75.178.63 - 10.75.178.63

Discovered: 2021-03-05 08:09:34.30162

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.241.2 - loopback0-ind-upl-bus-rt-02

Discovered: 2021-03-05 08:09:34.32327

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000268600001db43a022f94e3ec62d90c8b43b8c54f234b71b152f3e3ec65c69db22ec0e3ec65c69db22ec0

Web Vulnerabilities

10.100.250.53 - 10.100.250.53

Discovered: 2021-03-05 08:09:34.369191

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.70.244.52 - ind-con-gsd-bus-rt-02.genpact.com

Discovered: 2021-03-05 08:09:34.391166

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25

Web Vulnerabilities

10.70.244.59 - ind-con-gsd-int-rt-02.genpact.com

Discovered: 2021-03-05 08:09:34.43468

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25

Web Vulnerabilities

58.2.58.21 - ind-hyd-gsd-int-pa-01.genpact.com

Discovered: 2021-03-05 08:09:34.505647

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

58.2.241.1 - loopback0-ind-upl-bus-rt-01

Discovered: 2021-03-05 08:09:34.527331

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000278600005a263a022f94e3ec250989374d40c54f234b71b152f3e3ec65c66872b140e3ec65c66872b140

Web Vulnerabilities

58.2.37.53 - ind-dlf-gsd-bus-fw-01.genpact.com

Discovered: 2021-03-05 08:09:34.583305

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

10.100.252.5 - ind-cos-gsd-int-fw-01.genpact.com

Discovered: 2021-03-05 08:09:34.605156

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_12.1
443	tcp	https	(302-/php/login.php)

Web Vulnerabilities

58.2.243.181 - ind-hyd-gsd-dps-sw-02.genpact.com

Discovered: 2021-03-05 08:09:34.674559

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000274d00001a863a022f94e3ec615347ef9e78c54f234b71b152f3e3ec65c759db23c8e3ec65c759db23c8

Web Vulnerabilities

119.43.85.227 - GCPWINHYD2OKT01

Discovered: 2021-03-05 08:09:34.721532

Operating System: Windows 2012 R2

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
80	tcp	http	Microsoft-IIS/8.5 (Powered by ASP.NET)
135	tcp	dcerpc	Endpoint Mapper (272 services)
139	tcp	smb	
445	tcp	smb	Windows 2012 R2 Standard (build:9600) (name:GCPWINHYD2OKT01) (domain:INDCORP)
1025	tcp	dcerpc	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0
1026	tcp	dcerpc	3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 DHCP Client LRPC Endpoint
1027	tcp	dcerpc	58e604e8-9adb-4d2e-a464-3b0683fb1480 v1.0 AppInfo
3389	tcp	ms-wbt-server	
5986	tcp	winrm	Microsoft-HTTPAPI/2.0 Authentication Methods: ["Negotiate", "Kerberos"]
22617	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
47001	tcp	winrm	
52986	tcp	dcerpc	b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 v2.0 KeyIso
52987	tcp	dcerpc	76f03f96-cdfd-44fc-a22c-64950a001209 v1.0
53001	tcp	dcerpc	6b5bdd1e-528c-422c-af8c-a4079be4fe48 v1.0 Remote Fw APIs
65090	tcp	dcerpc	367abb81-9844-35f1-ad32-98f038001003 v2.0

Web Vulnerabilities

182.94.128.1 - ind-hyr-gsd-cor-sw.genpact.com

Discovered: 2021-03-05 08:09:34.943945

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25

Web Vulnerabilities

58.2.69.59 - ind-hyd-gsd-bus-01.genpact.com

Discovered: 2021-03-05 08:09:34.989066

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

182.94.138.77 - 182.94.138.77

Discovered: 2021-03-05 08:09:35.010148

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000271a00001fbf3a022f94e3ec5af4ddf3b8a8c54f234b71b152f3e3ec65c890624f60e3ec65c890624f60

Web Vulnerabilities

58.2.58.181 - ind-upl-acs-01.ind.corp.ad

Discovered: 2021-03-05 08:09:35.056058

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_7.6 PKIX[11.0]
80	tcp	http	(302-https://58.2.58.181:443/admin/)
443	tcp	https	(302-https://58.2.58.181:443/admin/)
8443	tcp	https	server (302-https://58.2.58.181:8443/portal/)

Port	Protocol	Name	Info
8444	tcp	https	server (302-https://58.2.58.181:8444/portal/)
8445	tcp	copy	

Web Vulnerabilities

10.100.254.196 - ind-cos-gsd-bus-rt-02.genpact.com

Discovered: 2021-03-05 08:09:35.235665

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	NTP v4 (unsynchronized)

Web Vulnerabilities

58.2.38.26 - 58.2.38.26

Discovered: 2021-03-05 08:09:35.279568

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

119.43.12.30 - 119.43.12.30

Discovered: 2021-03-05 08:09:35.3016

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

182.94.138.17 - 182.94.138.17

Discovered: 2021-03-05 08:09:35.321181

Operating System: Unknown

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-OpenSSH_12.1
443	tcp	https	(302-/php/login.php)

Web Vulnerabilities

58.2.58.34 - ind-hyd-gsd-il2-sw-62.genpact.com

Discovered: 2021-03-05 08:09:35.385808

Operating System: IOS

Credentials

Successful Attacks

Active Services

Port	Protocol	Name	Info
22	tcp	ssh	SSH-2.0-Cisco-1.25
123	udp	ntp	240504f60000269900001e1a3a022f94e3ec5ab456872bf0c54f234b71b152f3e3ec65c58ac08490e3ec65c58b020dc8

Web Vulnerabilities

10.100.254.194 - ind-cos-gsd-int-rt-02.genpact.com

Discovered: 2021-03-05 08:09:35.428851

Operating System: Unknown

Credentials

Successful Attacks

Web Vulnerabilities

Service Table

Service/Port	Instances
ssh/22	40
ntp/123	31
https/443	12
http/80	6
dcerpc/135	5
smb/139	5
smb/445	5
ms-wbt-server/3389	5
dcerpc/1025	4
dcerpc/1026	4
dcerpc/1027	4
shell/514	3
https/8443	3
copy/8445	3
winrm/47001	3
dns/53	2
winrm/5986	2
https/8444	2
http/9090	2
tacacs/49	1
ldap/389	1
dcerpc/1028	1
dcerpc/1029	1
dcerpc/1036	1
dcerpc/1058	1
mssql/1433	1
dcerpc/5040	1
winrm/5985	1
unknown/8014	1
dynamid/9002	1
dcerpc/17000	1
dcerpc/22094	1
dcerpc/22617	1
dcerpc/30792	1
dcerpc/30812	1
dcerpc/39705	1
dcerpc/39709	1
dcerpc/39745	1
dcerpc/44808	1
dcerpc/44821	1
dcerpc/44829	1
dcerpc/49664	1
dcerpc/49665	1

Service/Port	Instances
dcerpc/50000	1
dcerpc/52986	1
dcerpc/52987	1
dcerpc/53001	1
dcerpc/54004	1
dcerpc/57186	1
dcerpc/61447	1
dcerpc/61450	1
dcerpc/61452	1
dcerpc/61458	1
dcerpc/65090	1