The Queen's College IT Open Morning

OpenVAS

What does it do?

- Penetration Testing/Vulnerability Scanning
- Both authenticated and unauthenticated scans
- Detects out of date software
- Tells you about software you probably didn’t know was installed
- Highlights known bad configurations

Alternatives…

- Nessus
  - Hosted internally
  - or via IT Services
- Nmap
- Kali Linux (a full suite of tools including OpenVAS)

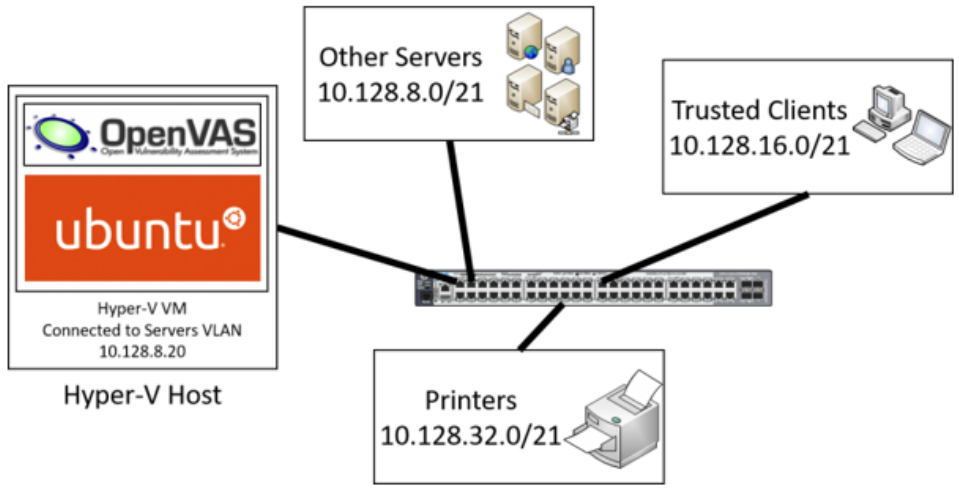
A Windows SysAdmin Installs OpenVAS

http://myworldofit.net/?series=a-windows-sysadmin-installs-and-uses-openvas

A Windows SysAdmin installs and uses OpenVAS – End to end guide – Installation

Published 25 July, 2017 | By James Preston

This entry is part 1 of 4 in the series A Windows SysAdmin installs and uses OpenVAS



This guide covers one (of I'm sure a 1,000) ways to deploy and use OpenVAS 9 in your environment on Ubuntu Server 16.04 for the purpose of White Hat Penetration Testing, more so it's also written from the viewpoint of a SysAdmin who mainly works with Windows Systems (Windows Server/Hyper-V/PowerShell/suchlike) and so takes a very simplistic approach to the setup.

The goals of this project are to

- Install Ubuntu Server 16.04 LTS on Hyper-V
- Deploy OpenVAS to that server
- Execute scripted commands against OpenVAS from a remote system
- Light up with a big warning sign all of the unknown issues within a network

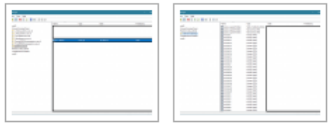
Lets get started!

To start out you will need

- A Hyper-V host (although no reason not to run it on VMWare/whatnot)
- The latest ISO for Ubuntu Server 16.04 LTS saved somewhere your Hyper-V server can get to
  - Download from – https://www.ubuntu.com/download/server
  - Worth noting that only the 16.04 LTS release is going to work with this guide, when I first tried getting OpenVAS to work with 17.04 (a newer release) there were various blocking issues that I could not overcome. In short – use 16.04!!!

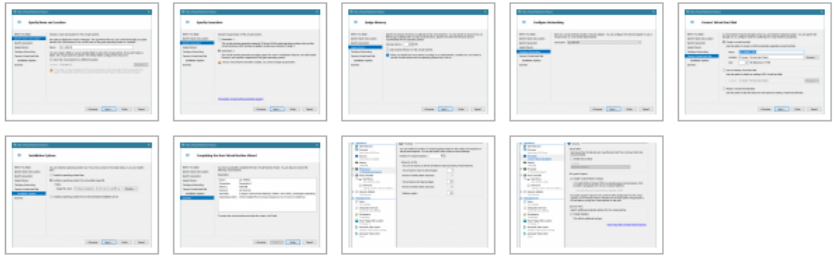
Step 0 – Get DNS in the right place

Configuring DNS correctly in particular with relation to Reverse Lookup will help your OpenVAS deployment loads, for a good guide on how to setup Reverse Lookup take a look at this link – http://de.community.dell.com/techcenter/os-applications/w/wiki/684.how-to-configure-dns-reverse-lookup-zone-in-windows-server-2012 (don't worry about the de. its in English!).



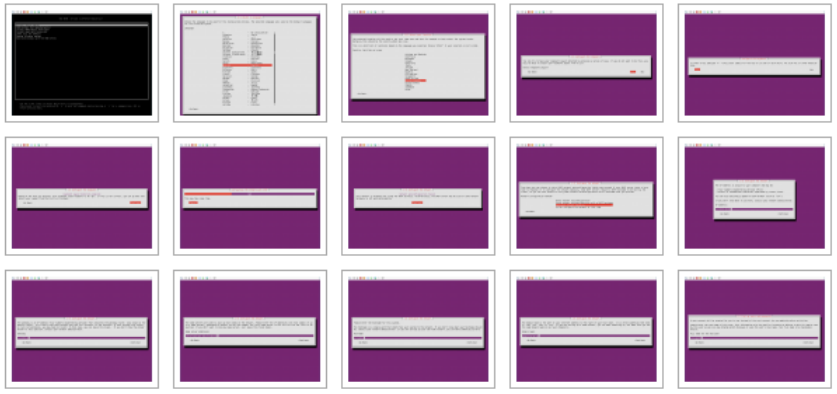
Step 1 – Configure a Hyper-V VM for OpenVAS

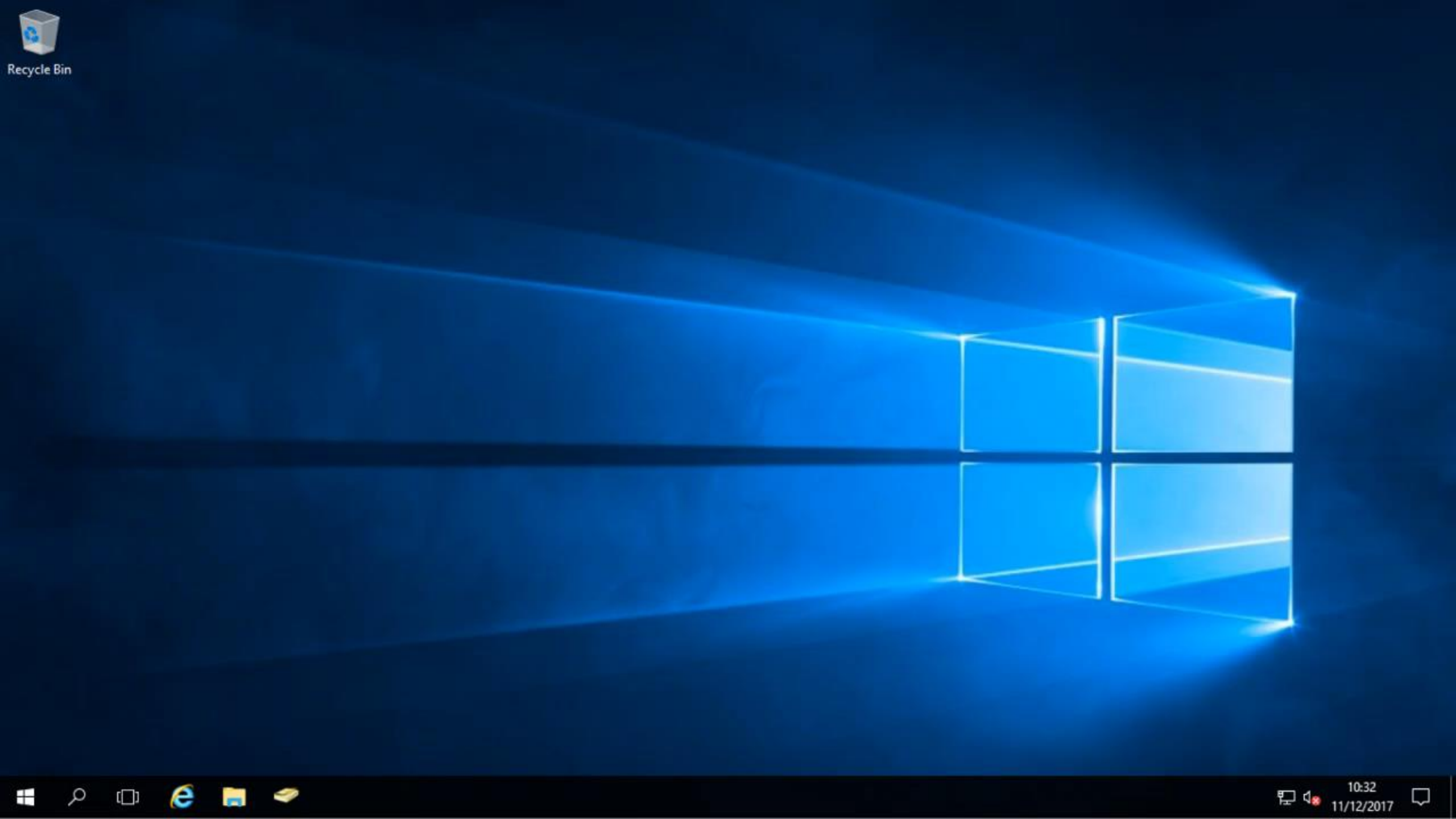
In this next step we configure a Hyper-V VM running on Windows Hyper-V Server 2016 (which is free by the way!).

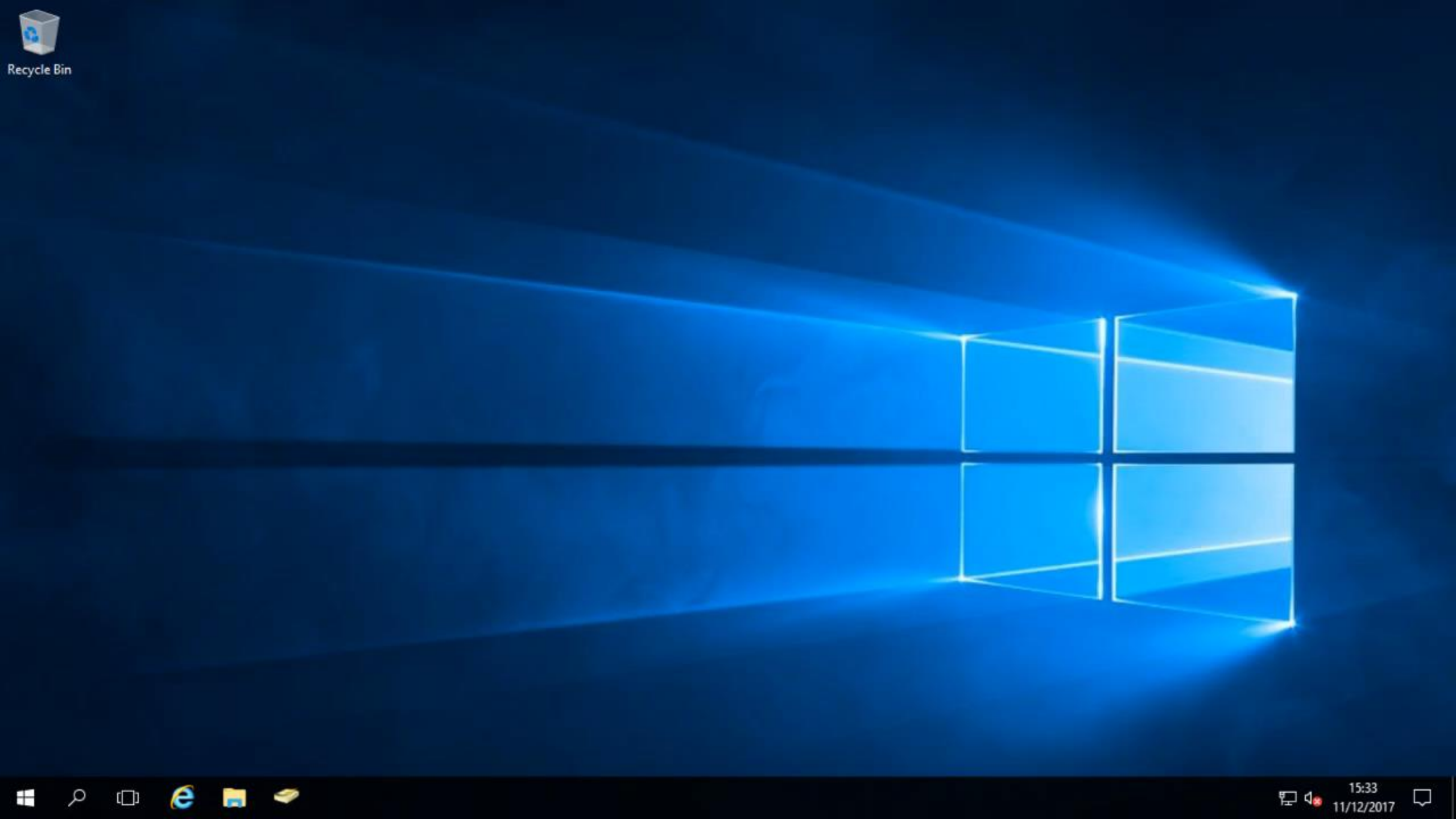


Step 2 – Install Ubuntu Server

Next up the install of Ubuntu Linux, as I understand OpenVAS can be installed on all kinds of flavours of Linux however the support I've seen in the past around Ubuntu seems much better than other options. This portion of the guide assumes you are not running your OpenVAS server on a network that's got DHCP enabled (in this example it's on our Servers VLAN).




Recycle Bin
10:32
11/12/2017


Recycle Bin
15:33
11/12/2017

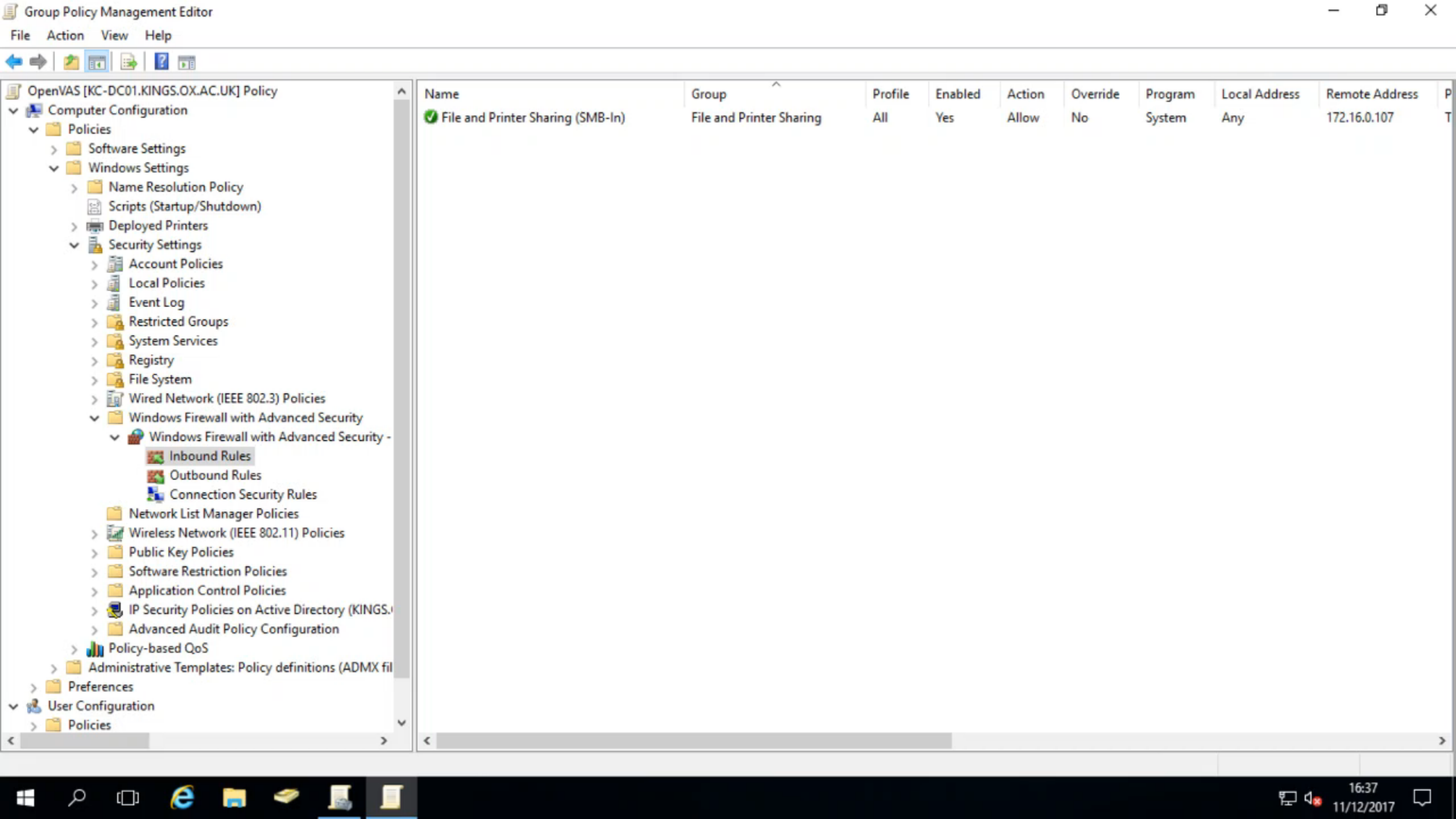
Group Policy Management Editor

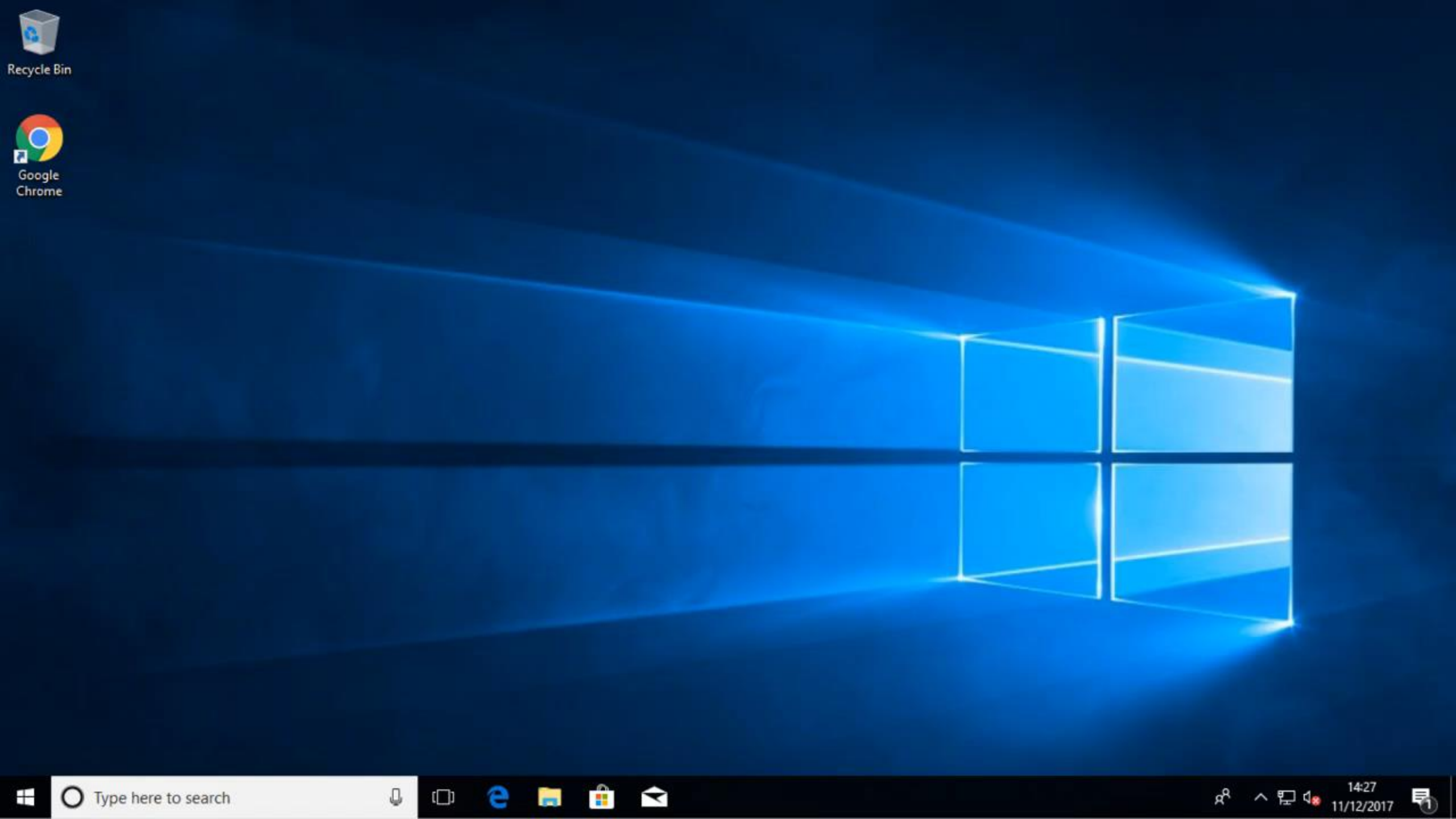
File Action View Help

OpenVAS [KC-DC01.KINGS.OX.AC.UK] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Polici
        - Windows Firewall with Advanced
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Pc
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active Dire
        - Advanced Audit Policy Configura
      - Policy-based QoS
    - Administrative Templates: Policy definiti
  - Preferences
- User Configuration
  - Policies
  - Preferences

Service Name	Startup	Permission
Radio Management Service	Not Defined	Not Defined
Remote Access Auto Con...	Not Defined	Not Defined
Remote Access Connecti...	Not Defined	Not Defined
Remote Desktop Configur...	Not Defined	Not Defined
Remote Desktop Services	Not Defined	Not Defined
Remote Desktop Services ...	Not Defined	Not Defined
Remote Procedure Call (R...	Not Defined	Not Defined
Remote Procedure Call (R...	Not Defined	Not Defined
Remote Registry	Automatic	Not Defined
Resultant Set of Policy Pr...	Not Defined	Not Defined
Routing and Remote Acc...	Not Defined	Not Defined
RPC Endpoint Mapper	Not Defined	Not Defined
Secondary Logon	Not Defined	Not Defined
Secure Socket Tunneling ...	Not Defined	Not Defined
Security Accounts Manager	Not Defined	Not Defined
Sensor Data Service	Not Defined	Not Defined
Sensor Monitoring Service	Not Defined	Not Defined
Sensor Service	Not Defined	Not Defined
Server	Not Defined	Not Defined
Shell Hardware Detection	Not Defined	Not Defined
Smart Card	Not Defined	Not Defined
Smart Card Device Enume...	Not Defined	Not Defined
Smart Card Removal Policy	Not Defined	Not Defined
SNMP Trap	Not Defined	Not Defined
Software Protection	Not Defined	Not Defined
Special Administration Co...	Not Defined	Not Defined
Spot Verifier	Not Defined	Not Defined
SSDP Discovery	Not Defined	Not Defined
State Repository Service	Not Defined	Not Defined
Still Image Acquisition Ev...	Not Defined	Not Defined
Storage Service	Not Defined	Not Defined
Storage Tiers Management	Not Defined	Not Defined

16:00
11/12/2017


Group Policy Management Editor
File Action View Help
OpenVAS [KC-DC01.KINGS.OX.AC.UK] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security -
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (KINGS.
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX fil
Preferences
User Configuration
Policies
Name
Group
Profile
Enabled
Action
Override
Program
Local Address
Remote Address
File and Printer Sharing (SMB-In)
File and Printer Sharing
All
Yes
Allow
No
System
Any
172.16.0.107
16:37
11/12/2017


Recycle Bin
Google Chrome
Type here to search
14:27
11/12/2017

Greenbone Security Ass

Certificate error https://kc-pen01.kings.ox.ac.uk:4000/omp?token=9071ddb2-d41c-42e0-864a-bddb2f1b7e69

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout
Mon Dec 11 14:30:54 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Dashboard

Tasks by Severity Class (Total: 0)

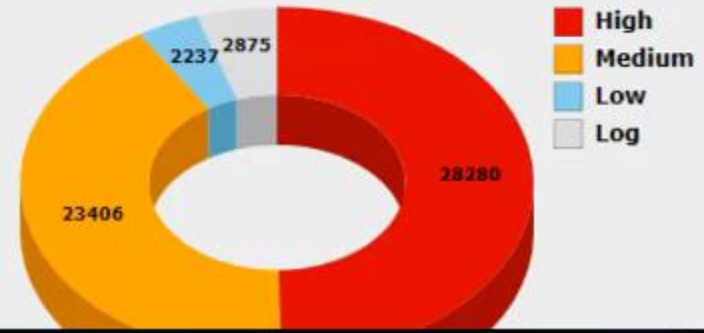
Tasks by status (Total: 0)

CVEs by creation time (Total: 98039)

Hosts topology

No hosts with topology selected

NVTs by Severity Class (Total: 56798)



Type here to search

14:32
11/12/2017

Greenbone Security Ass

Certificate error https://kc-pen01.kings.ox.ac.uk:4000/omp?cmd=get_credentials&token=9071ddb2-d41c-42e0-864a-bddb2f1b7e69

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout
Mon Dec 11 14:33:07 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Filter:

rows=10 first=1 sort=name

Credentials (1 of 1)

1 - 1 of 1

Name	Type	Allow insecure use	Login	Actions
Administrator	up (username + password)	No	kings\administrator	

√Apply to page conte...

(Applied filter: rows=10 first=1 sort=name)

1 - 1 of 1

Backend operation: 0.12s

Type here to search

14:34
11/12/2017

Greenbone Security Ass

Certificate error https://kc-pen01.kings.ox.ac.uk:4000/omp?cmd=get_targets&token=9071ddb2-d41c-42e0-864a-bddb2f1b7e69

Greenbone Security Assistant

No auto-refresh | Logged in as Admin **admin** | Logout
Mon Dec 11 14:34:54 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Filter:

rows=10 first=1 sort=name

Targets (1 of 1)

1 - 1 of 1

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Local Network	172.16.0.0/21	2046	All IANA assigned TCP 2012-02-10	SMB: Administrator	

√Apply to page conte...

(Applied filter: rows=10 first=1 sort=name)

1 - 1 of 1

Backend operation: 0.10s

Type here to search

14:34
11/12/2017

Greenbone Security Ass

Certificate error https://kc-pen01.kings.ox.ac.uk:4000/omp?cmd=get_task&task_id=de27fab4-7360-4fc0-9cb9-27f99d285fd7&overrides=1&min_qod=

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout
Mon Dec 11 14:37:46 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Task: Scan Local Network

ID: de27fab4-7360-4fc0-9cb9-27f99d285fd7
Created: Mon Dec 11 14:35:24 2017
Modified: Mon Dec 11 14:35:44 2017
Owner: admin

Name:	**Scan Local Network**
Comment:	
Target:	Local Network
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: Full and very deep
	Order for target hosts: Sequential
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 4
	Maximum concurrently scanned hosts: 20
Status:	1 %
Duration of last scan:	
Average scan duration:	
Reports:	1, Current: Dec 11 2017 (Finished: 0)
Results:	28
Notes:	0
Overrides:	0

User Tags (none)

Type here to search

14:37
11/12/2017

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
KC-ClientPC	Running	0%	4096 MB	03:43:40	
KC-ClientPCFast	Running	0%	4096 MB	03:14:36	
KC-DC01	Running	2%	2048 MB	4.23:09:54	
KC-Firewall	Running	0%	2048 MB	4.23:46:05	
KC-MDT01	Running	0%	2048 MB	4.23:06:58	
KC-PEN01	Running	88%	4096 MB	01:50:45	
KC-PRTG01	Running	0%	4096 MB	02:38:54	
KC-WSUS01	Running	3%	4096 MB	18:48:24	

Checkpoints

The selected virtual machine has no checkpoints.

Actions

QC-HYPERVTEST

- New
- Import Virtual Machine...
- Hyper-V Settings...
- Virtual Switch Manager...
- Virtual SAN Manager...
- Edit Disk...
- Inspect Disk...
- Stop Service
- Remove Server
- Refresh
- View
- New Window from Here
- Help

KC-PEN01

- Connect...
- Settings...
- Turn Off...
- Shut Down...
- Save
- Pause
- Reset

Greenbone Security Ass

Certificate error https://kc-pen01.kings.ox.ac.uk:4000/omp?cmd=get_reports&report_id=91ba7b64-26ca-4f26-a790-30367869d7ba&task_filt_id=&filt_i

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout
Mon Dec 11 22:55:53 2017 UTC

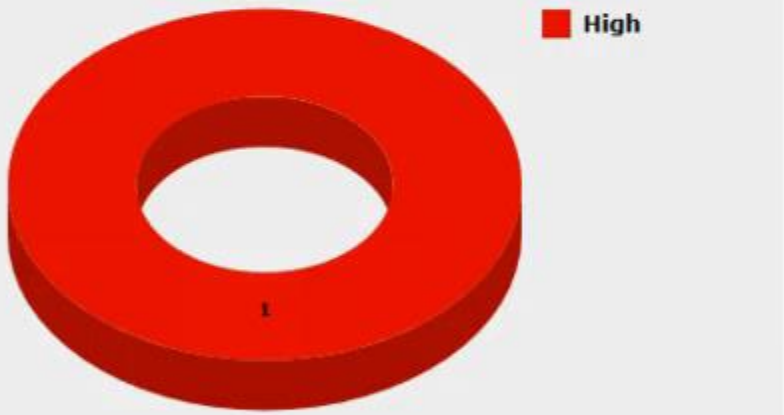
Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Filter:

task_id=de27fab4-7360-4fc0-9cb9-27f99d285fd7 apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10

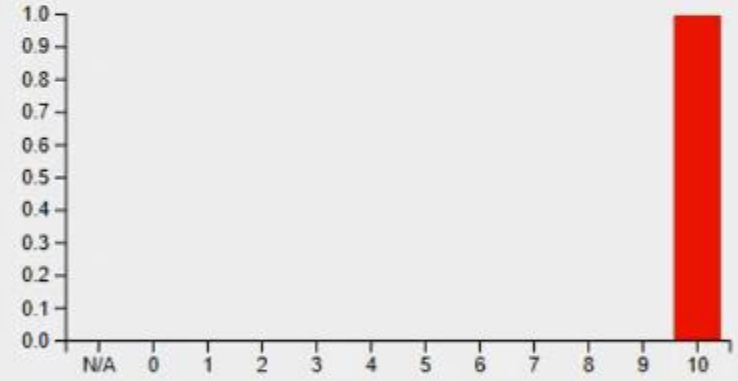
Reports (1 of 1)

Reports by Severity Class (Total: 1)



Reports: High results timeline

Reports by CVSS (Total: 1)



1 - 1 of 1

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Mon Dec 11 16:44:35 2017	Done	Scan Local Network	10.0 (High)	27	22	11	183	0	

√Apply to page conte...

(Applied filter: task_id=de27fab4-7360-4fc0-9cb9-27f99d285fd7 apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10)

1 - 1 of 1

Type here to search

22:56
11/12/2017

Name
Scan Application Servers - Monday
Scan Backup Servers - Tuesday
Scan Database Servers - Thursday
Scan Domain Controllers - Friday
Scan File Servers - Saturday
Scan Finance Servers - Sunday
Scan Hyper-V Hosts - Tuesday
Scan Print Servers - Thursday
Scan Public Websites
Scan VPN Servers - Friday
Scan Web Servers - Saturday
VLAN12 - Building Management System
VLAN13 - Out of Band
VLAN2 - Wired Infrastructure
VLAN4 - Wired Clients
VLAN5 - Wireless Clients
VLAN7 - Security
www.queens.ox.ac.uk

Vulnerability	Severity	QoD	Host
Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2014 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE Multiple Vulnerabilities -01 Feb 13 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 Oct 2013 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE JRE Multiple Unspecified Vulnerabilities-04 oct12 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE JRE Multiple Unspecified Vulnerabilities-02 oct12 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE Multiple Vulnerabilities -02 May 13 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE Multiple Vulnerabilities April 2016 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE Multiple Vulnerabilities -03 June 13 (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)
Oracle Java SE Java Runtime Environment Multiple Unspecified Vulnerabilities(01) - (Windows)	10.0 (High)	97%	10.128.16.60 (itof2017-001.queens.ox.ac.uk)

Vulnerability		Severity	QoD	Host	Location	Actions
Oracle Java SE Multiple Vulnerabilities -01 Feb 13 (Windows)		10.0 (High)	97%	10.128.16.60	general/tcp	

Summary
This host is installed with Oracle Java SE and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. Attackers can even execute arbitrary code on the target system. Impact Level: System/Application

Solution
Solution type: VendorFix

Apply patch from below link, http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html

Affected Software/OS
Oracle Java SE Version 7 Update 11 and earlier, 6 Update 38 and earlier, 5 Update 38 and earlier and 1.4.2_40 and earlier.

Vulnerability Insight
Multiple flaws due to unspecified errors in the following components: - Deployment - Scripting - COBRA - Sound - Beans - 2D - Networking - Libraries - Installation process of client - Abstract Window Toolkit (AWT) - Remote Method Invocation (RMI) - Java Management Extensions (JMX) - Java API for XML Web Services(JAX_WS) - Java Secure Socket Extension (JSSE)

Vulnerability Detection Method
Details: Oracle Java SE Multiple Vulnerabilities -01 Feb 13 (Windows) (OID: 1.3.6.1.4.1.25623.1.0.803307)

Version used: $Revision: 7699 $

References

CVE: CVE-2013-0431, CVE-2013-1489, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424, CVE-2012-3342, CVE-2012-3213, CVE-2012-1541, CVE-2013-1475, CVE-2013-0425, CVE-2013-0426, CVE-2013-0446, CVE-2013-0448, CVE-2013-0449, CVE-2013-0450, CVE-2013-1473, CVE-2013-1476, CVE-2013-1478, CVE-2013-1479, CVE-2013-1480, CVE-2013-0435, CVE-2013-0434, CVE-2013-0433, CVE-2013-0432, CVE-2013-0430, CVE-2013-0429, CVE-2013-0428, CVE-2013-0437, CVE-2013-0438, CVE-2013-1481, CVE-2013-0445, CVE-2013-0444, CVE-2013-0443, CVE-2013-0442, CVE-2013-0441, CVE-2013-0440, CVE-2013-0427

BID: 57707, 57702, 57708, 57712, 57715, 57719, 57723, 57724, 57726, 57728, 57681, 57686, 57687, 57689, 57691, 57692, 57694, 57696, 57697, 57699, 57700, 57703, 57706, 57709, 57711, 57713, 57717, 57718, 57701, 57704, 57710, 57714, 57716, 57720, 57722, 57727, 57731, 57729, 57730

CERT: DFN-CERT-2013-0590, DFN-CERT-2013-0589, DFN-CERT-2013-0576, DFN-CERT-2013-0574, DFN-CERT-2013-0573, DFN-CERT-2013-0572, DFN-CERT-2013-0565, DFN-CERT-2013-0564, DFN-CERT-2013-0563, DFN-CERT-2013-0555, DFN-CERT-2013-0539, DFN-CERT-2013-0526, DFN-CERT-2013-0525, DFN-CERT-2013-0520, DFN-CERT-2013-0466, DFN-CERT-2013-0460, DFN-CERT-2013-0339, DFN-CERT-2013-0333, DFN-CERT-2013-0258, DFN-CERT-2013-0257, DFN-CERT-2013-0256, DFN-CERT-2013-0255, DFN-CERT-2013-0248, DFN-CERT-2013-0233, DFN-CERT-2013-0230, DFN-CERT-2013-0228, DFN-CERT-2013-0227

Other: http://securitytracker.com/id/1028071

http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html

Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.
Microsoft Skype DLL Hijacking Vulnerability		7.2 (High)	97%	10.128.

Owner: admin

Result: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Vulnerability		Severity	QoD	Host	Location	Actions
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	10.128.16.4	3389/tcp	

Summary
The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject:              CN=QueensCollege
Signature Algorithm:  sha1WithRSAEncryption
```

Solution
Solution type: Mitigation

Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings.

Vulnerability Insight
Secure Hash Algorithm 1 (SHA-1) is considered cryptographically weak and not secure enough for ongoing use. Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when users visit web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

Vulnerability Detection Method
Check which algorithm was used to sign the remote SSL/TLS Certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: $Revision: 4781 $

References

Other: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Result: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

ID: e7753baf-0550-45fe-8adb-d68a2c615736
Created: Mon Dec 11 10:33:00 2017
Modified: Mon Dec 11 10:33:00 2017
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	10.128.16.2	443/tcp	

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

Solution
Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Version used: $Revision: 5232 $

References

CVE: CVE-2016-2183, CVE-2016-6329

CERT: CB-K17/1055, CB-K17/1026, CB-K17/0939, CB-K17/0917, CB-K17/0915, CB-K17/0877, CB-K17/0796, CB-K17/0724, CB-K17/0661, CB-K17/0657, CB-K17/0582, CB-K17/0581, CB-K17/0506, CB-K17/0504, CB-K17/0467, CB-K17/0345, CB-K17/0098, CB-K17/0089, CB-K17/0086, CB-K17/0082, CB-K16/1837, CB-K16/1830, CB-K16/1635, CB-K16/1630, CB-K16/1624, CB-K16/1622, CB-K16/1500, CB-K16/1465, CB-K16/1307, CB-K16/1296, DFN-CERT-2017-2070, DFN-CERT-2017-1954, DFN-CERT-2017-1885, DFN-CERT-2017-1831, DFN-CERT-2017-1821, DFN-CERT-2017-1785, DFN-CERT-2017-1626, DFN-CERT-2017-1326, DFN-CERT-2017-1239, DFN-CERT-2017-1238, DFN-CERT-2017-1090, DFN-CERT-2017-1060, DFN-CERT-2017-0968, DFN-CERT-2017-0947, DFN-CERT-2017-0946, DFN-CERT-2017-0904, DFN-CERT-2017-0816, DFN-CERT-2017-0746, DFN-CERT-2017-0677, DFN-CERT-2017-0675, DFN-CERT-2017-0611, DFN-CERT-2017-0609, DFN-CERT-2017-0522, DFN-CERT-2017-0519, DFN-CERT-2017-0482, DFN-CERT-2017-0351, DFN-CERT-2017-0090, DFN-CERT-2017-0089, DFN-CERT-2017-0088, DFN-CERT-2017-0086, DFN-CERT-2016-1943, DFN-CERT-2016-1937, DFN-CERT-2016-1732, DFN-CERT-2016-1726, DFN-CERT-2016-1715, DFN-CERT-2016-1714, DFN-CERT-2016-1588, DFN-CERT-2016-1555, DFN-CERT-2016-1391, DFN-CERT-2016-1378

Other: https://bettercrypto.org/

https://mozilla.github.io/server-side-tls/ssl-config-generator/

https://sweet32.info/

Block Ciphers and the Birthday Bound

Exploiting Block Cipher Collisions

64-bit Block Cipher Usage on the Internet

Attacking Authenticated HTTP over TLS and OpenVPN

Impact and Mitigation

FAQ

About us

Paper

Slides

Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN

CVE-2016-2183, CVE-2016-6329

Cryptographic protocols like TLS, SSH, IPsec, and OpenVPN commonly use block cipher algorithms, such as AES, Triple-DES, and Blowfish, to encrypt data between clients and servers. To use such algorithms, the data is broken into fixed-length chunks, called blocks, and each block is encrypted separately according to a mode of operation. Older block ciphers, such as Triple-DES and Blowfish use a block size of 64 bits, whereas AES uses a block size of 128 bits.

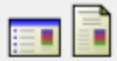
It is well-known in the cryptographic community that a short block size makes a block cipher vulnerable to birthday attacks, even if there are no cryptographic attacks against the block cipher itself. We observe that such attacks have now become practical for the common usage of 64-bit block ciphers in popular protocols like TLS and OpenVPN. Still, such ciphers are widely enabled on the Internet. Blowfish is currently the default cipher in OpenVPN, and Triple-DES is supported by nearly all HTTPS web servers, and currently used for roughly 1-2% of HTTPS connections between mainstream browsers and web servers.

We show that a network attacker who can monitor a long-lived Triple-DES HTTPS connection between a web browser and a website can recover secure HTTP cookies by capturing around 785 GB of traffic. In our proof-of-concept demo, this attack currently takes less than two days, using malicious Javascript to generate traffic. Keeping a web connection alive for two days may not seem very practical, but it worked easily in the lab. In terms of computational complexity, this attack is comparable to the recent attacks on RC4. We also demonstrate a similar attack on VPNs that use 64-bit ciphers, such as OpenVPN, where long-lived Blowfish connections are the norm.

Countermeasures are currently being implemented by browser vendors, OpenSSL, and the OpenVPN team, and we advise users to update to the latest available versions.

Our results are described in the following technical paper, presented at ACM CCS 2016:

On the Practical (In-)Security of 64-bit Block Ciphers — Collision Attacks on HTTP over TLS and OpenVPN
Karthikeyan Bhargavan, Gaëtan Leurent



Block Ciphers and the Birthday Bound

The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2^k.

IIS Crypto

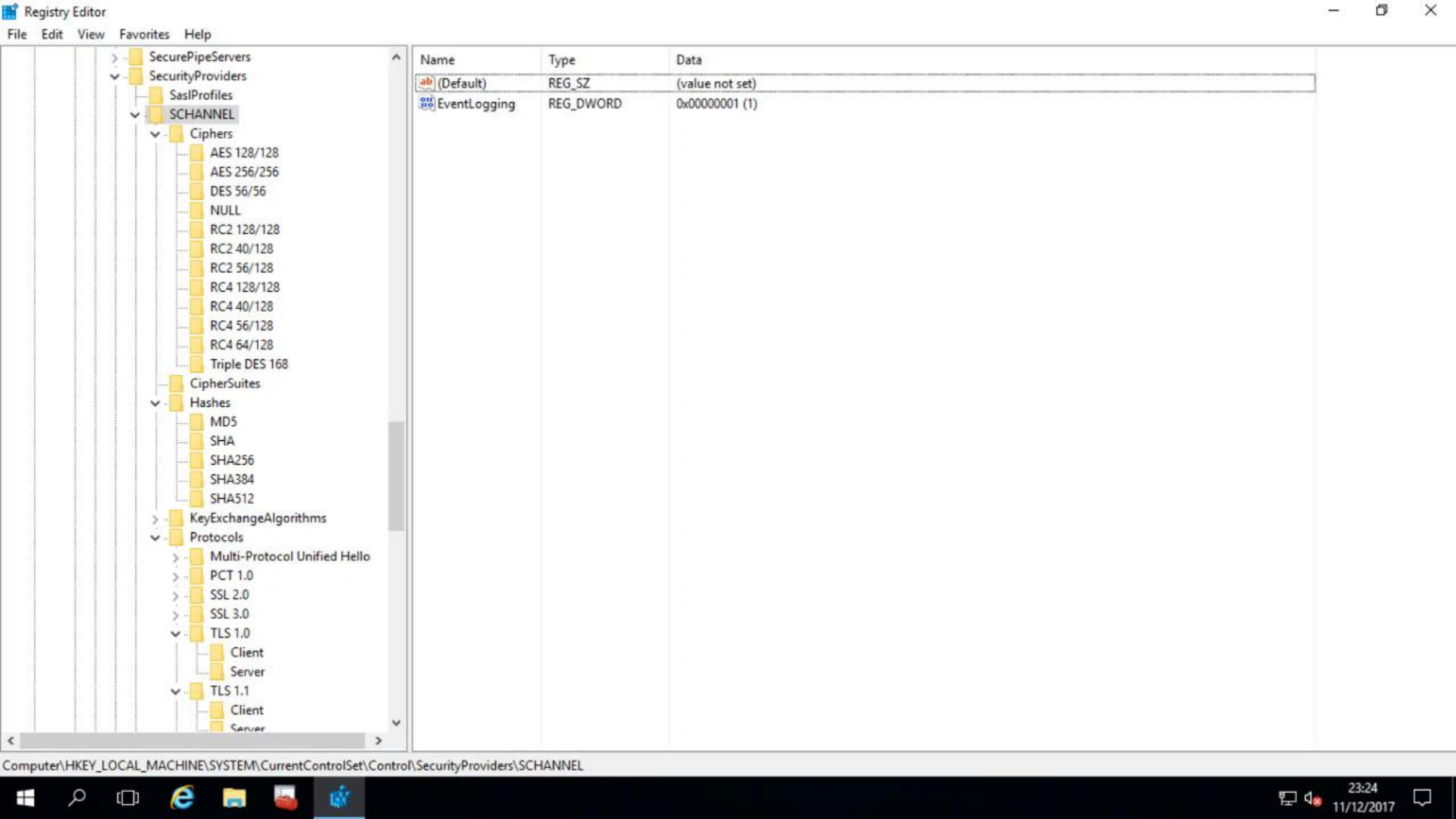
https://www.nartac.com/Products/IISCrypto/

NARTAC SOFTWARE

IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2008, 2012 and 2016. It also lets you reorder SSL/TLS cipher suites offered by IIS, implement best practices with a single click, create custom templates and test your website.

Features

- ✓ Single click to secure your website using best practices
- ✓ Create custom templates that can be saved and run on multiple servers
- ✓ Stop DROWN, logjam, FREAK, POODLE and BEAST attacks
- ✓ Disable weak protocols and ciphers such as SSL 2.0, 3.0 and MD5
- ✓ Enable TLS 1.1 and 1.2
- ✓ Enable forward secrecy
- ✓ Reorder cipher suites
- ✓ Built in Best Practices, PCI, PCI 3.1 and FIPS 140-2 templates


Registry Editor
File Edit View Favorites Help
SecurePipeServers
SecurityProviders
SaslProfiles
SCHANNEL
Ciphers
AES 128/128
AES 256/256
DES 56/56
NULL
RC2 128/128
RC2 40/128
RC2 56/128
RC4 128/128
RC4 40/128
RC4 56/128
RC4 64/128
Triple DES 168
CipherSuites
Hashes
MD5
SHA
SHA256
SHA384
SHA512
KeyExchangeAlgorithms
Protocols
Multi-Protocol Unified Hello
PCT 1.0
SSL 2.0
SSL 3.0
TLS 1.0
Client
Server
TLS 1.1
Client
Name
Type
Data
(Default)
REG_SZ
(value not set)
EventLogging
REG_DWORD
0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
23:24
11/12/2017

Further Reading

- OpenVAS http://www.openvas.org/
- myworldofit.net http://myworldofit.net/?series=a-windows-sysadmin-installs-and-uses-openvas
- Greenbone Security Manager https://www.greenbone.net/en/
- Kali Linux https://www.kali.org
- IIS Crypto https://www.nartac.com/Products/IISCrypto/
- Lynda.com https://www.lynda.com/Linux-tutorials/Introduction-Kali-Linux/455715-2.html