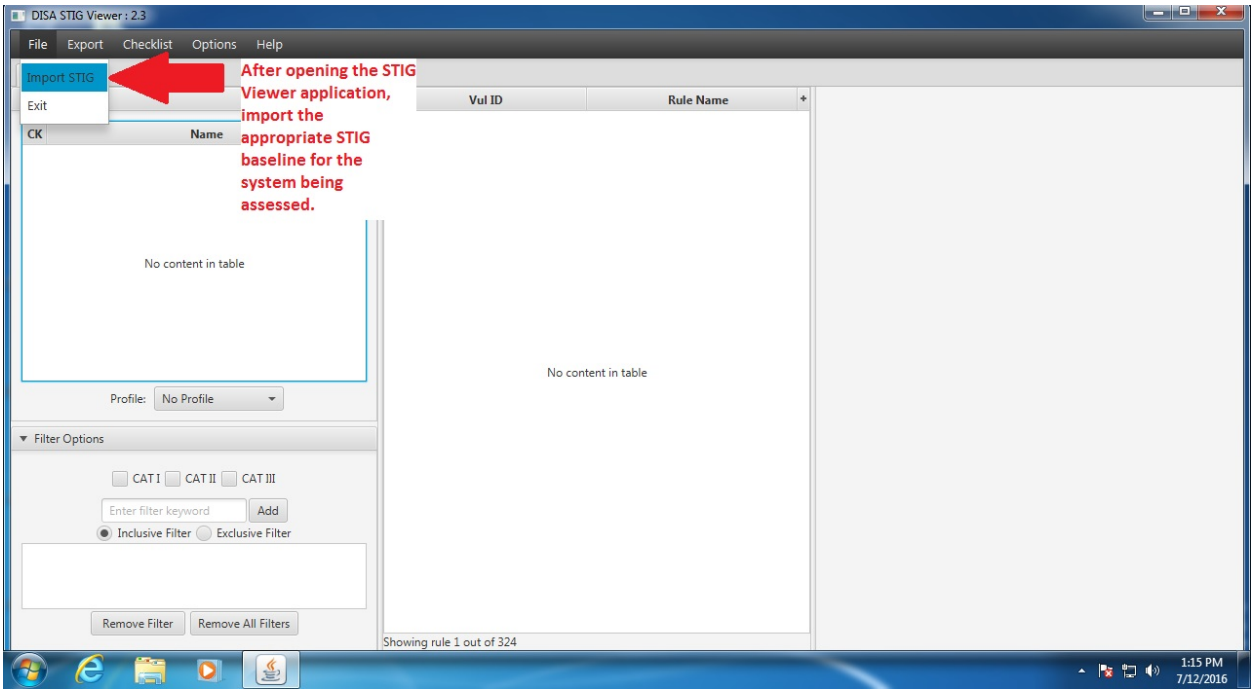
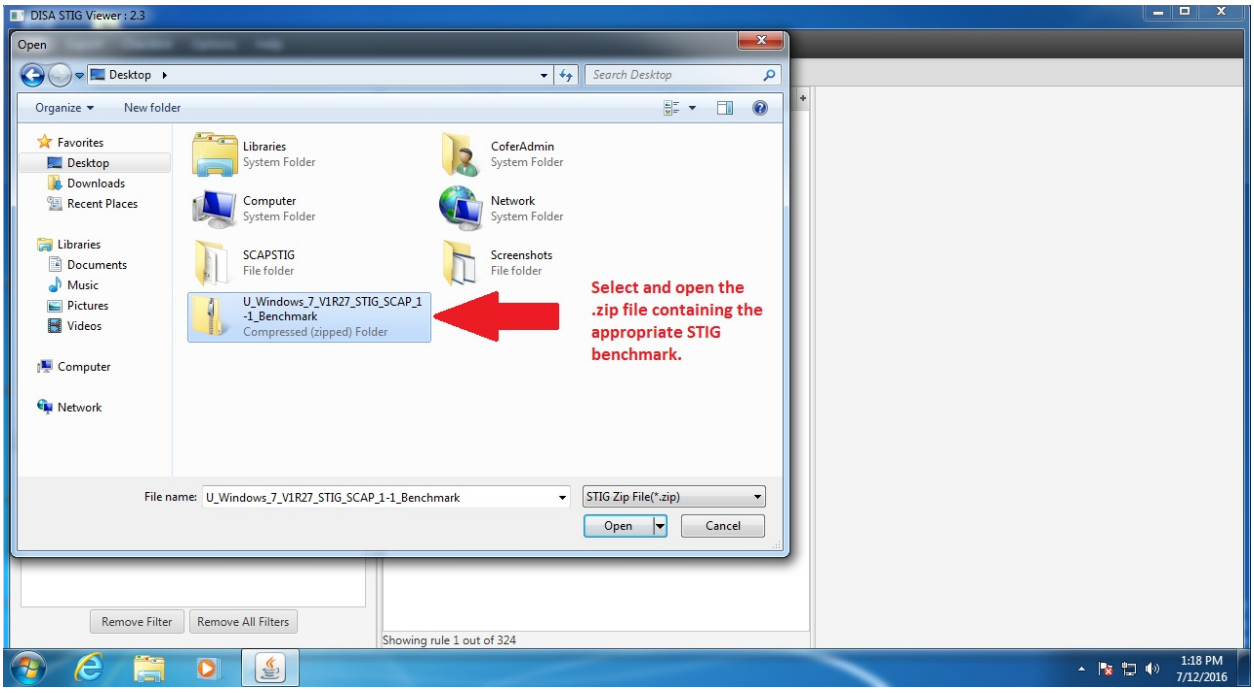
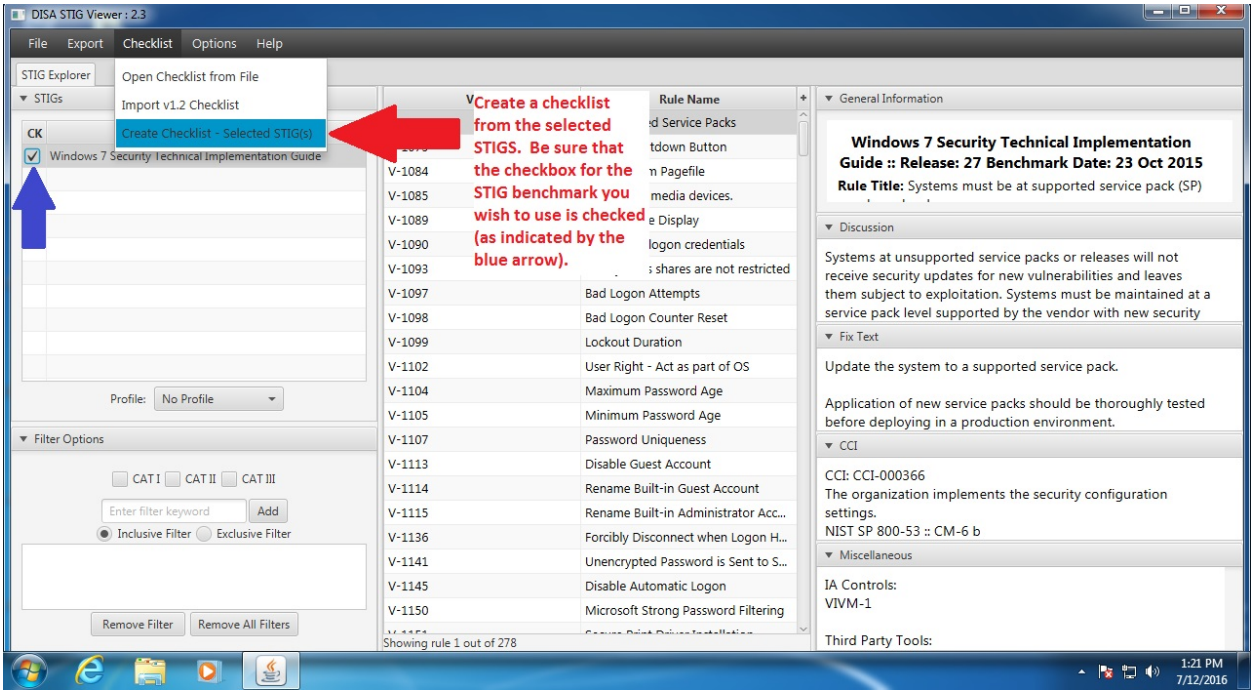
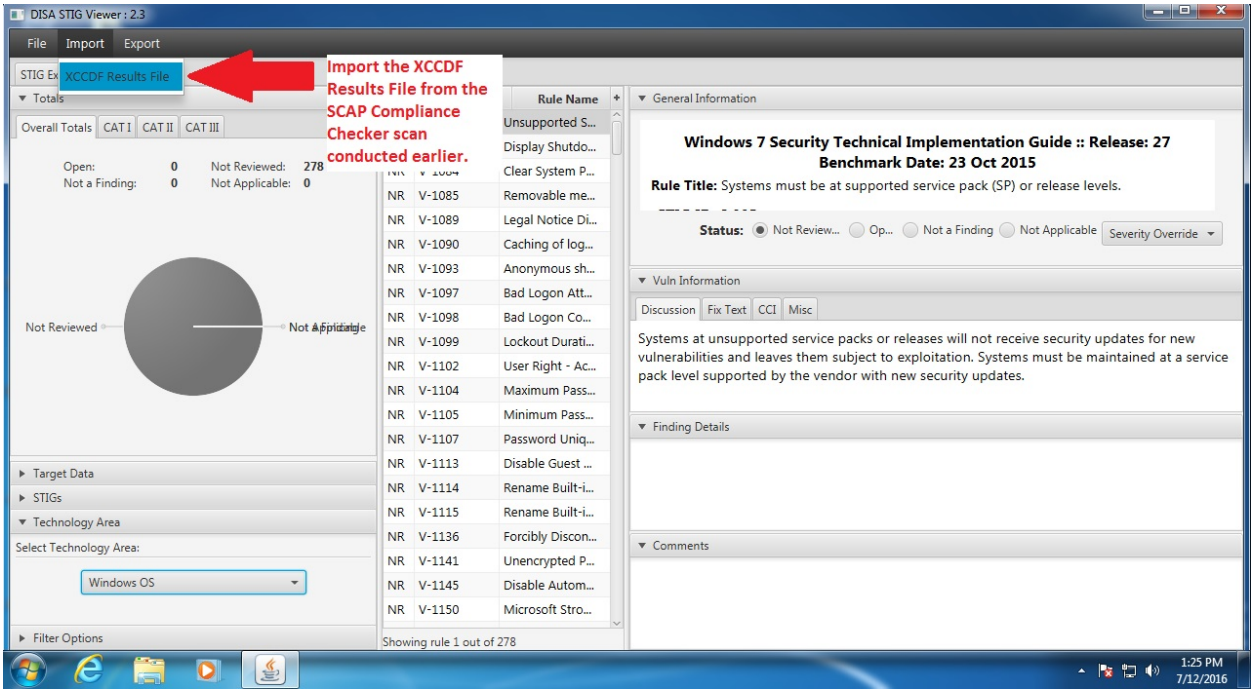
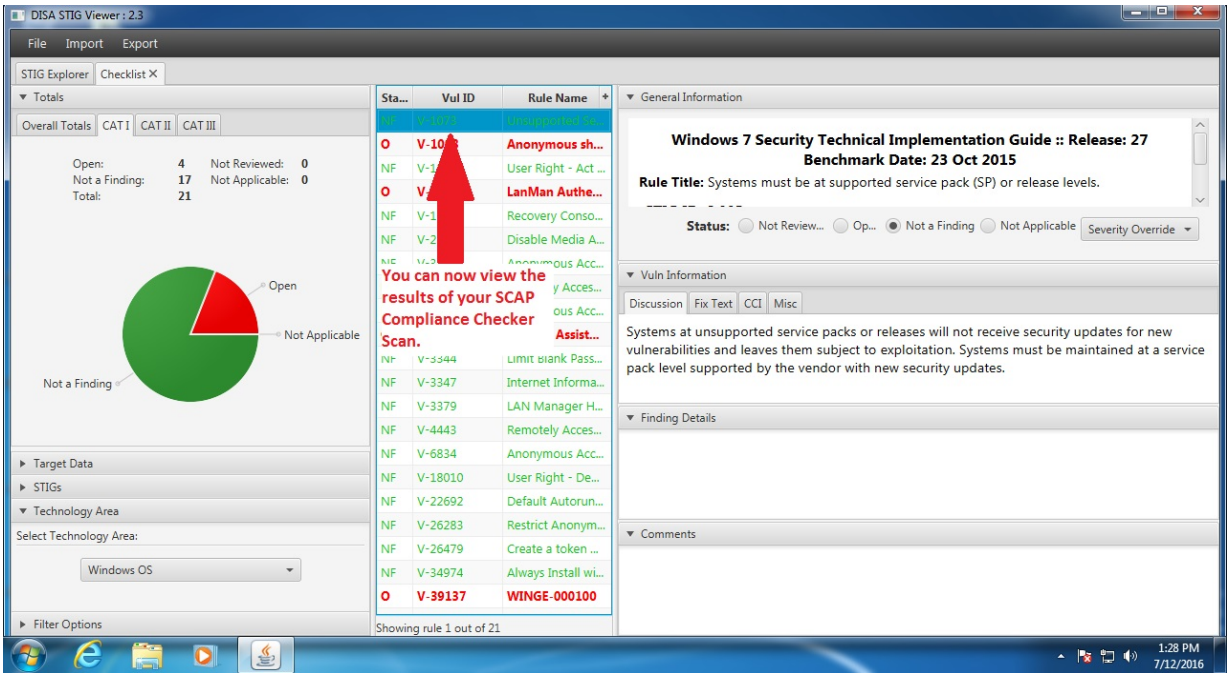

DISA STIG Viewer : 2.3
File
Export
Checklist
Options
Help
Import STIG
Exit
After opening the STIG Viewer application, import the appropriate STIG baseline for the system being assessed.
CK
Name
No content in table
Vul ID
Rule Name
No content in table
Profile:
No Profile
Filter Options
CAT I
CAT II
CAT III
Enter filter keyword
Add
Inclusive Filter
Exclusive Filter
Remove Filter
Remove All Filters
Showing rule 1 out of 324
1:15 PM
7/12/2016


DISA STIG Viewer : 2.3
Open
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Libraries
System Folder
CoferAdmin
System Folder
Computer
System Folder
Network
System Folder
SCAPSTIG
File folder
Screenshots
File folder
U_Windows_7_V1R27_STIG_SCAP_1-1_Benchmark
Compressed (zipped) Folder
Select and open the .zip file containing the appropriate STIG benchmark.
File name:
U_Windows_7_V1R27_STIG_SCAP_1-1_Benchmark
STIG Zip File(*.zip)
Open
Cancel
Remove Filter
Remove All Filters
Showing rule 1 out of 324
1:18 PM
7/12/2016


DISA STIG Viewer : 2.3
File
Export
Checklist
Options
Help
Open Checklist from File
Import v1.2 Checklist
Create Checklist - Selected STIG(s)
Create a checklist from the selected STIGS. Be sure that the checkbox for the STIG benchmark you wish to use is checked (as indicated by the blue arrow).
Windows 7 Security Technical Implementation Guide
Profile: No Profile
Filter Options
CAT I CAT II CAT III
Add
Inclusive Filter Exclusive Filter
Remove Filter
Remove All Filters
Rule Name
V-1097 Bad Logon Attempts
V-1098 Bad Logon Counter Reset
V-1099 Lockout Duration
V-1102 User Right - Act as part of OS
V-1104 Maximum Password Age
V-1105 Minimum Password Age
V-1107 Password Uniqueness
V-1113 Disable Guest Account
V-1114 Rename Built-in Guest Account
V-1115 Rename Built-in Administrator Acc...
V-1136 Forcibly Disconnect when Logon H...
V-1141 Unencrypted Password is Sent to S...
V-1145 Disable Automatic Logon
V-1150 Microsoft Strong Password Filtering
Showing rule 1 out of 278
General Information
Windows 7 Security Technical Implementation Guide :: Release: 27 Benchmark Date: 23 Oct 2015
Rule Title: Systems must be at supported service pack (SP)
Discussion
Systems at unsupported service packs or releases will not receive security updates for new vulnerabilities and leaves them subject to exploitation. Systems must be maintained at a service pack level supported by the vendor with new security
Fix Text
Update the system to a supported service pack.
Application of new service packs should be thoroughly tested before deploying in a production environment.
CCI
CCI: CCI-000366
The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
Miscellaneous
IA Controls:
VIVM-1
Third Party Tools:
1:21 PM
7/12/2016


DISA STIG Viewer : 2.3
File
Import
Export
XCCDF Results File
Import the XCCDF Results File from the SCAP Compliance Checker scan conducted earlier.
Totals
Overall Totals CAT I CAT II CAT III
Open: 0
Not a Finding: 0
Not Reviewed: 278
Not Applicable: 0
Not Reviewed
Target Data
STIGs
Technology Area
Select Technology Area:
Windows OS
Filter Options
Rule Name
NR V-1085 Removable me...
NR V-1089 Legal Notice Di...
NR V-1090 Caching of log...
NR V-1093 Anonymous sh...
NR V-1097 Bad Logon Att...
NR V-1098 Bad Logon Co...
NR V-1099 Lockout Durati...
NR V-1102 User Right - Ac...
NR V-1104 Maximum Pass...
NR V-1105 Minimum Pass...
NR V-1107 Password Uniq...
NR V-1113 Disable Guest ...
NR V-1114 Rename Built-i...
NR V-1115 Rename Built-i...
NR V-1136 Forcibly Discon...
NR V-1141 Unencrypted P...
NR V-1145 Disable Autom...
NR V-1150 Microsoft Stro...
Showing rule 1 out of 278
General Information
Windows 7 Security Technical Implementation Guide :: Release: 27 Benchmark Date: 23 Oct 2015
Rule Title: Systems must be at supported service pack (SP) or release levels.
Status: Not Review... Op... Not a Finding Not Applicable Severity Override
Vuln Information
Discussion Fix Text CCI Misc
Systems at unsupported service packs or releases will not receive security updates for new vulnerabilities and leaves them subject to exploitation. Systems must be maintained at a service pack level supported by the vendor with new security updates.
Finding Details
Comments
1:25 PM
7/12/2016


DISA STIG Viewer : 2.3
File
Import
Export
STIG Explorer
Checklist
Totals
Overall Totals
CAT I
CAT II
CAT III
Open: 4
Not a Finding: 17
Total: 21
Not Reviewed: 0
Not Applicable: 0
Open
Not Applicable
Not a Finding
Target Data
STIGs
Technology Area
Select Technology Area:
Windows OS
Filter Options
Sta...
Vul ID
Rule Name
O V-10
Anonymous sh...
NF V-1
User Right - Act ...
O V
LanMan Authe...
NF V-1
Recovery Conso...
NF V-2
Disable Media A...
You can now view the results of your SCAP Compliance Checker Scan.
NF V-3344
Limit Blank Pass...
NF V-3347
Internet Informa...
NF V-3379
LAN Manager H...
NF V-4443
Remotely Acces...
NF V-6834
Anonymous Acc...
NF V-18010
User Right - De...
NF V-22692
Default Autorun...
NF V-26283
Restrict Anonym...
NF V-26479
Create a token ...
NF V-34974
Always Install wi...
O V-39137
WINGE-000100
Showing rule 1 out of 21
General Information
Windows 7 Security Technical Implementation Guide :: Release: 27
Benchmark Date: 23 Oct 2015
Rule Title: Systems must be at supported service pack (SP) or release levels.
Status:
Not Review...
Op...
Not a Finding
Not Applicable
Severity Override
Vuln Information
Discussion
Fix Text
CCI
Misc
Systems at unsupported service packs or releases will not receive security updates for new vulnerabilities and leaves them subject to exploitation. Systems must be maintained at a service pack level supported by the vendor with new security updates.
Finding Details
Comments
1:28 PM
7/12/2016