Cisco Firewall ASA Nipper Vulnerability Extractor Script

Introduction

This script made in Python. This script is used for extracting IP addresses as per vulnerabilities name and help to find older version of OS and make three “csv” files. This script only work for “**Cisco Firewall ASA**”.

1. Make csv file from nipper HTML output by analyzing “Security Audit” in HTML file.
2. Make csv file from nipper HTML output by analyzing “CIS Benchmark” in HTML file.
3. Make csv file for older version.

Why we Need it?

After saving output in html form or any other form from Nipper. It’s taking large time for making report by copying IP addresses from that HTML output in report. Which is very frustrated. So this script help by saving time and using csv file it’s easy to copy IP addresses in the report.

What is mandatory?

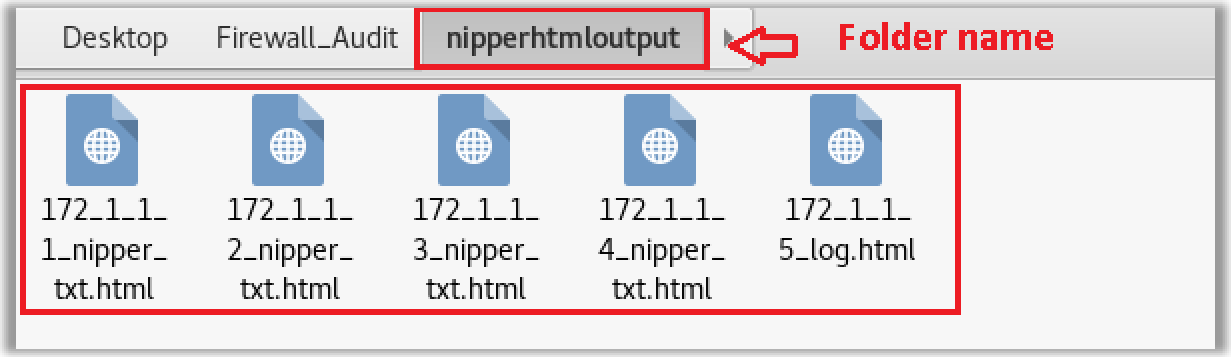
**It’s mandatory to save HTML file with name mentioned below.

IP_Address_anything.html

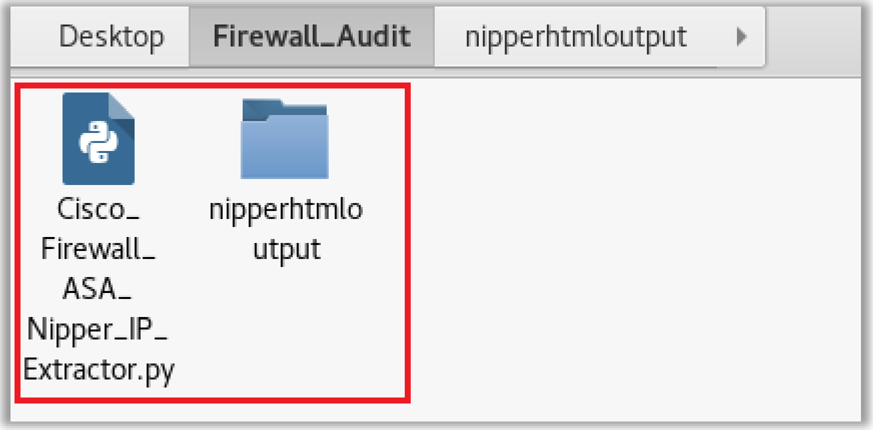
Example: 172_1_1_1_nipper_txt.html

How to use this script?

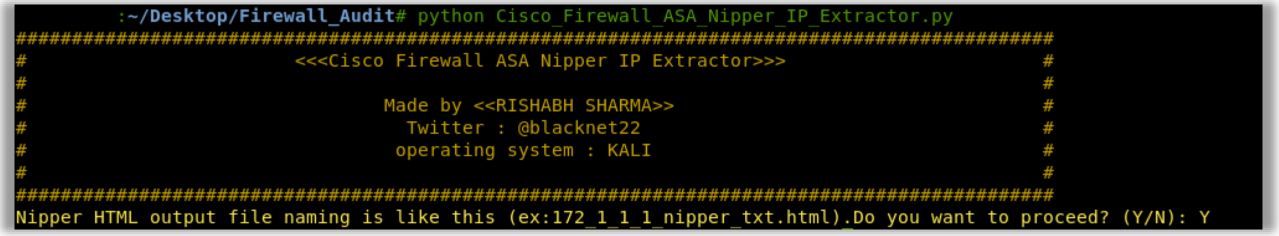
Step1. Make one folder with any name and save all HTML output in that folder.


Desktop
Firewall_Audit
nipperhtmloutput
Folder name
172_1_1_1_nipper_txt.html
172_1_1_2_nipper_txt.html
172_1_1_3_nipper_txt.html
172_1_1_4_nipper_txt.html
172_1_1_5_log.html

Step2. Save “Cisco_Firewall_ASA_Nipper_IP_Extractor.py” where above folder exist.

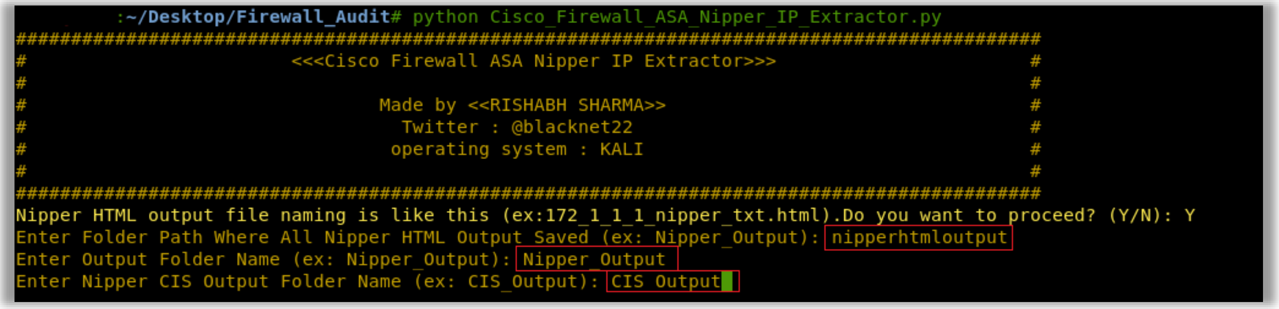


Step3. Run script “python Cisco_Firewall_ASA_Nipper_IP_Extractor.py”. Then it’s ask for that HTML output file naming is like that which is mentioned above. Type “Y” and click enter.



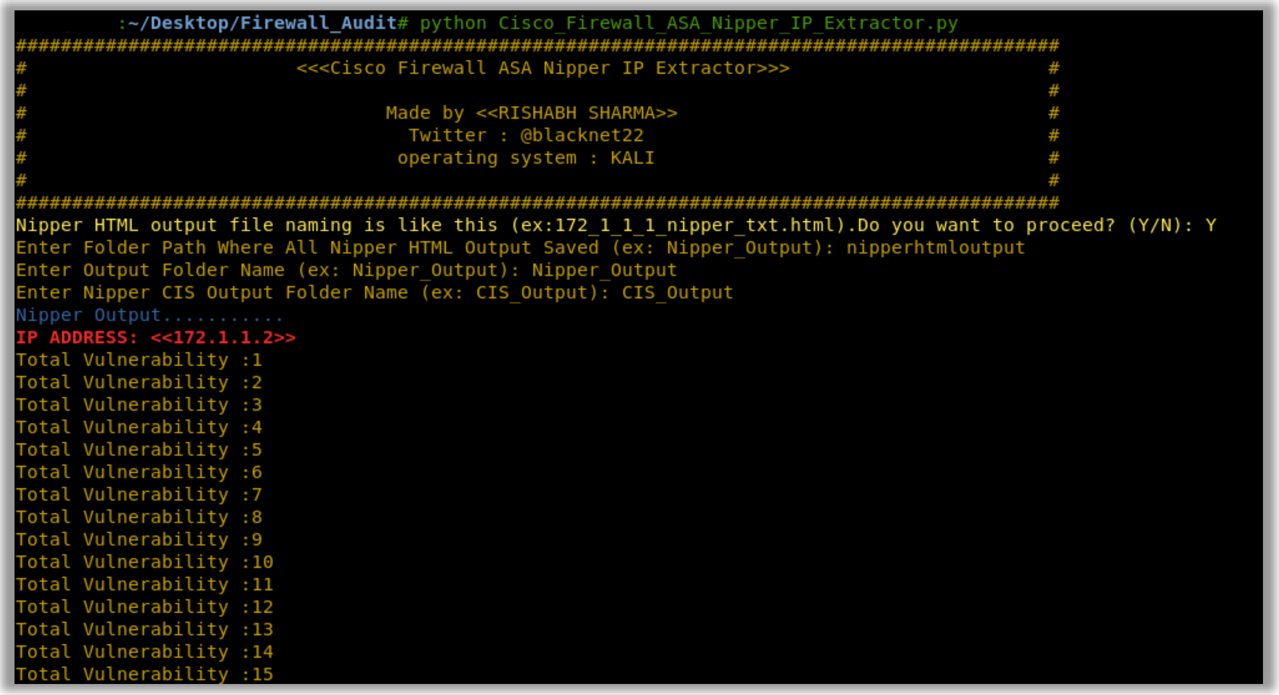
```
         :~/Desktop/Firewall_Audit# python Cisco_Firewall_ASA_Nipper_IP_Extractor.py
#############################################################################################
#                        <<<Cisco Firewall ASA Nipper IP Extractor>>>                       #
#                                                                                           #
#                                Made by <<RISHABH SHARMA>>                                 #
#                                  Twitter : @blacknet22                                    #
#                                 operating system : KALI                                   #
#                                                                                           #
#############################################################################################
Nipper HTML output file naming is like this (ex:172_1_1_1_nipper_txt.html).Do you want to proceed? (Y/N): Y
```

Step4. After click on enter it’s ask for the folder name where all Nipper HTML output saved. Like in our case it’s “nipperhtmloutput”. Then it’s ask for Output folder name where it save all IP addresses with vulnerability name. In this case we give name “Nipper_Output”. Then it’s ask for output folder name for saving CIS benchmark vulnerabilities. In this case we give name “CIS_Output” and click enter.

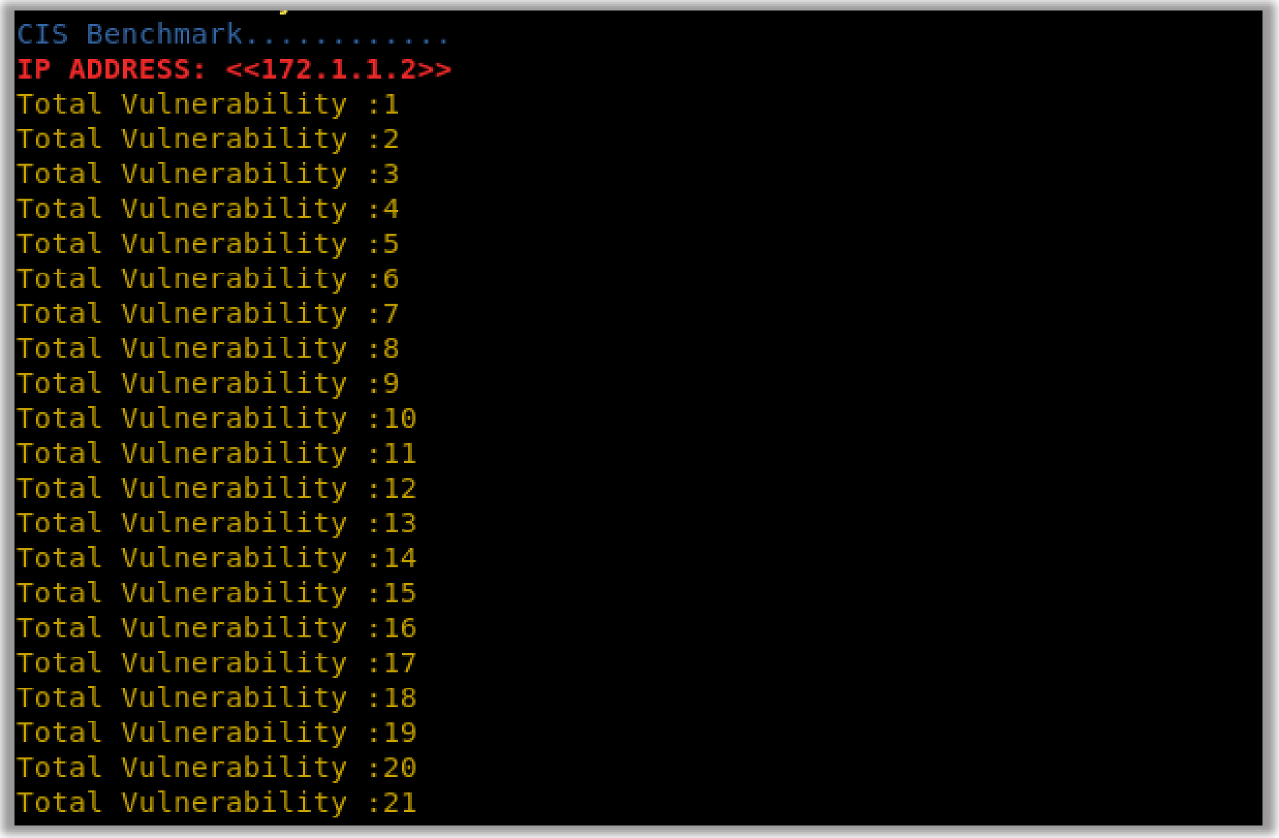


```
         :~/Desktop/Firewall_Audit# python Cisco_Firewall_ASA_Nipper_IP_Extractor.py
#############################################################################################
#                        <<<Cisco Firewall ASA Nipper IP Extractor>>>                       #
#                                                                                           #
#                                Made by <<RISHABH SHARMA>>                                 #
#                                  Twitter : @blacknet22                                    #
#                                 operating system : KALI                                   #
#                                                                                           #
#############################################################################################
Nipper HTML output file naming is like this (ex:172_1_1_1_nipper_txt.html).Do you want to proceed? (Y/N): Y
Enter Folder Path Where All Nipper HTML Output Saved (ex: Nipper_Output): nipperhtmloutput
Enter Output Folder Name (ex: Nipper_Output): Nipper_Output
Enter Nipper CIS Output Folder Name (ex: CIS_Output): CIS_Output
```

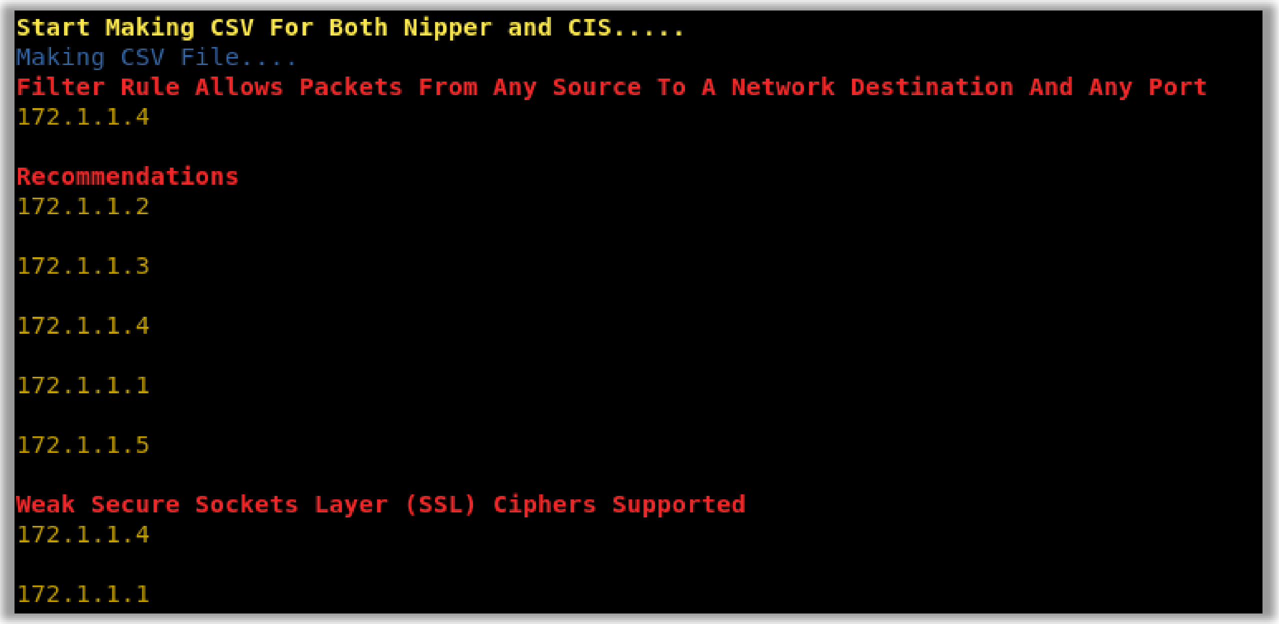
Step5. After clicking enter POC is showing below.



```
:~/Desktop/Firewall_Audit# python Cisco_Firewall_ASA_Nipper_IP_Extractor.py
#############################################################################################
#                        <<<Cisco Firewall ASA Nipper IP Extractor>>>                       #
#                                                                                           #
#                                Made by <<RISHABH SHARMA>>                                 #
#                                  Twitter : @blacknet22                                    #
#                                 operating system : KALI                                   #
#                                                                                           #
#############################################################################################
Nipper HTML output file naming is like this (ex:172_1_1_1_nipper_txt.html).Do you want to proceed? (Y/N): Y
Enter Folder Path Where All Nipper HTML Output Saved (ex: Nipper_Output): nipperhtmloutput
Enter Output Folder Name (ex: Nipper_Output): Nipper_Output
Enter Nipper CIS Output Folder Name (ex: CIS_Output): CIS_Output
Nipper Output...........
IP ADDRESS: <<172.1.1.2>>
Total Vulnerability :1
Total Vulnerability :2
Total Vulnerability :3
Total Vulnerability :4
Total Vulnerability :5
Total Vulnerability :6
Total Vulnerability :7
Total Vulnerability :8
Total Vulnerability :9
Total Vulnerability :10
Total Vulnerability :11
Total Vulnerability :12
Total Vulnerability :13
Total Vulnerability :14
Total Vulnerability :15
```

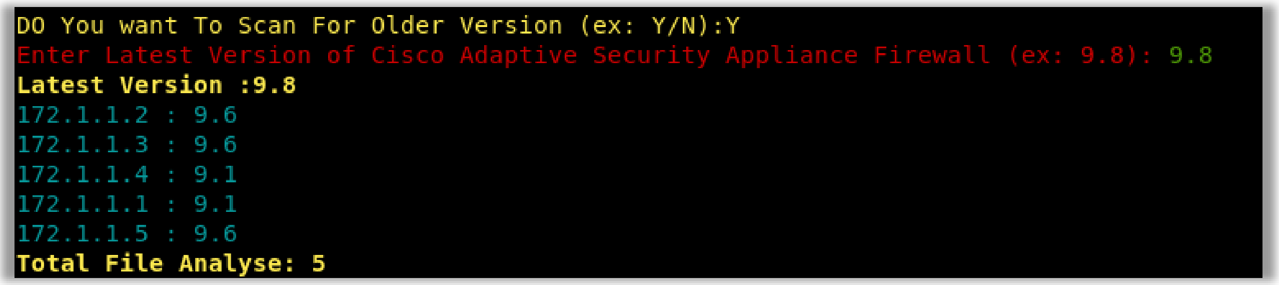


```
CIS Benchmark............
IP ADDRESS: <<172.1.1.2>>
Total Vulnerability :1
Total Vulnerability :2
Total Vulnerability :3
Total Vulnerability :4
Total Vulnerability :5
Total Vulnerability :6
Total Vulnerability :7
Total Vulnerability :8
Total Vulnerability :9
Total Vulnerability :10
Total Vulnerability :11
Total Vulnerability :12
Total Vulnerability :13
Total Vulnerability :14
Total Vulnerability :15
Total Vulnerability :16
Total Vulnerability :17
Total Vulnerability :18
Total Vulnerability :19
Total Vulnerability :20
Total Vulnerability :21
```



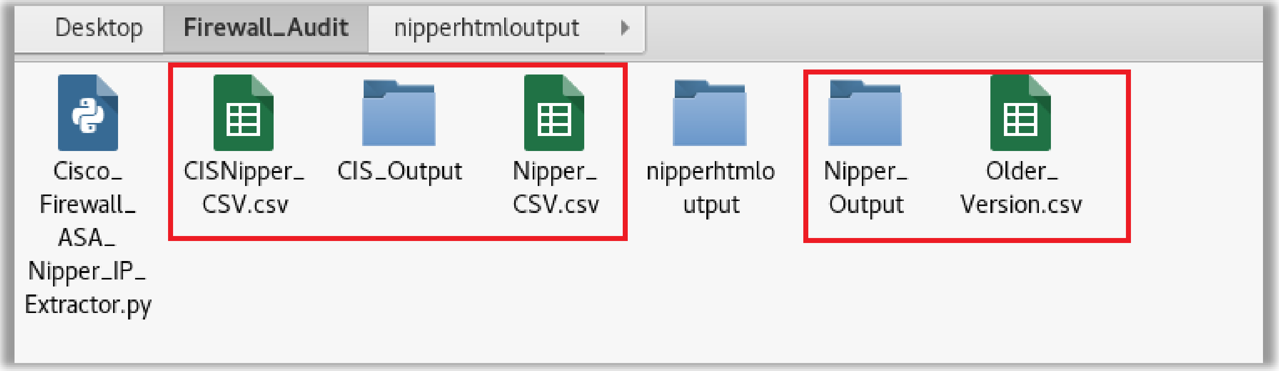
```
Start Making CSV For Both Nipper and CIS.....
Making CSV File....
Filter Rule Allows Packets From Any Source To A Network Destination And Any Port
172.1.1.4

Recommendations
172.1.1.2

172.1.1.3

172.1.1.4

172.1.1.1

172.1.1.5

Weak Secure Sockets Layer (SSL) Ciphers Supported
172.1.1.4

172.1.1.1
```

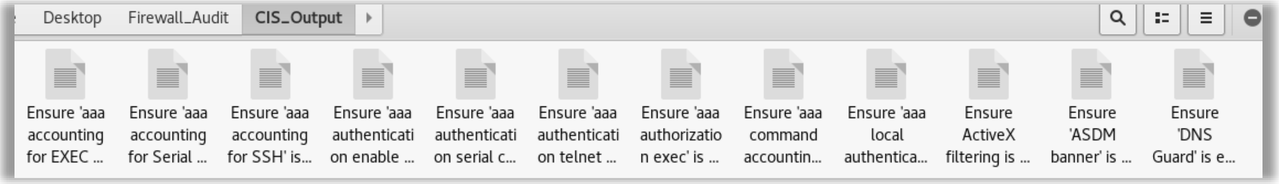
Step6. At last it's ask "Do you want to scan for older version?", When you click on "Y" it's ask for latest version number, so that it compare it with the version found in Nipper HTML output.



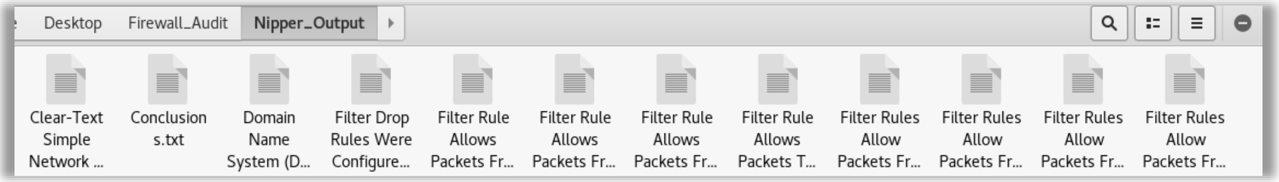
```
DO You want To Scan For Older Version (ex: Y/N):Y
Enter Latest Version of Cisco Adaptive Security Appliance Firewall (ex: 9.8): 9.8
Latest Version :9.8
172.1.1.2 : 9.6
172.1.1.3 : 9.6
172.1.1.4 : 9.1
172.1.1.1 : 9.1
172.1.1.5 : 9.6
Total File Analyse: 5
```

Step7. Now all work done. CSV file saved, Output saved in same directory.

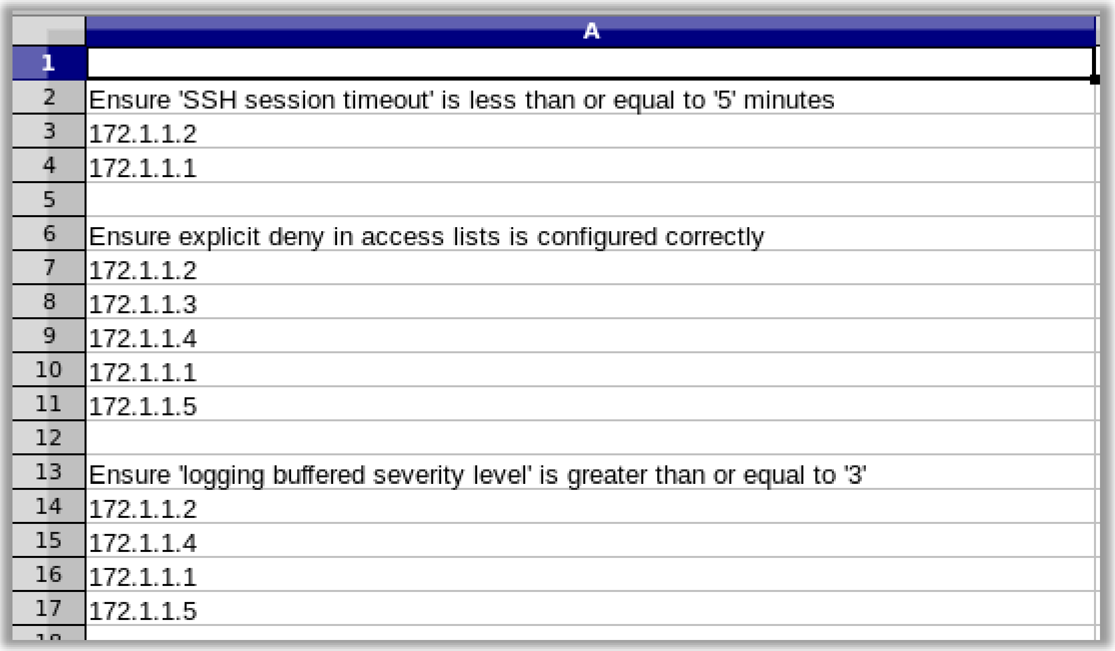




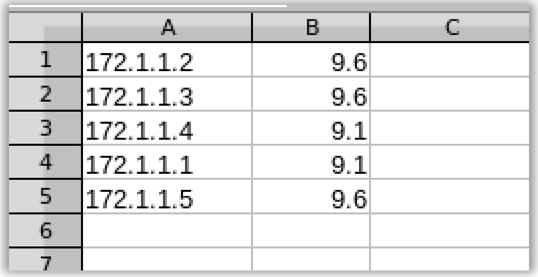
Ensure 'aaa accounting for EXEC ...
Ensure 'aaa accounting for Serial ...
Ensure 'aaa accounting for SSH' is...
Ensure 'aaa authentication enable ...
Ensure 'aaa authentication serial c...
Ensure 'aaa authentication telnet ...
Ensure 'aaa authorization exec' is ...
Ensure 'aaa command accountin...
Ensure 'aaa local authentica...
Ensure ActiveX filtering is ...
Ensure 'ASDM banner' is ...
Ensure 'DNS Guard' is e...



Clear-Text Simple Network ...
Conclusions.txt
Domain Name System (D...
Filter Drop Rules Were Configure...
Filter Rule Allows Packets Fr...
Filter Rule Allows Packets Fr...
Filter Rule Allows Packets Fr...
Filter Rule Allows Packets T...
Filter Rules Allow Packets Fr...
Filter Rules Allow Packets Fr...
Filter Rules Allow Packets Fr...
Filter Rules Allow Packets Fr...



	A
1	
2	Ensure 'SSH session timeout' is less than or equal to '5' minutes
3	172.1.1.2
4	172.1.1.1
5	
6	Ensure explicit deny in access lists is configured correctly
7	172.1.1.2
8	172.1.1.3
9	172.1.1.4
10	172.1.1.1
11	172.1.1.5
12	
13	Ensure 'logging buffered severity level' is greater than or equal to '3'
14	172.1.1.2
15	172.1.1.4
16	172.1.1.1
17	172.1.1.5



	A	B	C
1	172.1.1.2	9.6	
2	172.1.1.3	9.6	
3	172.1.1.4	9.1	
4	172.1.1.1	9.1	
5	172.1.1.5	9.6	
6			
7			