Unit 2 Lab – Network Standards and Compliance

Required Materials

Putty or other connection tool

Lab Server

Root or sudo command access

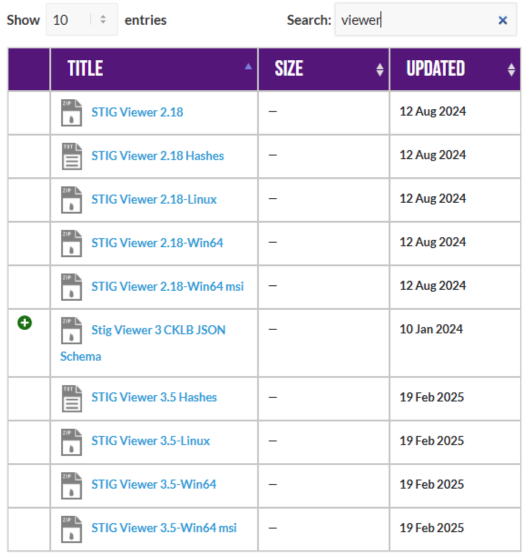
STIG Viewer 2.18 (download from https://public.cyber.mil/stigs/downloads/)

EXERCISES (Warmup to quickly run through your system and familiarize yourself)

1. sysctl -a | grep -i ipv4 | grep -i forward
    a. Does this system appear to be set to forward? Why or why not?
2. sysctl -a | grep -i ipv4 | grep -i martian
    a. What are martians and is this system allowing them?
3. sysctl -a | grep -i panic
    a. How does this system handle panics?
4. sysctl -a | grep -i crypto
    a. What are the settings you see? Is FIPS enabled?
5. cat /proc/cmdline
6. fips-mode-setup --check
7. sestatus
8. cat /etc/selinux/config
    a. What information about the security posture of the system can you see here?
        i. Can you verify SELINUX status?
        ii. Can you verify FIPS status?

PreLAB

Download the STIG Viewer 2.18 from - https://public.cyber.mil/stigs/downloads/

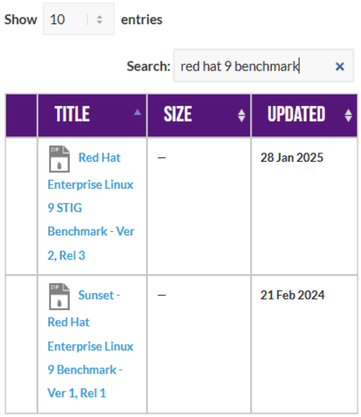


Show 10 entries

Search: viewer

	TITLE	SIZE	UPDATED
	STIG Viewer 2.18	–	12 Aug 2024
	STIG Viewer 2.18 Hashes	–	12 Aug 2024
	STIG Viewer 2.18-Linux	–	12 Aug 2024
	STIG Viewer 2.18-Win64	–	12 Aug 2024
	STIG Viewer 2.18-Win64 msi	–	12 Aug 2024
⊕	Stig Viewer 3 CKLB JSON Schema	–	10 Jan 2024
	STIG Viewer 3.5 Hashes	–	19 Feb 2025
	STIG Viewer 3.5-Linux	–	19 Feb 2025
	STIG Viewer 3.5-Win64	–	19 Feb 2025
	STIG Viewer 3.5-Win64 msi	–	19 Feb 2025

Download the STIG for RHEL 9 and the import it into your STIG viewer

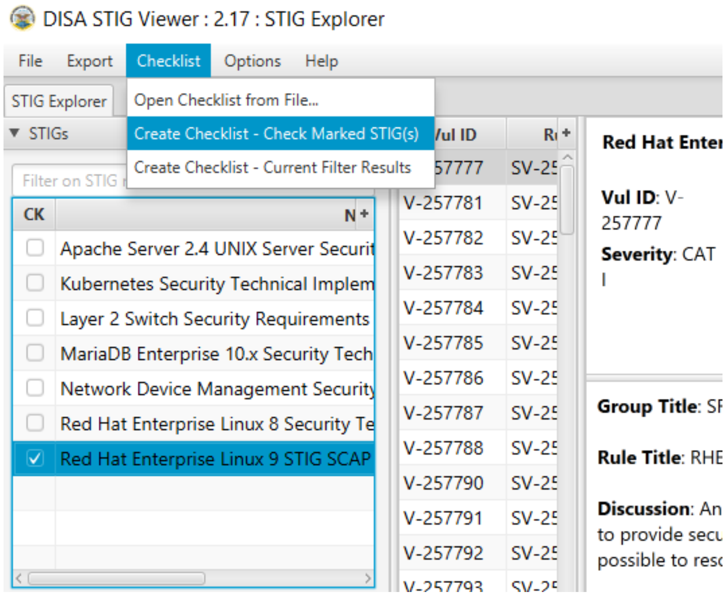


Show 10 entries

Search: red hat 9 benchmark

	TITLE	SIZE	UPDATED
	Red Hat Enterprise Linux 9 STIG Benchmark - Ver 2, Rel 3	–	28 Jan 2025
	Sunset - Red Hat Enterprise Linux 9 Benchmark - Ver 1, Rel 1	–	21 Feb 2024

Create a checklist from the opened STIG for RHEL 9



DISA STIG Viewer : 2.17 : STIG Explorer

File
Export
Checklist
Options
Help
STIG Explorer
Open Checklist from File...
Create Checklist - Check Marked STIG(s)
Create Checklist - Current Filter Results
STIGs
Filter on STIG n

CK	N
☐	Apache Server 2.4 UNIX Server Securit
☐	Kubernetes Security Technical Implem
☐	Layer 2 Switch Security Requirements
☐	MariaDB Enterprise 10.x Security Tech
☐	Network Device Management Security
☐	Red Hat Enterprise Linux 8 Security Te
☑	Red Hat Enterprise Linux 9 STIG SCAP

Vul ID	R
57777	SV-25
V-257781	SV-25
V-257782	SV-25
V-257783	SV-25
V-257784	SV-25
V-257785	SV-25
V-257786	SV-25
V-257787	SV-25
V-257788	SV-25
V-257790	SV-25
V-257791	SV-25
V-257792	SV-25
V-257793	SV-25

Red Hat Ente

Vul ID: V-257777

Severity: CAT I

Group Title: SF

Rule Title: RHE

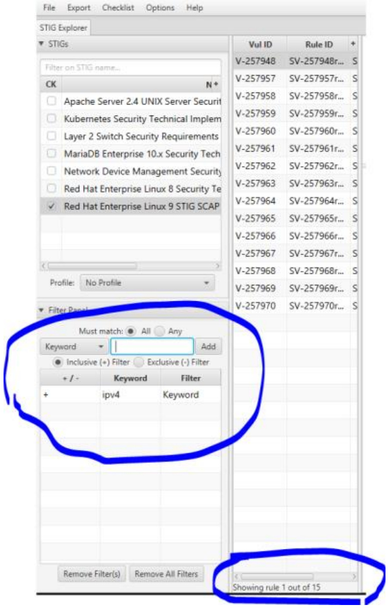
Discussion: An to provide secu possible to res

LAB

This lab is designed to have the engineer practice securing a Linux server or service against a set of configuration standards. These standards are sometimes called benchmarks, checklists, or guidelines. The engineer will be using STIG Viewer 2.18 to complete this lab.

Network Service configuration:

1. Connect to a hammer server
2. Filter by ipv4 and see how many STIGS you have.



CK	N
☐	Apache Server 2.4 UNIX Server Securit
☐	Kubernetes Security Technical Implem
☐	Layer 2 Switch Security Requirements
☐	MariaDB Enterprise 10.x Security Tech
☐	Network Device Management Security
☐	Red Hat Enterprise Linux 8 Security Te
✓	Red Hat Enterprise Linux 9 STIG SCAP

+ / -	Keyword	Filter
+	ipv4	Keyword

Vul ID	Rule ID	
V-257948	SV-257948r...	S
V-257957	SV-257957r...	S
V-257958	SV-257958r...	S
V-257959	SV-257959r...	S
V-257960	SV-257960r...	S
V-257961	SV-257961r...	S
V-257962	SV-257962r...	S
V-257963	SV-257963r...	S
V-257964	SV-257964r...	S
V-257965	SV-257965r...	S
V-257966	SV-257966r...	S
V-257967	SV-257967r...	S
V-257968	SV-257968r...	S
V-257969	SV-257969r...	S
V-257970	SV-257970r...	S

Showing rule 1 out of 15

3. Examine STIG V-257957

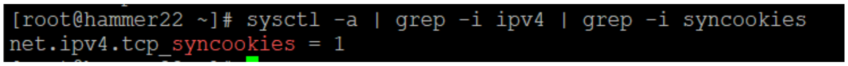
a. What is the problem?

b. What is the fix?

c. What type of control is being implemented?

d. Is it set properly on your system?

i. sysctl -a | grep -i ipv4 | grep -i syncookies



```
[root@hammer22 ~]# sysctl -a | grep -i ipv4 | grep -i syncookies
net.ipv4.tcp_syncookies = 1
```

ii. Can you remediate this finding?

In this case it’s already correctly set.

But if we needed to, we would set that value in /etc/sysctl.d/00-remediate.conf

And then reload sysctl with `sysctl --system`

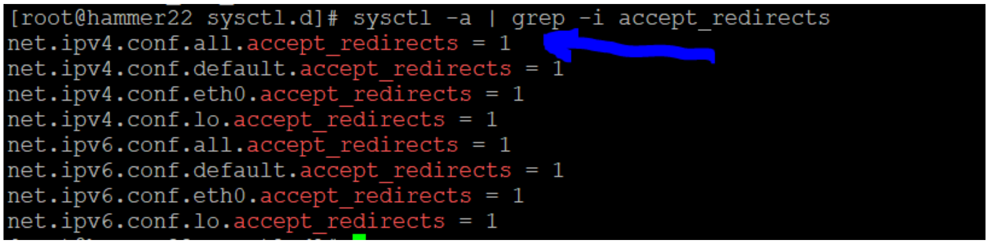
4. Check and remediate V-257958 STIG

a. What is the problem?

b. What is the fix?

c. What type of control is being implemented?

d. Is it set properly on your system?



```
[root@hammer22 sysctl.d]# sysctl -a | grep -i accept_redirects
net.ipv4.conf.all.accept_redirects = 1
net.ipv4.conf.default.accept_redirects = 1
net.ipv4.conf.eth0.accept_redirects = 1
net.ipv4.conf.lo.accept_redirects = 1
net.ipv6.conf.all.accept_redirects = 1
net.ipv6.conf.default.accept_redirects = 1
net.ipv6.conf.eth0.accept_redirects = 1
net.ipv6.conf.lo.accept_redirects = 1
```

e. How would you go about remediating this on your system?

5. Check and remediate V-257960 and V-257961 STIGs

a. What is the problem? How are they related?

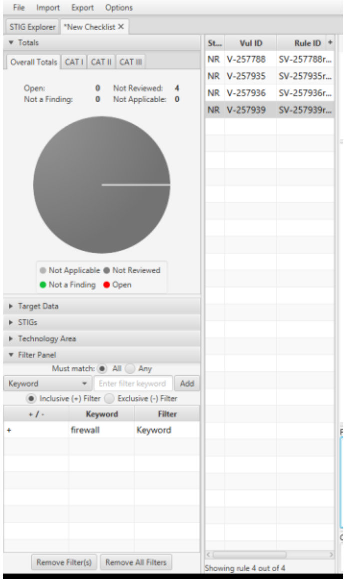
b. What is the fix?

c. What type of control is being implemented?

d. Is it set properly on your system?

6. Filter by firewall

a. How many STIGS do you see?



Open: 0
Not a Finding: 0
Not Reviewed: 4
Not Applicable: 0

Must match: ● All ○ Any

Keyword | Enter filter keyword | Add

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter
+	firewall	Keyword

St...	Vul ID	Rule ID
NR	V-257788	SV-257788r...
NR	V-257935	SV-257935r...
NR	V-257936	SV-257936r...
NR	V-257939	SV-257939r...

Showing rule 4 out of 4

b. What do these STIGS appear to be trying to do? What types of controls are they?

Firewall port exposure

Your team needs to use node_exporter with Prometheus to allow scraping of system information back to your network monitoring solution. You are running a firewall, so you need to expose the port that node_exporter runs on to the network outside of your system.

7. Expose a network port through your firewall
   a. Verify that your firewall is running
      systemctl status firewalld
   b. Verify that your firewall has the service defined
      firewall-cmd --get-services | grep -i node
      ls /usr/lib/firewalld/services | grep -i node
   c. Verify that the service is not currently enabled for node_exporter
      firewall-cmd –list-services
   d. Examine the structure of the firewall .xml file
      cat /usr/lib/firewalld/services/prometheus-node-exporter.xml
   e. Enable the service through your firewall
      firewall-cmd --permanent --add-service=prometheus-node-exporter
      firewall-cmd --reload
   f. Verify that the service is currently enabled for node_exporter
      firewall-cmd --list-services

Automate STIG remediation on a system

There are many options and the STIG remediation steps are well known. Here the learner will examine a few ways to generate Ansible and Shell fixes to your system. Then one can apply all of them, or just some of them. This is the real value of a security engineer focused Linux engineer, the tradeoff between security and productivity.

8. Download and extract a STIG remediation tool

```
cd /root

mkdir stigs

cd stigs

wget -O U_RHEL_9_V2R3_STIG_Ansible.zip https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_RHEL_9_V2R3_STIG_Ansible.zip

unzip U_RHEL_9_V2R3_STIG_Ansible.zip

mkdir ansible

cp rhel9STIG-ansible.zip ansible/

cd ansible

unzip rhel9STIG-ansible.zip
```

9. Examine the default values for stigs

```
cd /root/stigs/ansible/roles/rhel9STIG/defaults/

vim main.yml
```

Search for a few of the STIG numbers you used earlier and see their default values.

#use /257784 to search

10. Examine the playbook to see how those are applied in a running system.

```
vim /root/stigs/ansible/roles/rhel9STIG/tasks/main.yml
```

#use /257784 to search for the STIG from above and see how it is fixed in the playbook.

11. Create an Ansible playbook from openscap.

```
dnf -y  install openscap-scanner openscap-utils openscap-scanner scap-security-guide

cd /root
```

```
mkdir openscap
```

```
cd openscap
```

#Generate the Ansible

```
oscap xccdf generate fix --profile ospp --fix-type ansible /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml > draft-disa-remediate.yml
```

#Examine the file

```
vim draft-disa-remediate.yml
```

#Generate a BASH version

```
oscap xccdf generate fix --profile ospp --fix-type bash /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml > draft-disa-remediate.sh
```

#Examine the file

```
vim draf-disa-remediate.sh
```