Security Platform Presentation

Or everyday security features around us

Lukas Vrabec
Open House Brno
2019-04-17

Agenda

- Who is Platform Security?
- What technologies are provide?
- Why should you care?
- Real examples of our work

Platform Security

Platform Security is an engineering that
deliver security technologies and best practices for the benefit of open source communities and Red Hat in an open source way.

Platform Security

- **Security Compliance**
  - *We help customers make sure their systems are configured in a safe manner, and according to the requirements mandated by governments and industries.*
- **Security Controls**
  - *We provide SELinux technology to help mitigate security risks at the lowest level of the software stack by making sure processes can access only resources they really need.*
- **Crypto**
  - *We enable the development and deployment of cryptography-using software in an easy and safe way, and enable users to safely use standardized cryptography."*

Platform Security

- **Audit**
  - *"Provide auditing tools to help administrators monitor systems and perform forensic analysis."*
- **Special Projects**
  - *"Development of new tools based on emerging approaches to security. Responsible for maintaining several security technologies"*

Technologies

What we're doing

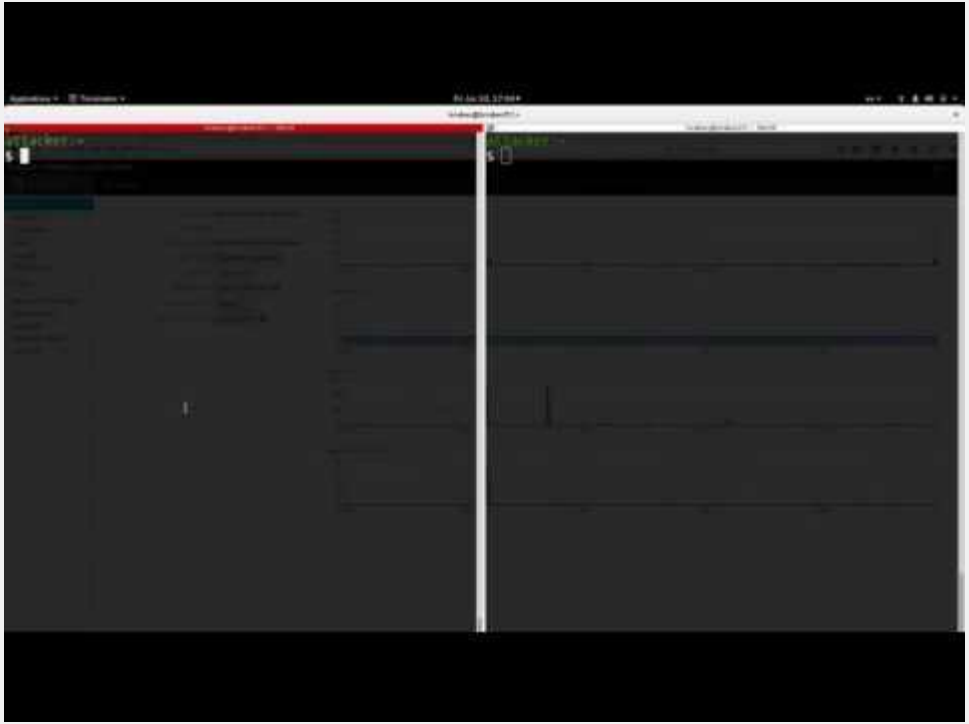
- **Crypto**
  - Implementation and testing of low-level crypto primitives and security protocols such as TLS or SSH
- **Smart Cards**
  - Personal identification, national eID cards and tokens drivers for secure private-key authentication in your applications accessible through PKCS#11 interface
- **OpenSCAP**
  - *Security compliance is a state where computer systems are in line with a specific security policy.*
- **SELinux**
  - *Technology for process isolation to mitigate attacks via privilege escalation*

What we're doing

- **Sudo**
  - *The sudo allows to execute a command as another user (e.g: root)*
- **USBGuard**
  - *The USBGuard software framework helps to protect your computer against rogue USB devices (a.k.a. BadUSB) by implementing basic whitelisting and blacklisting*
- **Rsyslog**
  - The Rsyslog software stack allows log collection from various inputs (local services/events, endpoint for remote sources), log processing and storage/distribution to many different locations (files, remote syslog, databases...)
- **IPsec**
  - IPsec encrypts network traffic at the IP level. This can be between two hosts (host-to-host), between networks or datacenters (site-to-site), a Remote Access VPN, or between all nodes in a mesh network.

Real examples

Shellshock exploit



Confined Root user

```
$ su -
# whoami
root

# cat /root/.bashrc
cat: /root/.bashrc: Permission denied

# rm /etc/passwd
rm: cannot remove '/etc/passwd': Permission denied

# id -Z
staff_u:staff_r:staff_t:s0-s0:c0.c1023
```

Sniffing non-crypted communication

```
$ mail -r 'tony@localhost' -s 'Secret number' jane@localhost
<<EOF

# cat /var/spool/mail/jane

$ cat <<EOF | gpg2 -eas -r 'tony@localhost' | \
    mail -r 'jane@localhost' -s 'Re: Secret number'
tony@localhost

$ mail | gpg2 -d
```

USBGuard

```
$ sudo dnf install usbguard usbguard-applet-qt

$ sudo usbguard generate-policy > rules.conf

$ vi rules.conf
(review/modify the rule set)

$ sudo install -m 0600 -o root -g root rules.conf
/etc/usbguard/rules.conf

$ sudo systemctl restart usbguard
```

Audit

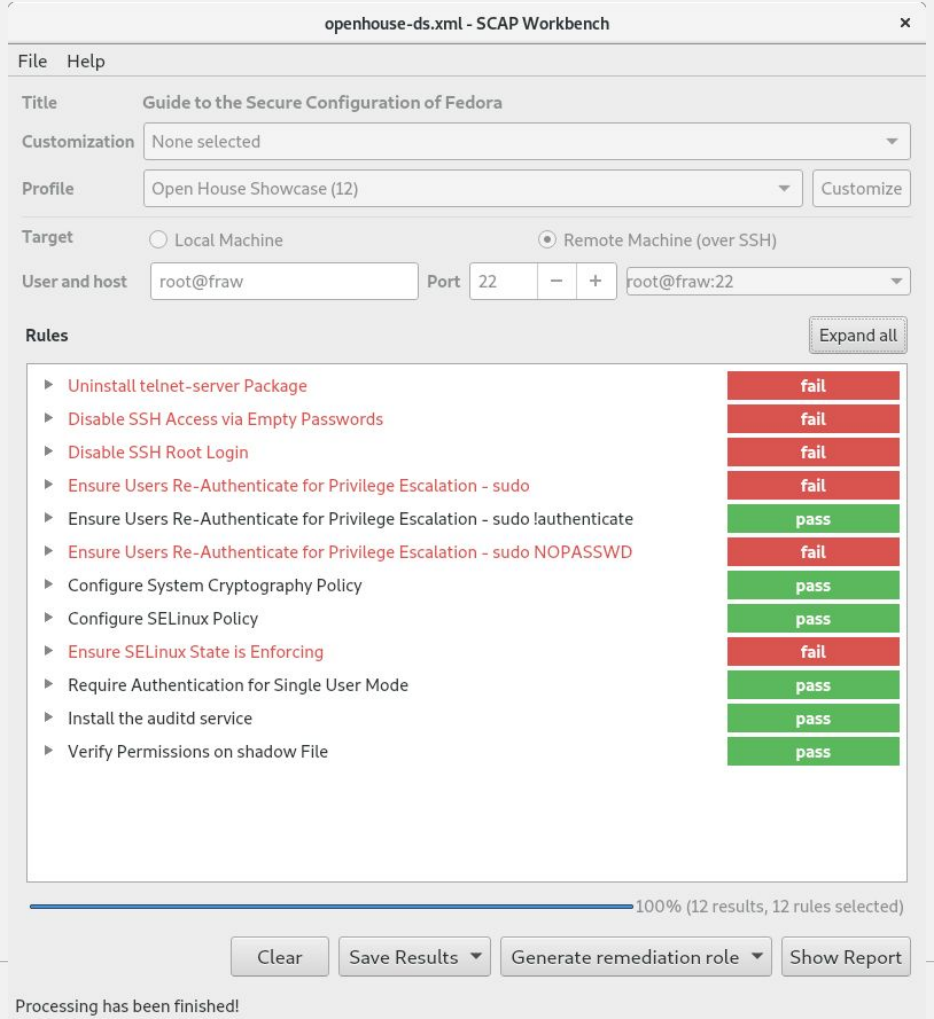
```
# cat /etc/suspicious
# rm  /etc/suspicious

# auditctl -a exit,always -F path=/etc/suspicious -p w -k
suspicious

# rm  /etc/suspicious
# cat /etc/suspicious

# ausearch -i -k suspicious -ts 17:16:44
```

Compliance


openhouse-ds.xml - SCAP Workbench
File
Help
Title
Guide to the Secure Configuration of Fedora
Customization
None selected
Profile
Open House Showcase (12)
Customize
Target
Local Machine
Remote Machine (over SSH)
User and host
root@fraw
Port
22
root@fraw:22
Rules
Expand all
Uninstall telnet-server Package
fail
Disable SSH Access via Empty Passwords
fail
Disable SSH Root Login
fail
Ensure Users Re-Authenticate for Privilege Escalation - sudo
fail
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
pass
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
fail
Configure System Cryptography Policy
pass
Configure SELinux Policy
pass
Ensure SELinux State is Enforcing
fail
Require Authentication for Single User Mode
pass
Install the auditd service
pass
Verify Permissions on shadow File
pass
100% (12 results, 12 rules selected)
Clear
Save Results
Generate remediation role
Show Report
Processing has been finished!

Why I’m telling this?

We’re hiring!

Interested?

- **Crypto Internship**
- **Security Controls Internship**

More information on Lightning talks

April 17th at 17:00 - 18:20 in TPB-C 3rd floor kitchen

Links

https://lukas-vrabec.com

https://gitlab.com/bachradsusi/openhouse2019-demos

https://research.redhat.com/internships_cpt/security-controls-internship/

https://research.redhat.com/internships_cpt/software-engineering-intern-crypto/

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHat

youtube.com/user/RedHatVideos