# Defend Yourself with RHEL Security Lab Overview

Red Hat

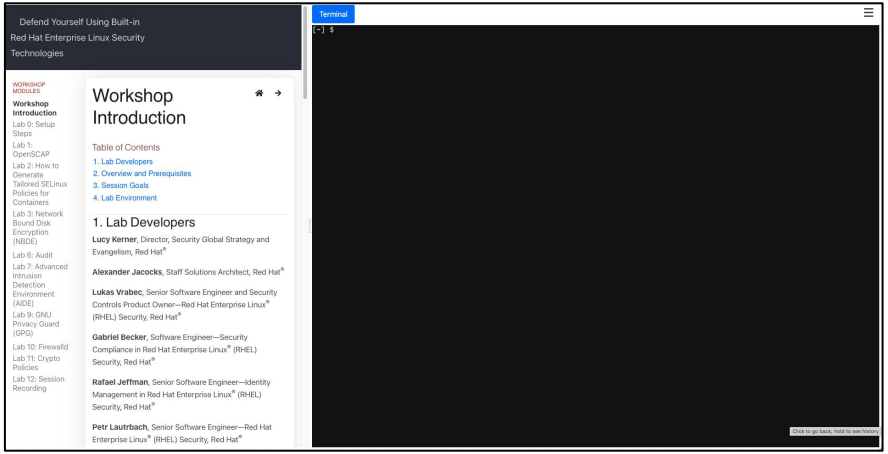


# Accessing the labs

1. Navigate to **red.ht/summitlabs**
2. Log in with the:
   a. Email you registered with
   b. Password: **dec6**
3. Within the catalog, click the **“Live Today”** label and select your lab
4. Click “**Request Service**” and wait a few moments for the lab to become available
5. Click the link in the “Lab Instructions” section
   a. Note the additional information on the details page, you may need this in your lab
6. You are now ready to start working on your lab.

# Lab Instructions

- Click the link in the “Lab Instructions” section
  a. Note the additional information on the details page, you may need this in your lab
- A pop up window will appear with a terminal and your lab instructions



# Breakout rooms for 1:1 help

- Ask your question in the Q&A, and, should it not be able to be answered the Q&A tool, we will send you a private message with information on how to join the breakout room.
- In these breakout rooms, you can speak privately, share screens, and resolve your issues!

Red Hat

# Lab 1 - OpenSCAP




- Access the graphical user interface of your dedicated OpenSCAP environment.
- Use automated OpenSCAP security and compliance scanning.
- Use SCAP workbench to customize security profiles.
- Automate security remediations with OpenSCAP and Ansible.



# Lab 2 - SELinux


- Install `utica` and `podman`.
- Evaluate the current situation.
- Generate Tailored SELinux Policies for Containers



# Lab 3 - Network Bound Disk Encryption (NBDE)

- (Also uses an SSH tunnel)
- Install `Tang` server and `Clevis` Client.
- Verify LUKS.
- Enable decryption on the boot process.
- Reboot and test NBDE.
- Use Cockpit to initialize LUKs binding to the `tang` server.



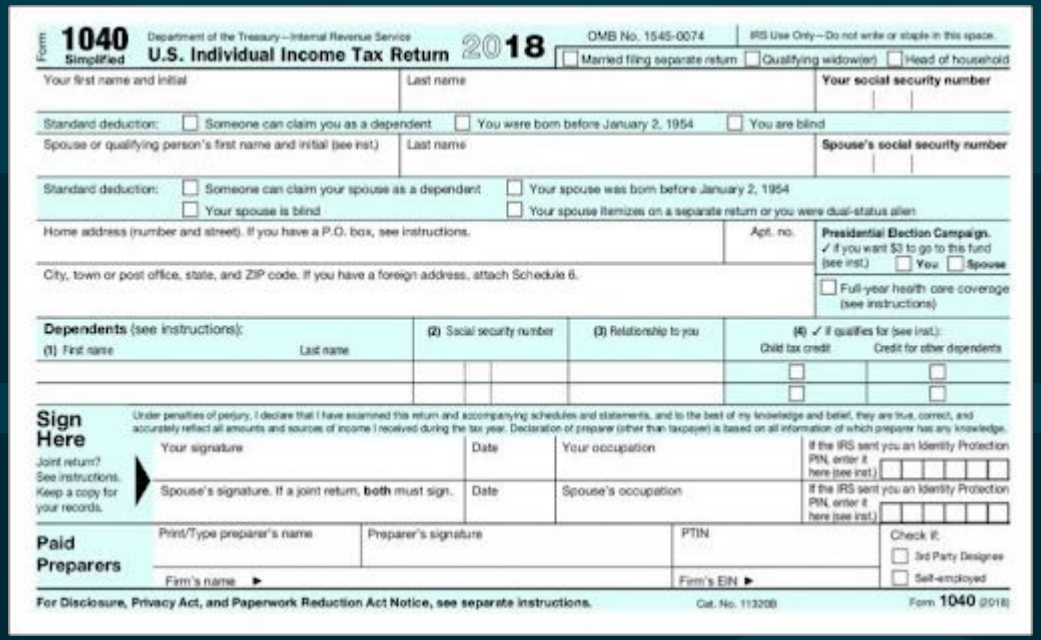
# Lab 4 - IPSEC (not for 12/6/2021)



# Lab 5 - USB Guard (not for 12/6/2021)




# Lab 6 - Audit



Form **1040** Simplified — Department of the Treasury—Internal Revenue Service — **U.S. Individual Income Tax Return** — 2018 — OMB No. 1545-0074 — IRS Use Only—Do not write or staple in this space.

Married filing separate return ☐ Qualifying widow(er) ☐ Head of household

Your first name and initial | Last name | **Your social security number**

Standard deduction: ☐ Someone can claim you as a dependent ☐ You were born before January 2, 1954 ☐ You are blind

Spouse or qualifying person's first name and initial (see inst.) | Last name | **Spouse's social security number**

Standard deduction: ☐ Someone can claim your spouse as a dependent ☐ Your spouse was born before January 2, 1954
☐ Your spouse is blind ☐ Your spouse itemizes on a separate return or you were dual-status alien

Home address (number and street). If you have a P.O. box, see instructions. | Apt. no. | **Presidential Election Campaign.** ✓ if you want $3 to go to this fund (see inst.) ☐ You ☐ Spouse

City, town or post office, state, and ZIP code. If you have a foreign address, attach Schedule 6. | ☐ Full-year health care coverage (see instructions)

**Dependents** (see instructions): | (1) First name / Last name | (2) Social security number | (3) Relationship to you | (4) ✓ if qualifies for (see inst.): Child tax credit | Credit for other dependents

**Sign Here** — Under penalties of perjury, I declare that I have examined this return and accompanying schedules and statements, and to the best of my knowledge and belief, they are true, correct, and accurately reflect all amounts and sources of income I received during the tax year. Declaration of preparer (other than taxpayer) is based on all information of which preparer has any knowledge.

Joint return? See instructions. Keep a copy for your records.

Your signature | Date | Your occupation | If the IRS sent you an Identity Protection PIN, enter it here (see inst.)

Spouse's signature. If a joint return, **both** must sign. | Date | Spouse's occupation | If the IRS sent you an Identity Protection PIN, enter it here (see inst.)

**Paid Preparers** — Print/Type preparer's name | Preparer's signature | PTIN | Check if: ☐ 3rd Party Designee ☐ Self-employed

Firm's name ▶ | Firm's EIN ▶

**For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see separate instructions.** Cat. No. 11320B Form **1040** (2018)

- Configure the audit daemon and kernel.
- Inspect the audit log.



# Lab 7 - Advanced Intrusion Detection Environment (AIDE)

- Install `aide`.
- Baseline scan.
- Change a permission.
- Set an audit watch.
- Make it permanent.



# Lab 8 - IdM (not for 12/6/2021)

# Lab 9 - GNU Privacy Guard (GPG)

- Generate a new key pair
- Encrypt a document.



# Lab 10 - firewalld

- Verify the firewall is running.
- List firewall rules.
- Enable a
  - port
  - service
  - custom service



# Lab 11 - crypto policies

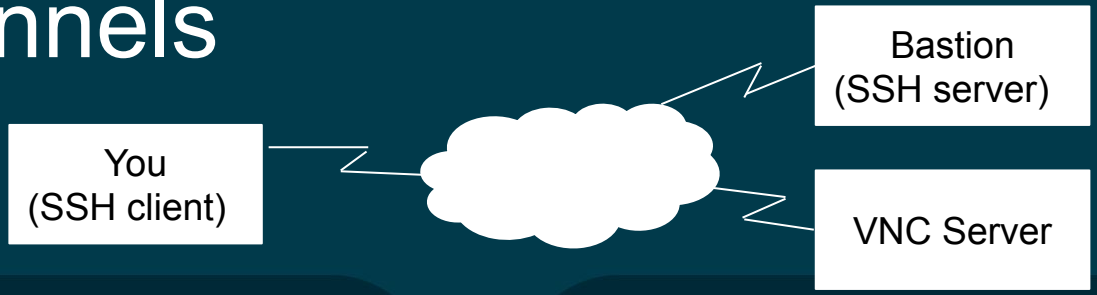
- Connect to a web server using TLS 1.1.
- Connect to a web server using a SHA-1 certificate.
- Switch to FIPS mode.
- Repeat.

# Lab 12 - Session Recording


- Set up recording.
- Create sessions recorded by `tlog`.
- Investigate recording problems.
- Use session player from the Cockpit UI.



# SSH Tunnels



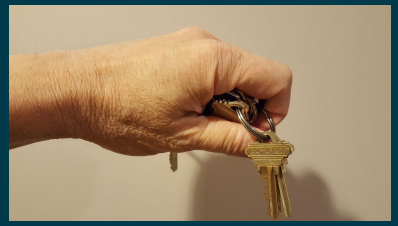

- Bastion server listens on TCP port 22.
- VNC server listens on TCP port 5901, but only to the bastion host.
- Your ssh client tunnels TCP port 5901 thru port 22 to the bastion host.
- The bastion host ssh server forwards to the VNC server.
- That's why you do a VNC connection to yourself at 127.0.0.1
- (Do your ssh from a local terminal window on your workstation. Activities...terminal)
  - Note - ssh from puTTY on Windows establishes a session. Ssh from a Linux workstation will just sit there after putting in the password.



## Lab 1 - OpenSCAP

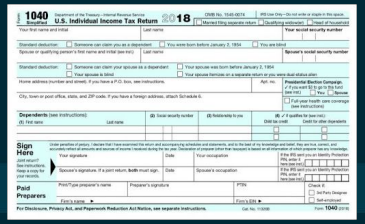



## Lab 2 - SELinux



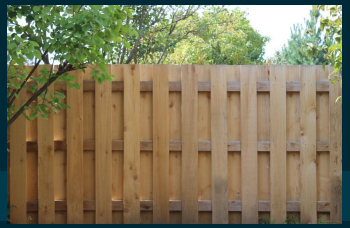
## Lab 3 - NBDE

## Lab 6 - Audit




## Lab 7 - AIDE

## Lab 9 - GNU Privacy Guard (GPG)



## Lab 10 - firewalld

## Lab 11 - crypto policies

## Lab 12 - Session Recording



Lab documentation:
https://2020-summit-labs.gitlab.io/rhel-security/

Video demo of all lab exercises:
https://drive.google.com/file/d/1a1RHpxiAjh4H0HSqMGaM1UdBGxzf_Rb4/view?usp=sharing