Zero Trust for Linux Admins

With Open-Source IAM

Thomas Cameron, RHCA, AWS SA Pro (he/him)
Senior Principal Solution Architect, Automation
thomas@redhat.com

Red Hat

What we'll discuss today

- Introductions: Who Am I?
- Introduction: De-fuzzing the Buzzword
- The Backbone: Centralized Identity with IdM
- Policy-Based Access: HBAC and sudo

Source:
Insert source data here
Insert source data here

What we'll discuss today

- Modern Auth: SSH Certificate Authorities
- Local Enforcement: Firewalld & SELinux
- Automation & Lessons Learned
- Conclusion & Q&A

Source:
Insert source data here
Insert source data here

Introductions:

Who Am I?

I’m Thomas Cameron!

- Professionally:
- I’ve been in IT since 1993.
- I started out with Novell NetWare
- Worked with Microsoft technologies
- Discovered Linux in 1995. I’ve been an Open Source geek ever since.
- I’ve managed large scale Linux environments for organizations from banking to real estate to chip manufacturing.
- I worked at Red Hat from 2005 through 2019, as a regional chief architect and global technical evangelist.
- I then went to AWS, where I was a senior technical trainer.
- In September of ‘24, I came back to Red Hat as a senior principal solution architect specializing in Ansible Automation.

Source:
Insert source data here
Insert source data here

De-fuzzing the Buzzword

Melted Perimeter

Melted Perimeter

It used to be that folks would come into the office, log in to their local network, and do their work. We had security at the physical level, and were protected by firewalls.

If folks needed remote access, they had to log in via a VPN.

Source:
Insert source data here
Insert source data here

Melted Perimeter

Now, we have SaaS for everything, and folks work remotely. We are expected to have work email and Slack/Teams/GChat/whatever installed on our phones (we're not going to argue the merits of this today - I only have an hour).

Source:
Insert source data here
Insert source data here

Credit Gemini

Melted Perimeter

The Flaw: Once a packet or a user crossed the drawbridge, they had "Lateral Liberty." We assumed that because you were on the internal VLAN, you were supposed to be there.

The concept of “internal vs. external” is DEAD. ☠️

Source:
Insert source data here
Insert source data here

The "Melted" Reality: Assume Breach

In a Zero Trust architecture, we treat the internal network as if it were a public Starbucks Wi-Fi.

- Network Location does not equal Trust: Just because an IP address comes from your local subnet doesn't mean it gets a pass.
- The Identity is the New Perimeter: Instead of a IP-based firewall rule, the "wall" is now a Kerberos ticket or an SSH Certificate tied to a specific human or service account.

Source:
Insert source data here
Insert source data here

The "Melted" Reality: Explicit Verification

In a Zero Trust architecture, **identity** is superior to IP address

- Even if you're logged into a VPN, do you **really** have permission to do what you're asking to?

Source:
Insert source data here
Insert source data here

The "Melted" Reality: Least Privilege

In a Zero Trust architecture, we grant the minimum necessary privileges to perform tasks

- Now we know who you are, what do you have permission to do?
- What apps can you use?
- What hosts can you log into?

Source:
Insert source data here
Insert source data here

The Linux Connection

In RHEL, we aren't just hardening the firewall to keep people out; we are using SSSD and Red Hat Identity Management to ensure that even if someone is 'inside' the network, they can't see or touch a single byte of data without a cryptographically proven identity.

Source:
Insert source data here
Insert source data here

The Backbone

Centralized Identity with Red Hat Identity Management

The Problem

Local /etc/passwd and hand-copied SSH keys are a security **nightmare**.

Source:
Insert source data here
Insert source data here

The Solution

Red Hat Identity Manager as the "Linux Domain Controller."

Source:
Insert source data here
Insert source data here

DEMO: Setting up IdM

DEMO: Registering to the Directory Server

DEMO: Show Registered Servers

Policy-Based Access: HBAC and Sudo

Host-Based Access Control (HBAC)

Moving beyond "can you log in" to "where are you allowed to be?"

- Example: DBAs can touch DB servers, but Web Devs cannot.

Source:
Insert source data here
Insert source data here

Centralized Sudo

Stop editing /etc/sudoers on each host!

- Define a rule in IdM.
- It propagates to the whole fleet via SSSD.

Source:
Insert source data here
Insert source data here

DEMO: Managing Access
Policy/HBAC

DEMO: Managing sudo

Policy/sudo

Modern Auth: SSH Certificate Authorities

SSH Certificate Authorities

The Risk

- Static SSH keys are "forever credentials." If a laptop is stolen, you're rotating 1,000 keys.

Source:
Insert source data here
Insert source data here

(Time permitting)

DEMO: IdM

As a CA

Local Enforcement: Firewalld & SELinux

Local Enforcement: Firewalld & SELinux

Micro-segmentation

- Using firewalld zones to ensure only the IdM server can talk to the Kerberos ports.

Source:
Insert source data here
Insert source data here

Local Enforcement: Firewalld & SELinux

SELinux as the Last Line

- Why "Assume Breach" means keeping SELinux in Enforcing mode to contain a compromised service.

Source:
Insert source data here
Insert source data here

Automation & Lessons Learned

Automation & Lessons Learned

GitOps for Identity

- Using Ansible to manage IdM users and HBAC rules as code.

Source:
Insert source data here
Insert source data here

Automation & Lessons Learned

Pitfalls to Avoid

- Time Sync: Kerberos will break if NTP drifts by >5 minutes.
- Break-glass Accounts: Always keep one local admin user in case the network/IdM is down.
- DNS: IdM is highly dependent on clean SRV records.

Source:
Insert source data here
Insert source data here

Conclusion & Q&A

Conclusion & Q&A

Summary

- Zero Trust isn't a product you buy; it's a configuration state you maintain.

Source:
Insert source data here
Insert source data here

Conclusion & Q&A

Call to Action

- Start by migrating one group’s sudo rules to IdM this week.

Source:
Insert source data here
Insert source data here

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

facebook.com/RedHat

youtube.com/@redhat

x.com/RedHat

Red Hat