

# Ultimate Linux Hardening Bootcamp

Defending against Linux attacks on-premises and in the cloud

**Omar Santos**  
**Joseph Mlodzianowski**

<https://hackinglinux.org>

# Agenda – Day 1

- Course Introduction and Setup
- Introduction to the Linux attack surface
- Linux Threat Modeling and Tools
- Distribution Independent Hardening
- Open-source security, SBOMs and VEX
- Introduction to Cloud Systems and Services Security
  
- Breaks – On the Hour for 15 min.

# Agenda – Day 2

- Hardening Red Hat Enterprise Linux
- Hardening Debian-based Linux
- Linux Security Modules
- Hardening Amazon Linux
- Container-optimized Linux Distributions
- Q&A

- During this live training we will share several additional resources.
- Note that all of the following slides include resources that you should leverage during this course.

<https://websploit.org>

<https://darkarts.io>





Class Website:

<https://hackinglinux.org>

# Ultimate Linux Hardening Bootcamp

Authors: Omar Santos and Joseph Mlodzianowski



GET STARTED

WebSploit Labs:  
<https://websploit.org>



# Course Introduction and Setup

# Distributions:

- Debian; Parrott, Kali, Ubuntu
- RHEL 8, 9
- Amazon & Cloud Linux



debian

<https://websploit.org>

<https://darkarts.io>



# Introduction to the Linux attack surface and threat modeling

# Common Linux Secure Tasks

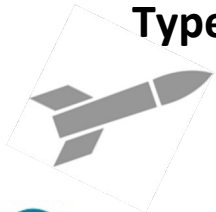
1. Physically secure your assets (servers)
2. Secure your Server Bios, UEFI
3. Utilize secure passwords, 2FA, setup PAM for controlled access to servers
4. Setup Secure Certificates access and disable (remote) root login
5. Keep your system up to date, apt update, apt dist-upgrade, yum update
6. Remove and/or disable unnecessary packages
7. Change the SSH keys, and use certificates, always a best practice
8. Restrict usage of the Root account, create specific user activity accounts
9. Install Antivirus and rootkit checkers
10. Install an auditing tool like lynis “apt install lynis” or OpenSCAP
11. Install and configure a firewall like UFW (uncomplicated firewall)
12. Enable logging, Tune it and ensure you are monitoring it.
13. Setup File integrity Monitoring, and encrypt sensitive files and data

## What is an attack surface?

An attack surface is defined as the total number of all possible entry points for unauthorized access into any system. It includes all vulnerabilities and endpoints that can be exploited to carry out a successful security attack.

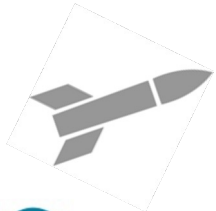
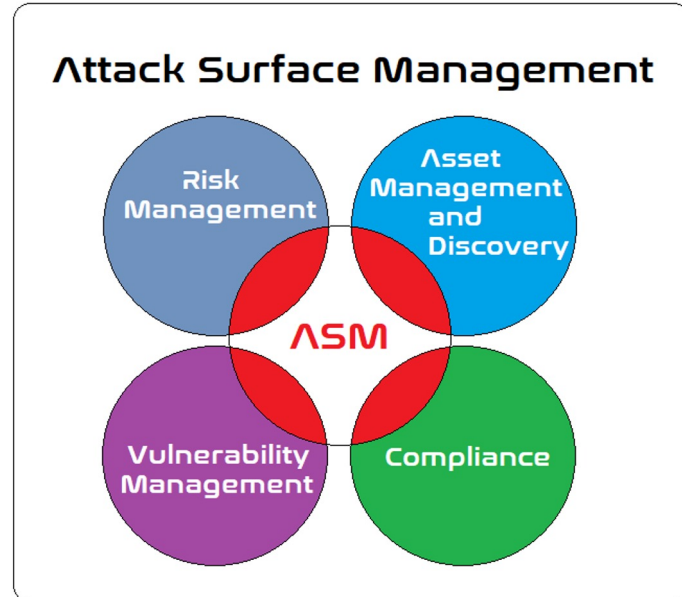
The attack surface is also the entirety of an organization exposure, the devices, applications and systems that are susceptible to hacking, in most organizations the attack surface is complex and massive.

**Types of Attack Surfaces:** Digital, Physical and Social Attack Surfaces



# Attack Surface Management

**Attack surface management (ASM)** refers to processes and technologies that take a hacker's view and approach to an organization's attack surface, discovering and continuously monitoring the assets and vulnerabilities that hackers see and attempt to exploit when targeting the organization.





# Attack Surface Monitoring

## Free:

1. OWASP Zed Attack Proxy
2. Attack Surface Mapper (ASM)
3. Axiom
4. Faraday

## Paid for:

1. CyCognito – Attack Surface Management
2. Rapid7 – InsightVM
3. IBM Randori Recon
4. Qomplx ASM

**Faraday** - <https://github.com/infobyte/faraday>

```
$ wget https://raw.githubusercontent.com/infobyte/faraday/master/docker-compose.yml
```

```
$ docker-compose up
```

**ATTACKSURFACEMAPPER**  
EXPAND YOUR ATTACK SURFACE

a x i o m

The dynamic infrastructure framework for everybody

**F Faraday**



# The Attack Surface & Risk Mitigation

## Six steps to creating a risk mitigation plan



### Identify the Risks

Identify systems and services, events and event sequences where risk is presented. Risk can be in the form of existing vulnerabilities or know threats.



### Perform a Risk Assessment

Weight potential impact and likelihood for it to occur for each risk. Find the quantitative value of each risk



### Rank & Prioritize

Rank and prioritize the potential risks from the most severe to the least. Areas with the most risk should be considered priority.



### Track All Risks

From weather to Cybersecurity, to cybersecurity attacks, if its a risk it should be followed and assessed. Plan your mitigation plan on frequency and potential occurrence.



### Implement and Monitor Progress

Once the Mitigation plan is active and in place, setup a process of continuous monitoring. Ensure the process is working as intended and schedule and perform tests to ensure it functions when needed. Make sure you update your plan as risks change.

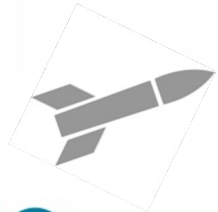
The final step - six is to start at one and run through the process as often as required.

# Threat Modeling

• **Threat modeling** is a method of optimizing Software, Systems, network security by locating vulnerabilities, identifying objectives, and developing countermeasures to either prevent or mitigate the effects of cyber-attacks against the system.



• **The Threat Modeling Process** consists of defining an enterprise's assets, identifying what function each application serves in the grand scheme, and assembling a security profile for each application. The process continues with identifying and prioritizing potential threats, then documenting both the harmful events and what actions to take to resolve them.



# Ten Threat Modeling Methodologies

- **Stride** – mnemonic for identifying security threats in six categories
- **Dread** – A way to rank and assess security risks in five categories
- **Pasta** – Dynamic Threat Identification, enumeration and scoring
- **Trike** – Focused on threat models as a risk management tool.
- **Vast** – Provides actionable outputs for various stakeholders.
- **Attack Tree** – A conceptual diagram showing how assets could be attacked
- **Common Vulnerability Scoring System CVSS** (not a threat model, but a scoring system for vulnerabilities) Low, Medium, High, Critical – Ranking 0 – 10, 10 being worst
- **T-Map** – Commercial off the Shelf (COTS) Calculate Attack path weights
- **Octave** – Risk-Based Strategic assessment and Planning method
- **Quantitative Threat Modeling** – Hybrid that combines Trees, Stride and CVSS

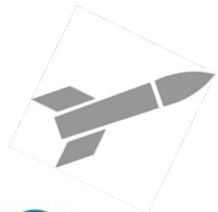


# Threat Modeling Tools



1. [OWASP Threat Dragon](#) is a modeling tool used to create threat model diagrams as part of a secure development lifecycle.
2. [OWASP Cornucopia](#) is a mechanism in the form of a card game to assist software development teams identify security requirements in Agile, conventional and formal development processes. It is language, platform and technology agnostic
3. [Threat Manager Suite](#) (TMS) / Threat Manager Studio (threatsmanager.com)

Others: [Cairis](#), Irius Risk, [OWASP Pytm](#), Threagile, ThreatModeler, Kenna.vm –now Cisco Vulnerability Management, [Microsoft Threat Modeling Tool](#) (follows STRIDE), [SDElements](#), and not last – [Tutamantic](#)

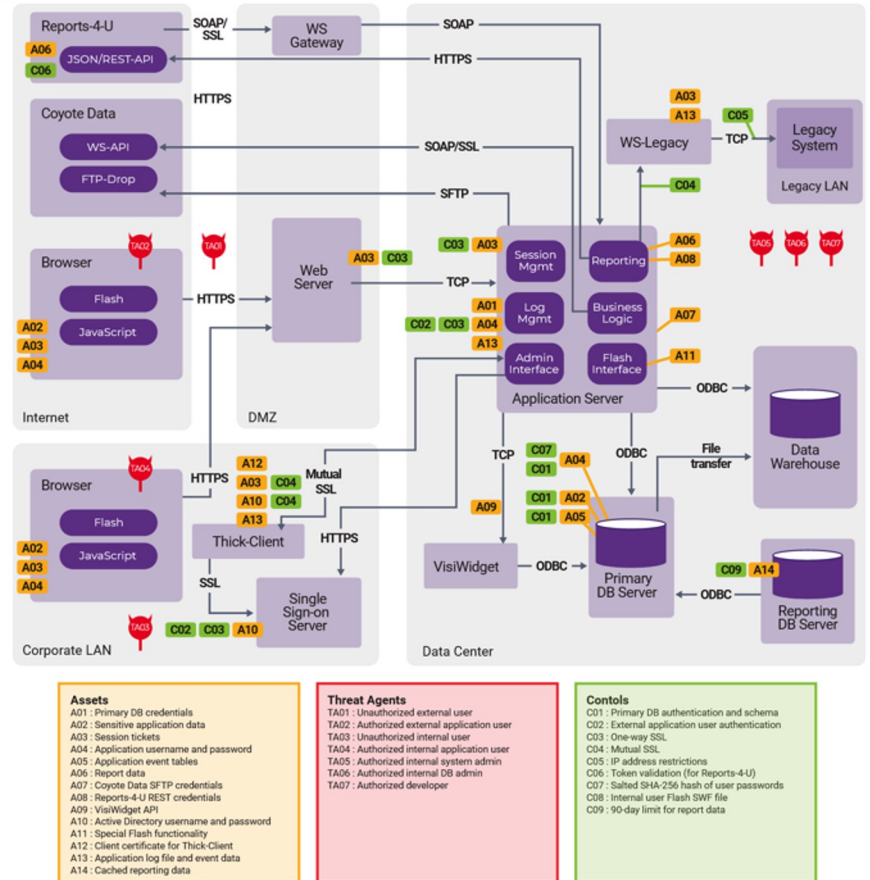


# Complexities of Threat Modeling - Lifecycle

As a security process, threat modeling is subject to several misconceptions. Some people believe threat modeling is only a design-stage activity, some see it as an optional exercise for which penetration testing or code review can substitute, and potentially catch issues.

Truth is that it must be considered part of the lifecycle of any program, applications, systems and services.

You must conduct a threat model after deployment. By understanding the issues in the current deployment, future security architecture strategy will be influenced.



Courtesy of Synopsys





# Install Debian, Kali, Parrott | RHEL

- Lab 1
- Install Your Preferred Debian type OS

- Run Websploit Script

- Lab 1.5
- Install RHEL 8.8 or 9.3



- Run rhel8 script



[Home](#) > [Products](#) > [Red Hat Enterprise Linux](#)

# Red Hat Enterprise Linux

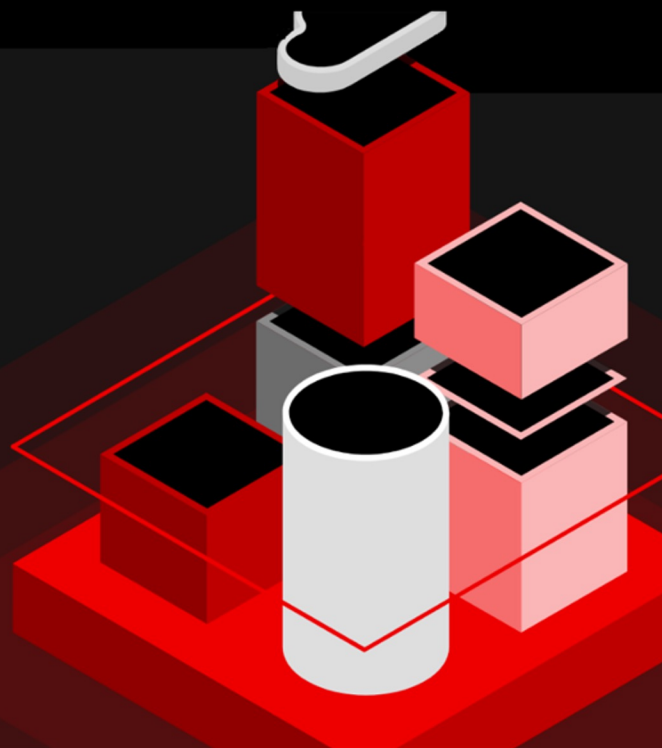
Everywhere enterprise IT is headed, Red Hat® Enterprise Linux® is there. From the public cloud to the edge, it evolves to bring flexibility and reliability to new frontiers. This is the stable foundation for untold innovation.

[Try it](#)

[Buy it](#)

[Talk to a Red Hatter](#)

Available on



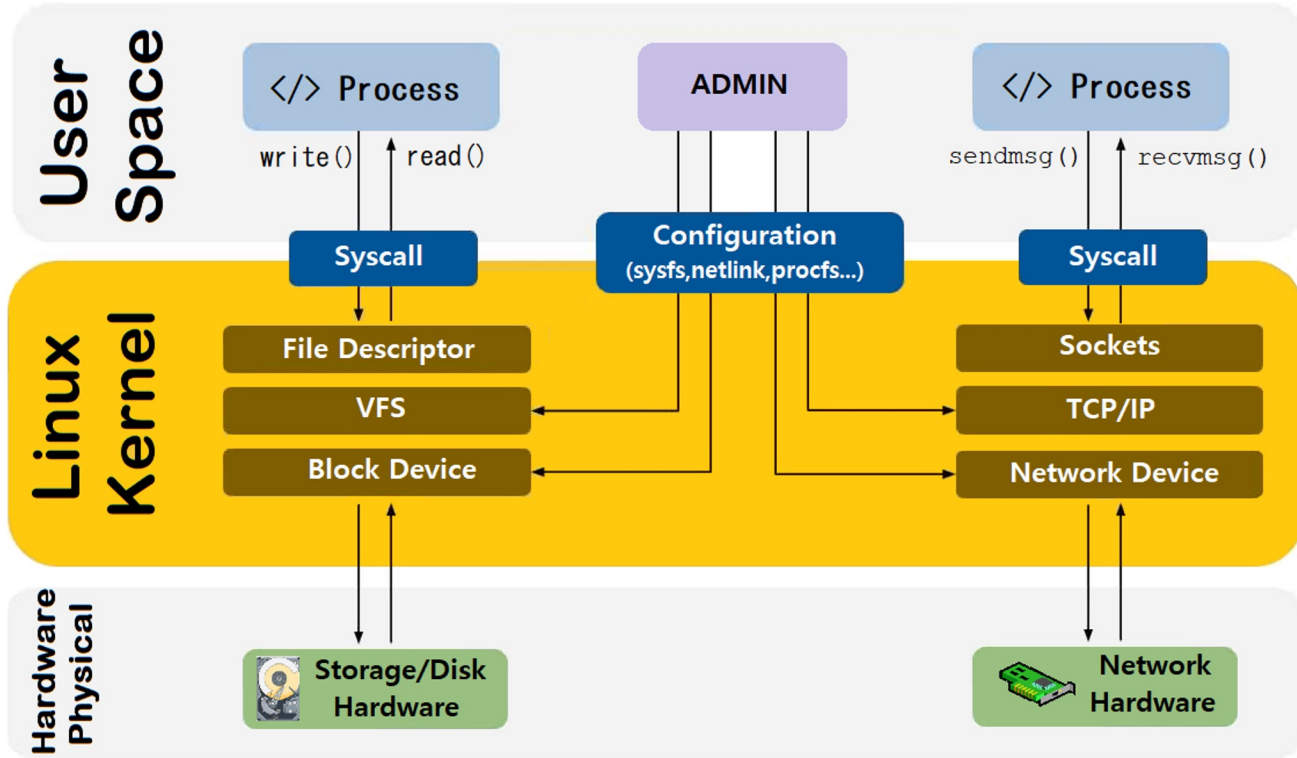


## Understanding the Linux kernel system

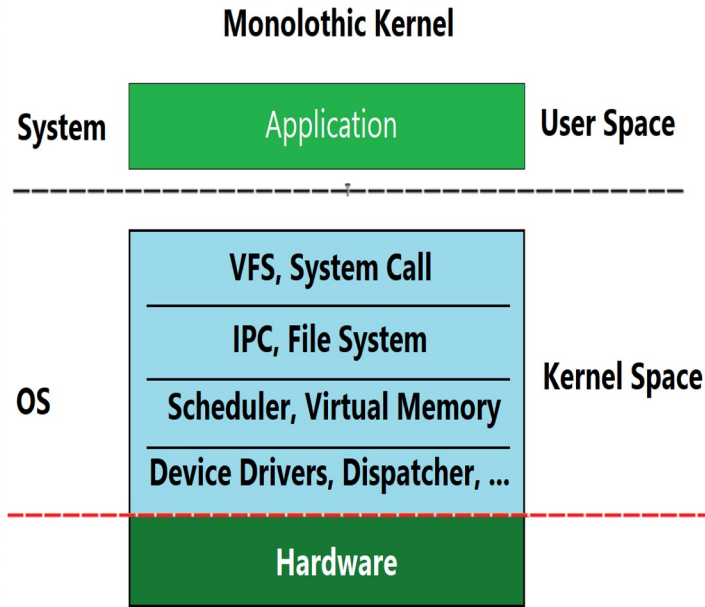
- The Linux kernel is a free and open-source, monolithic, modular, multitasking, Unix-like operating system component.
- Linux itself is provided under the GNU General Public License version 2 only. Since the late 1990s, it has been included as part of a large number of operating system distributions, many of which are commonly also called Linux, Such as Debian, Ubuntu, Red Hat, Fedora
- Linux Kernel Archives - <https://cdn.kernel.org>
- Linux Distrowatch - <https://distrowatch.com>



# Kernel Architecture



# Monolithic Kernel



Monolithic kernel is an operating system architecture where the entire operating system is running in kernel space. In a monolithic kernel, the OS runs in supervisor mode and the applications run in user mode. Supervisor mode enables execution of all instructions, including privileged instructions. As more code are executed in supervisor mode, the monolithic kernel has a larger memory and install footprint.

In Linux, developers found a way to solve this problem by creating dynamically loadable modules. Modules can be loaded dynamically at runtime. These modules allow easy extension of the operating system's capabilities as a per user requirement. A module typically adds functionality to OS for devices, file systems, and system calls.

# Kernel and User Space



**Userspace:** Computer operating system segregate virtual memory into user space and kernel space. Primarily, this separation serves to provide memory protection and hardware protection from malicious or errant software behavior.

<https://docs.kernel.org/userspace-api/index.html>



**Kernel Space:** Kernel Space is strictly reserved for running a privileged operating system kernel, kernel extensions, and most device drivers.

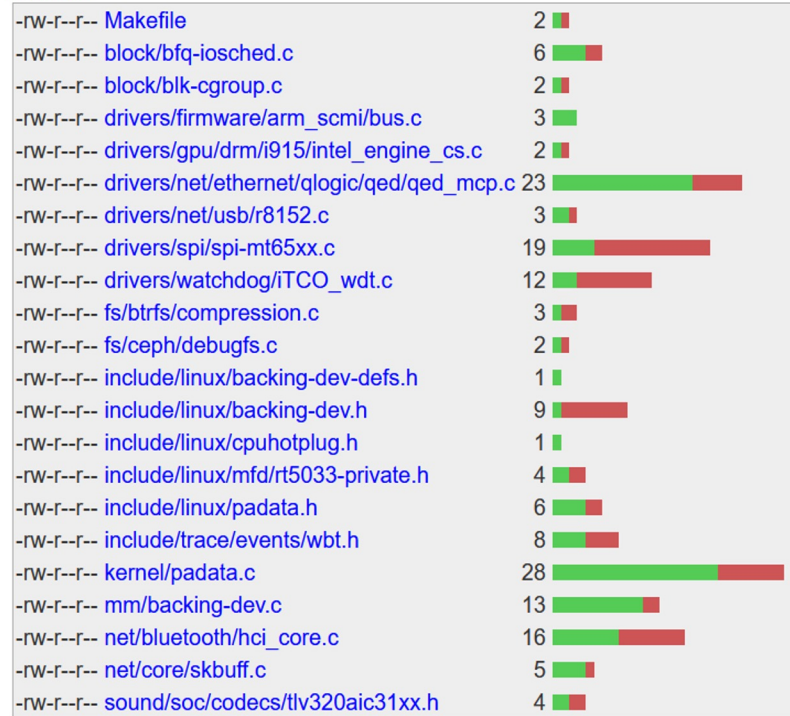
Kernel Space	User Space
Kernels and OS core execute here.	Normal program and applications softwares run here.
Its the core space of OS.	It's a form of sand-boxing that restricts user processes to access OS kernel.
It has full access to all memory and machine hardware.	It has limited access to memory and access kernel through system calls only.
It contains the page table for process, kernel data structure, threads, and kernel code etc.	It contains the program code, data, stacks, and heap of the process.



Summary of changes each time the kernel is updated can be located at Kernel.org

<https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/diff/?id=v4.19.202&id2=v4.19.201&dt=2>

#### Diffstat



22 files changed, 97 insertions, 75 deletions



# Check your Kernel

## LAB 1

To see what your running perform the following command as a general user or root.

> hostnamectl | grep Kernel

```
root@dw00k0:~# hostnamectl | grep Kernel
Kernel: Linux 5.18.0-kali7-amd64
```

Next let's check our linux distribution level

> uname -a

```
mxrxdp@dw00k0:~$ uname -a
Linux dw00k0 5.18.0-kali7-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.16-1kali1 (2022-08-31) x86_64 GNU/Linux
```

Next let's check what is publicly available for our distribution

> apt search linux-headers | grep headers



**Cloud Computing** is the delivery of computing services—which includes servers, storage, databases, networking, software, analytics, and intelligence - delivered over the Internet (“the cloud”) or Private Network to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.

**Cloud security** (also known as cloud computing security) includes many of the same security controls, technologies, practices and procedures that are used to protect physical data centers, network and compute environments—only they are deployed as a service to protect your data that resides in the cloud



# Benefits of Cloud Compute



## Cost

Cloud computing eliminates the capital expense of buying hardware and software and setting up and running on-site datacenters—the racks of servers, the round-the-clock electricity for power and cooling, and the IT experts for managing the infrastructure. It adds up fast.



## Speed

Most cloud computing services are provided self service and on demand, so even vast amounts of computing resources can be provisioned in minutes, typically with just a few mouse clicks, giving businesses a lot of flexibility and taking the pressure off capacity planning.



## Global scale

The benefits of cloud computing services include the ability to scale elastically. In cloud speak, that means delivering the right amount of IT resources—for example, more or less computing power, storage, bandwidth—right when they're needed, and from the right geographic location.



## Productivity

On-site datacenters typically require a lot of “racking and stacking” —hardware setup, software patching, and other time-consuming IT management chores. Cloud computing removes the need for many of these tasks, so IT teams can spend time on achieving more important business goals.



## Performance

The biggest cloud computing services run on a worldwide network of secure datacenters, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This offers several benefits over a single corporate datacenter, including reduced network latency for applications and greater economies of scale.



## Reliability

Cloud computing makes data backup, disaster recovery, and business continuity easier and less expensive because data can be mirrored at multiple redundant sites on the cloud provider's network.



## Security

Many cloud providers offer a broad set of policies, technologies, and controls that strengthen your security posture overall, helping protect your data, apps, and infrastructure from potential threats.

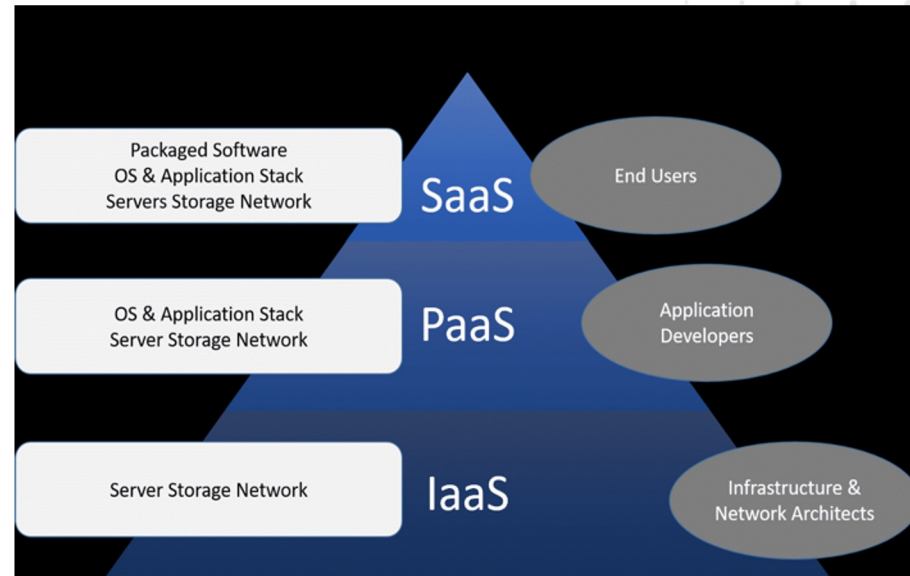


# Types of Cloud Services

## Types of cloud services: IaaS, PaaS, serverless, and SaaS

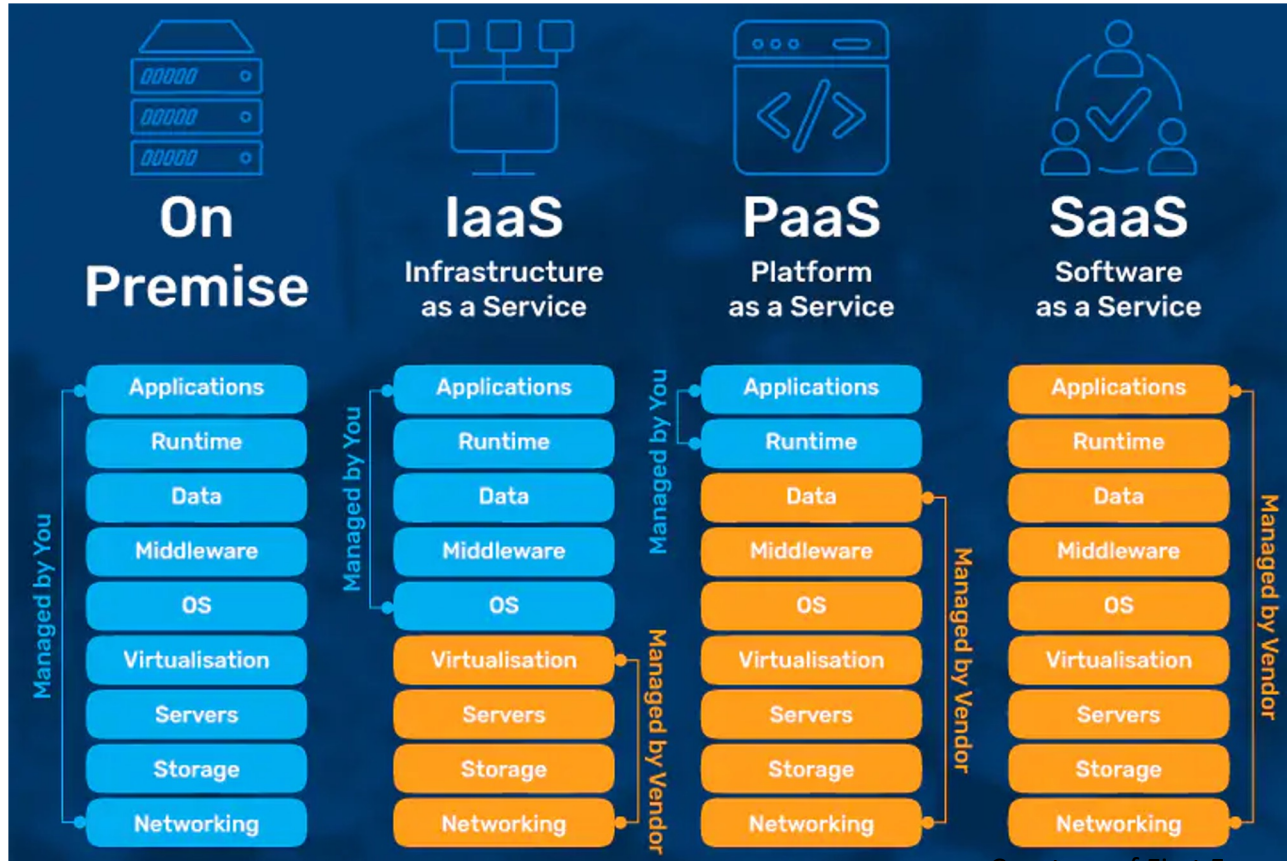
Most cloud computing services fall into four broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), serverless, and software as a service (SaaS). These are sometimes called the cloud computing "stack" because they build on top of one another. Knowing what they are and how they're different makes it easier to accomplish your business goals.

**Infrastructure as a service (IaaS)** The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

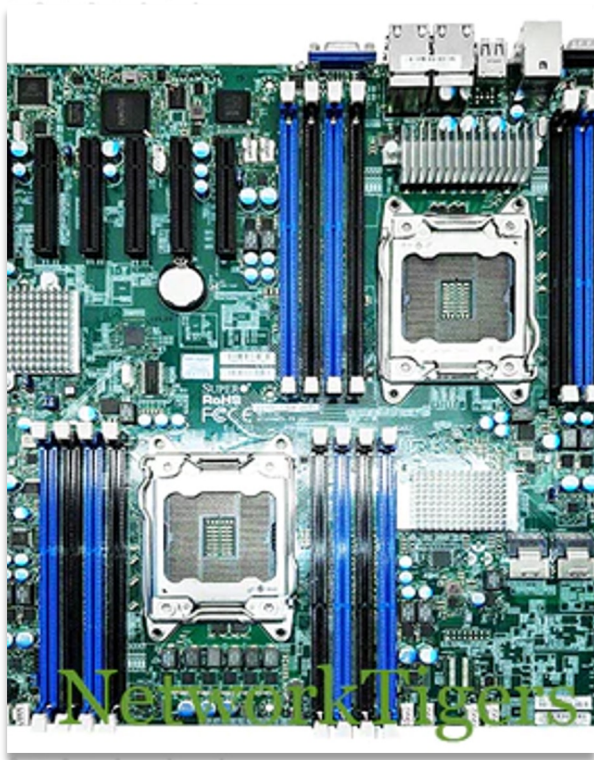


# aaS managed by/used by

- Private Cloud
- Public Cloud
- Hybrid Cloud
- App Cloud
- Backup Cloud
- DR Cloud



# Securing the Front line 'Bios



Administrators can access the BIOS at startup to change how the hardware operates as needed; businesses that make use of legacy devices, for example, can alter the BIOS to enable the motherboard to detect and utilize older hardware. You can access the BIOS from the boot screen using a specific keyboard combination.

In some cases, it's the DEL key, in other cases is the F2 key, check your specific manufactures details to gain access to your system Bios.

Keep your bios up to date with manufacture updates



# Common BIOS settings for ASUS Motherboard

Common BIOS settings for ASUS Motherboards

For common BIOS setting options, you can refer to below FAQs.

Update BIOS	Introduction of methods for update BIOS	[Motherboard] How to update BIOS of the motherboard ?
	Method 1: EZ Flash	[Motherboard] ASUS EZ Flash 3 - Introduction
	Method 2: EZ Update	[Motherboard] EZ Update - Introduction
	Method 3: USB BIOS FlashBack	[Motherboard] How to use USB BIOS FlashBack™?
Fail to update BIOS	Fail to update BIOS	[Motherboard] Troubleshooting - BIOS fails to update
Clear CMOS	CMOS	How to clear CMOS?
Save and load the BIOS settings	User Profile	[Motherboard] How to save and load the BIOS settings?
Switch BIOS language	switch BIOS language	[Motherboard] How to switch (select) BIOS language
Battery	How to replace CMOS battery on motherboard	[Motherboard] How to replace CMOS battery on motherboard when it runs out power ?
An error after boot up: WARNING!BIOS Recovery mode has been detected	An error after boot up: WARNING!BIOS Recovery mode has been detected	[Motherboard] Troubleshooting-When "WARNING! BIOS Recovery mode has been detected" message is displayed Processing method of abnormal boot
Need to press F1 when boot the system	Need to press F1 when boot the system	[Motherboard]Error shows when I boot the system, need to press F1 to enter operation system
An error "CPU Over Temperature Error" occurs after bootup	An error "CPU Over Temperature Error" occurs after bootup	[Motherboard] Troubleshooting-An error "CPU Over Temperature Error" occurs after bootup
Setup TPM 2.0 in BIOS	TPM2.0	[Motherboard] Which ASUS model supports Windows 11 and how to setup TPM 2.0 in BIOS?
Virtualization Technology	VT/SVM	[Motherboard]How to set VT(Virtualization Technology) in BIOS and install Virtual Machine in Windows
DRAM overclock	XMP/DOCP	[Motherboard]How to optimize the Memory performance by setting XMP or DOCP in BIOS?
RAID	RAID	[Motherboard]How to create RAID in BIOS Setup
WOL	WOL	[Motherboard]How to set and enable WOL(Wake On Lan) function in BIOS
RTC	RTC	[Motherboard] How to turn on your computer automatically by setting BIOS RTC (Real time clock) ?
Power on by keyboard	PS/2 keyboard	[Motherboard] How to enable "power on by PS/2 keyboard" via BIOS setting
Disable standby power of the USB connected device	Standby power of the USB connected device	[Motherboard] How to disable standby power of the USB connected device
Disable automatic download	Armoury Create	[Motherboard] How to disable automatic download of Armoury Crate via BIOS Setting?
Can't enable CSM option	Intel 500series motherboards	[Motherboard] When I use the integrated graphics card on the Intel® 500 series motherboard , why does the CSM option under BIOS appear gray and non-configurable?

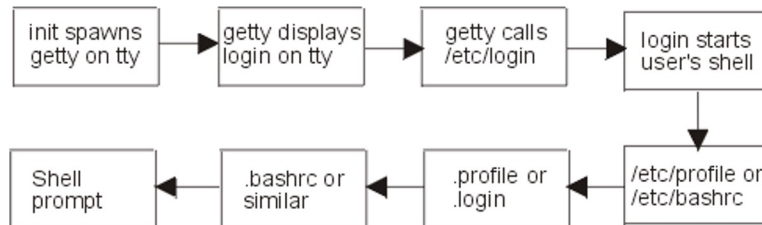


# Unix Passwords

Unix passwords are encrypted with a one-way function, which makes it nearly impossible to decrypt. The login program accepts the text you enter at the password window and uses it as a key to encrypt a 64-bit block of nulls.

The first seven bits of each character are extracted to form a 56-bit key. The results of that algorithm are then compared against the encrypted form of your Unix password stored in the password file.

This means that only eight characters are significant in a standard Unix password, the E-table is then modified using the salt, which is a 12-bit value, coerced into the first two chars of the stored password.



# The Unix Salt



The DES salt is a 12-bit number, between 0 and 4,095, which slightly changes the result of the DES function. Each of the 4,096 different salts makes a password encrypt a different way.

When you change your password, the `/bin/passwd` program selects a salt based on the time of day. The salt is converted into a two-character string and is stored in the `/etc/passwd` file along with the encrypted “password.”

So when you type your password at login time, the same salt is used again. Unix stores the salt as the first two characters of the encrypted password.

# Unix Password Audits

The purpose of the salt's is to make precompiled password lists and DES hardware chips more time consuming to use. There is 64-bit output block from the 25 iterations DES is invoked, the results coerced into a 64-character alphabet (A-Z,a-z, ".", "/").

This involves translations in which several different values are represented by the same character, which is why Unix passwords cannot be decrypted.

The more time consuming and compute intensive we can make decrypting, the less likelihood of a compromised password with-in the change window.

# Modular Crypt Format (MCF)

The Modular Crypt Format (MCF) specifies an extensible scheme for formatting encrypted passwords. MCF is one of the most popular formats for encrypted passwords around today.

Dollar signs are used to delimit the MCF fields,

- #1 Specifies encryption algorithm to use - 1 - MD5 / 2 - Blowfish
- #2 Salt – Limited to 16 Characters
- #3 Encrypted Password – Does not include salt





**Passwords:** The reuse of passwords can lead to online account attacks and compromises, called credential stuffing, where password collectors' pickup your passwords compromised on a specific website and then try to reuse them on many sites. And while one of our labs shows you how to remove passwords from your system and rely on key pairs, passwords are still a fact of life. Using a password manager is the preferred method, never reuse passwords on public sites – ever.



# Password Audit Tools

**Tool:** John the Ripper



**Tool:** Hashcat

**Tool:** Salt Scanner

**Tool:** Hydra

```
lit@kali$ john --wordlist=matkweb7-orp1000.txt --format=Raw-md5 md5-passwords.txt
Using default input encoding: UTF-8
Loaded 18765 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16x3])
Remaining 12764 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2022-09-26 23:27) 0g/s 124937p/s 124937c/s 1594MC/s gribouille..starstar
Session completed.
```



# What does PAM do for me ?

PAM separates the standard and specialized tasks of authentication from applications. Programs such as login, gdm, sshd, ftpd, and many more all want to know that a user is who they say they are, yet there are many ways to do that. A user can provide a user name and password credential which can be stored locally or remotely with LDAP or Kerberos. A user can also provide a fingerprint or a certificate as a credential. It would be painful to ask each application developer to rewrite the authentication checks for each new method. A call to PAM libraries leaves the checks to authentication experts. PAM is pluggable in that we can have different applications run different tests and modular in that we can add new methods with new libraries.

*Pluggable Authentication Modules (PAM) was been around since 1997*



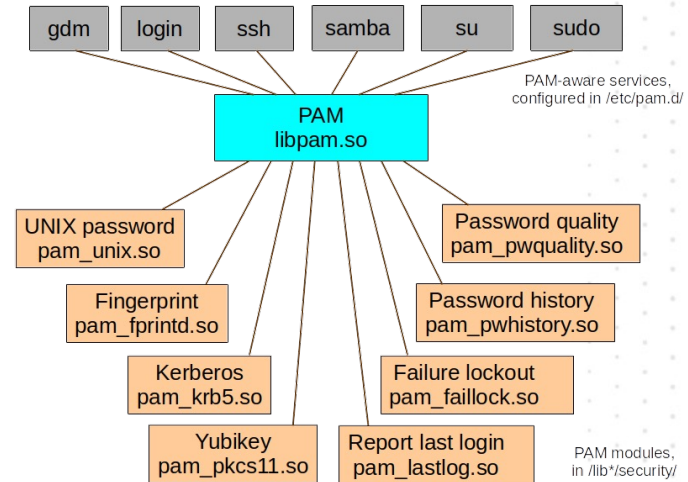


# Passwords, PAM and NSS

- Configure PAM on Debian
- <https://www.debian.org/doc/manuals/debian-reference/ch04.en.html>

- Configure PAM for AWS  
<https://docs.aws.amazon.com/emr/latest/ReleaseGuide/emr-jupyterhub-pam-users.html>

- Configure PAM on RHEL
- <https://tinyurl.com/296hd4w>



# Enabling Multi-Factor Authentication

```
GNU nano 2.2.6 File: sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details
#
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

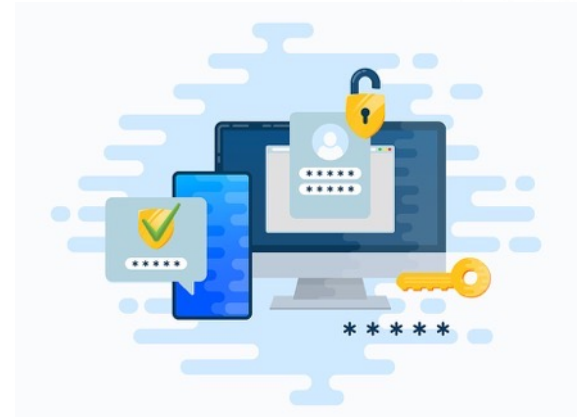
# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin without-password
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

Read 88 lines
AC Get Help      AC WriteOut     AR Read File    AY Prev Page    AK Cut Text     AC Cur Pos
AX Exit         AJ Justify      AW Where Is    AV Next Page    AU UnCut Text  AT To Spell
```



<https://duo.com/docs/loginduo>

<https://www.redhat.com/sysadmin/mfa-linux>

# Audit

Password Audits, Vulnerability Assessments, Pentesting, CIS audits, logging are all part of best practices when managing a server(s). We will get into specifics of scanning, audits and remediation in great detail further in this course

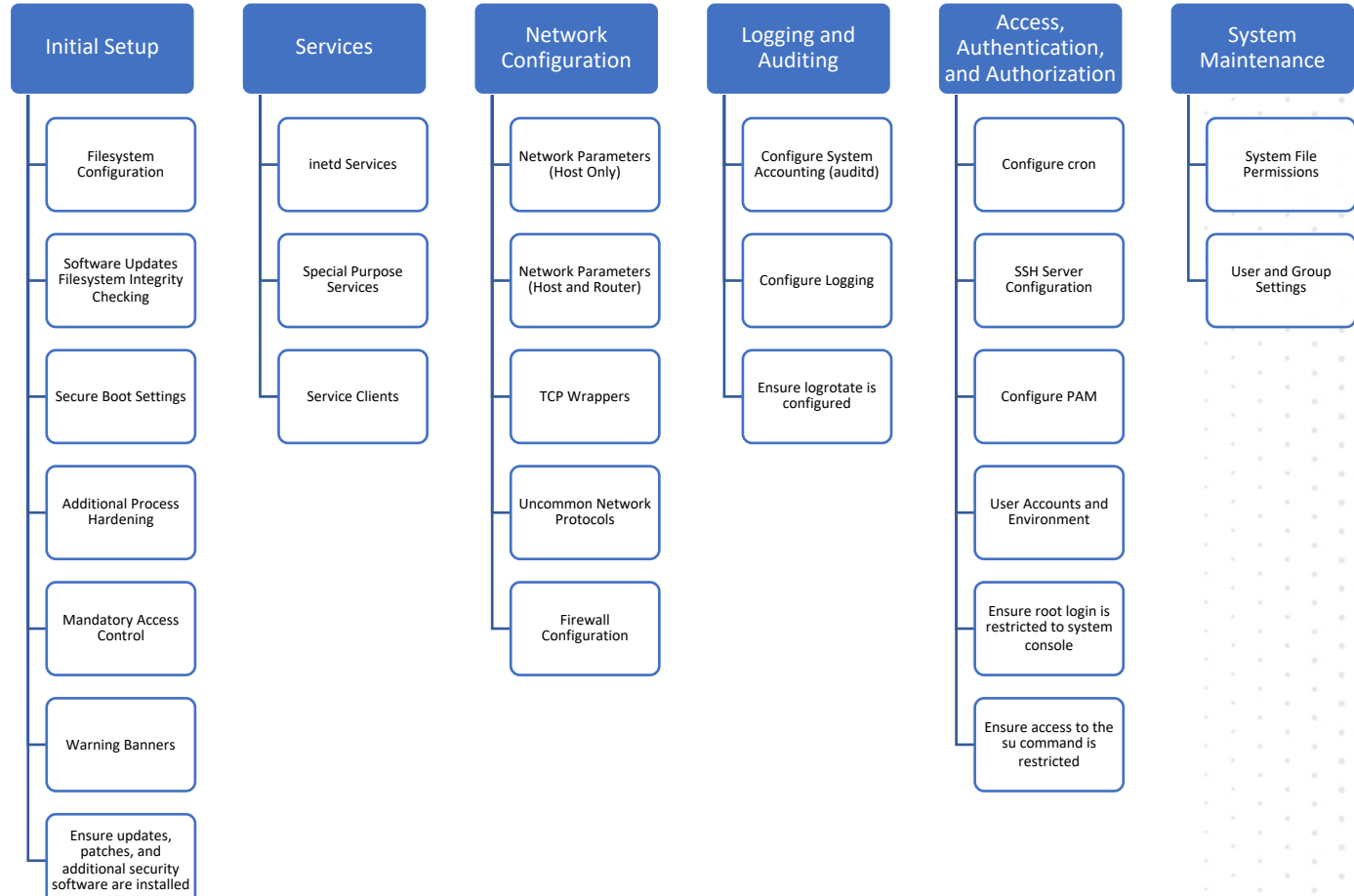




# Distribution Independent Hardening



# CIS Benchmark: Distribution Independent Best Practices



# CIS WORKBENCH & DIL TOOLS DEMO

The screenshot displays the CIS Workbench web application. The top navigation bar includes links for Communities, Benchmarks, Tickets, Downloads, and Support Center. The left sidebar shows a tree view of benchmarks, with '6.2 - User and Group Settings' selected. The main content area is titled '6.2 User and Group Settings' and contains an 'Overview' section with a note about auditing local users and groups. Below the overview, there is a section for 'Recommendations' which lists three items: 6.2.1, 6.2.2, and 6.2.3. The right-hand panel shows 'Tickets for User and Group Settings' with a message 'No tickets listed'.

CIS Workbench

Communities Benchmarks Tickets Downloads Support Center

Files Tickets

1 - Initial Setup  
2 - Services  
3 - Network Configuration  
4 - Logging and Auditing  
5 - Access, Authentication and Author...  
6 - System Maintenance  
6.1 - System File Permissions  
6.2 - User and Group Settings  
6.2.1 - Ensure password fields are not...  
6.2.2 - Ensure no legacy "+" entries ex...  
6.2.3 - Ensure no legacy "+" entries ex...  
6.2.4 - Ensure no legacy "+" entries ex...  
6.2.5 - Ensure root is the only UID 0 a...  
6.2.6 - Ensure root PATH Integrity  
6.2.7 - Ensure all users' home...  
6.2.8 - Ensure users' home dir...  
6.2.9 - Ensure users own their home d...  
6.2.10 - Ensure users' dot files are not...  
6.2.11 - Ensure no users have .forward...  
6.2.12 - Ensure no users have .netrc fi...  
6.2.13 - Ensure users' .netrc Files are...

6.2 User and Group Settings

Overview

This section provides guidance on securing aspects of the users and groups.

**Note:** The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

No Subsections Listed

Recommendations

6.2.1	Ensure password fields are not empty
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow

Tickets Discussions

Tickets for User and Group Settings

No tickets listed

<https://workbench.cisecurity.org>

# CIS Distribution Independent Linux Benchmark - InSpec Profile

☰ README.md

## CIS Distribution Independent Linux Benchmark - InSpec Profile

---

### Description

This profile implements the [CIS Distribution Independent Linux 2.0.0 Benchmark](#).

---

### Attributes

To switch between the CIS profile levels the following attribute can be used:

- `cis_level: 2` define which profile level to use, accepted values are `1` and `2`.

---

### License and Author

- Author:: Kristian Vlaardingerbroek [kvlaardingerbroek@schubergphilis.com](mailto:kvlaardingerbroek@schubergphilis.com)

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

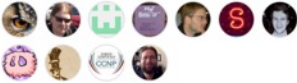
<http://www.apache.org/licenses/LICENSE-2.0>

### Packages

No packages published

---

### Contributors 23



+ 12 contributors

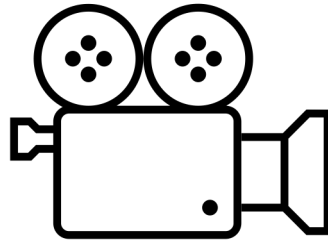
---

### Languages

● Ruby 100.0%

<https://github.com/dev-sec/cis-dil-benchmark>

# CIS Benchmark Automation Demo



I also posted the longer version of the video at:

<https://youtu.be/rozH4ZhA028>

# OpenSCAP

# SCAP Standards Support

- OpenSCAP is based on the Security Content Automation Protocol (SCAP) standards, which define a standardized approach for expressing and sharing security-related information.
- It supports SCAP content in the form of Security Content Automation (SCAP) data streams, such as XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language).

<https://www.open-scap.org>

# Security Baselines and Policies

- OpenSCAP allows users to create security baselines and policies based on various industry standards, such as DISA STIGs (Security Technical Implementation Guides) and CIS (Center for Internet Security) benchmarks.
- OpenSCAP can scan Linux systems to evaluate their compliance with the defined security policies. It checks the configurations of various components, including services, packages, filesystem permissions, and more.



You Know What's Also Important?

# ASSET MANAGEMENT AND ACCURATE SYSTEM IDENTIFICATION

# Not only for Security, also for Financial Control

- Effective asset management allows organizations to have better financial control.
- By knowing what assets they own, their value, and their condition, organizations can make informed decisions about budgeting, investments, and resource allocation.
- Asset management helps optimize costs by preventing unnecessary purchases and ensuring assets are utilized efficiently.
- It helps identify underutilized or redundant assets that can be retired or repurposed, saving money in the process.

# Risk Mitigation

- Proper asset management reduces the risk of financial and operational losses.
- It ensures that assets are well-maintained, reducing the likelihood of breakdowns or failures that could lead to costly downtime or accidents.

# Compliance and Accountability

- Many industries have regulatory compliance requirements related to asset management.
- Maintaining accurate records and adhering to compliance standards helps organizations avoid penalties and legal issues.
- It also promotes accountability and transparency within the organization.

# Open source security, SBOMs and VEX

# 1

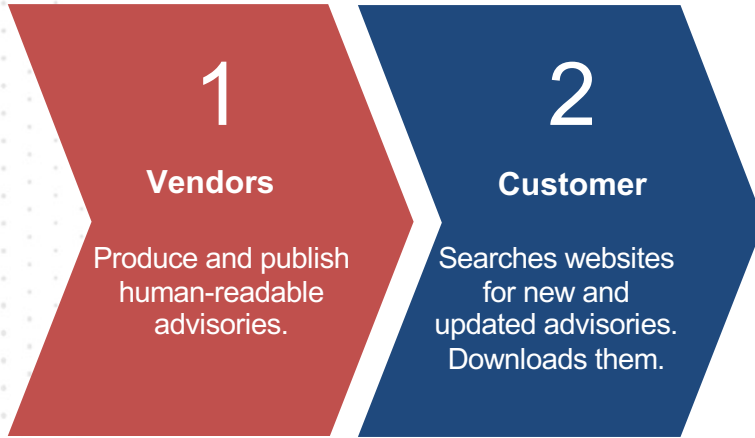
## Vendors

Produce and publish human-readable advisories.

Severity	
	critical
	high
	medium
	low

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

∪ ∪



**Severity**

- critical
- high
- medium
- low

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15





**Severity**

- critical
- high
- medium
- low

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

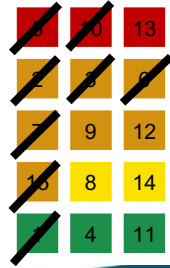
1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

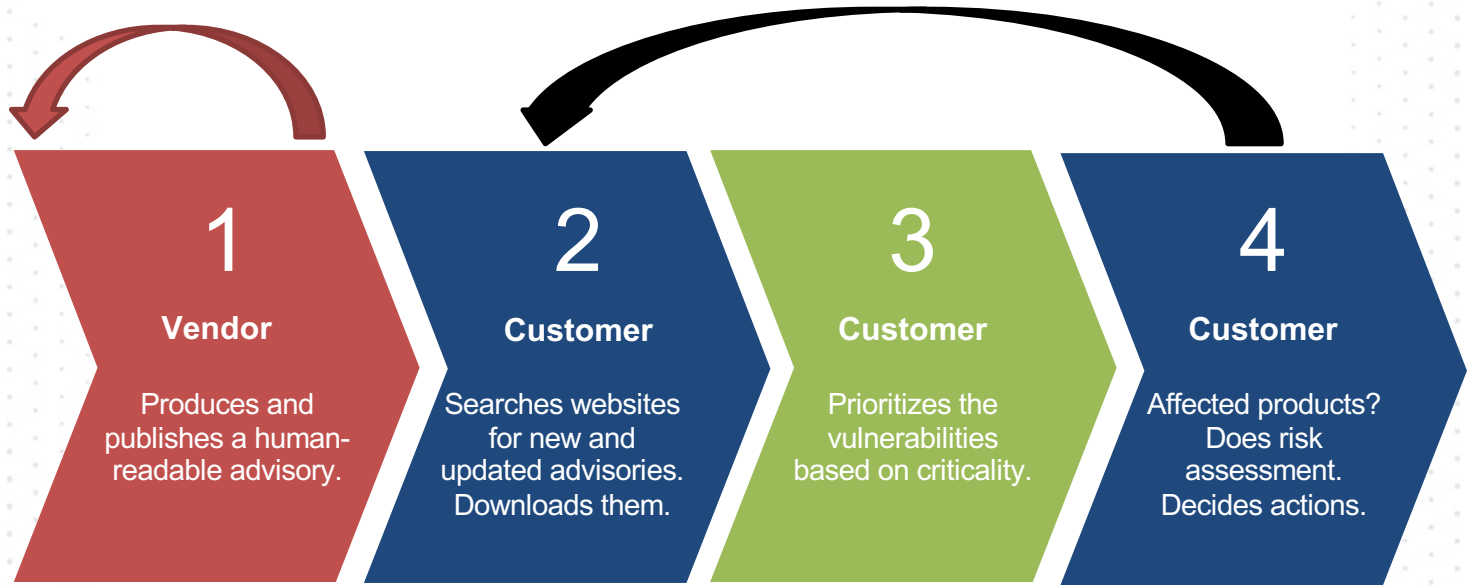
5	10	13
2	3	6
7	9	12
15	8	14
1	4	11



**Severity**

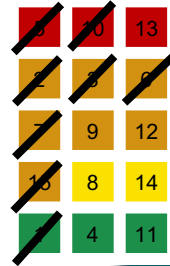
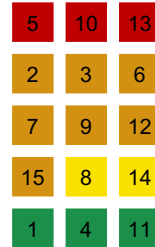
- critical
- high
- medium
- low





**Severity**

- critical
- high
- medium
- low



# Problems to Solve

- Many vendors – all with different formats and distribution methods
  - Number of security advisories is rising
  - SBOM adds to overload
  - Not every vulnerability can be exploited
- 
- Scalability
- Exploitability

# The Common Security Advisory Framework (CSAF)

*An open and definitive reference for the language which supports the creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties.*

Spec, Docs, Tools, Presentations, FAQs:

<https://csaf.io>



Is CSAF a Replacement or  
Alternative to CVE?

**NO**

CSAF is the replacement for the Common Vulnerability Reporting Framework (CVRF).

However, it introduces a completely new ecosystems and several additional features.



# Profiles

CSAF Base

Security Advisory

Informational Advisory

Security Incident Response

Vulnerability Exploitability Exchange (VEX)

# VEX Profile

The Vulnerability Exploitability eXchange (VEX) allows a software supplier or other parties to assert the status of specific vulnerabilities in a particular product..

## References:

CISA's VEX Use Cases: [https://www.cisa.gov/sites/default/files/publications/VEX\\_Use\\_Cases\\_April2022.pdf](https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_April2022.pdf)

CISA's VEX Justifications: [https://www.cisa.gov/sites/default/files/publications/VEX\\_Status\\_Justification\\_Jun22.pdf](https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf)

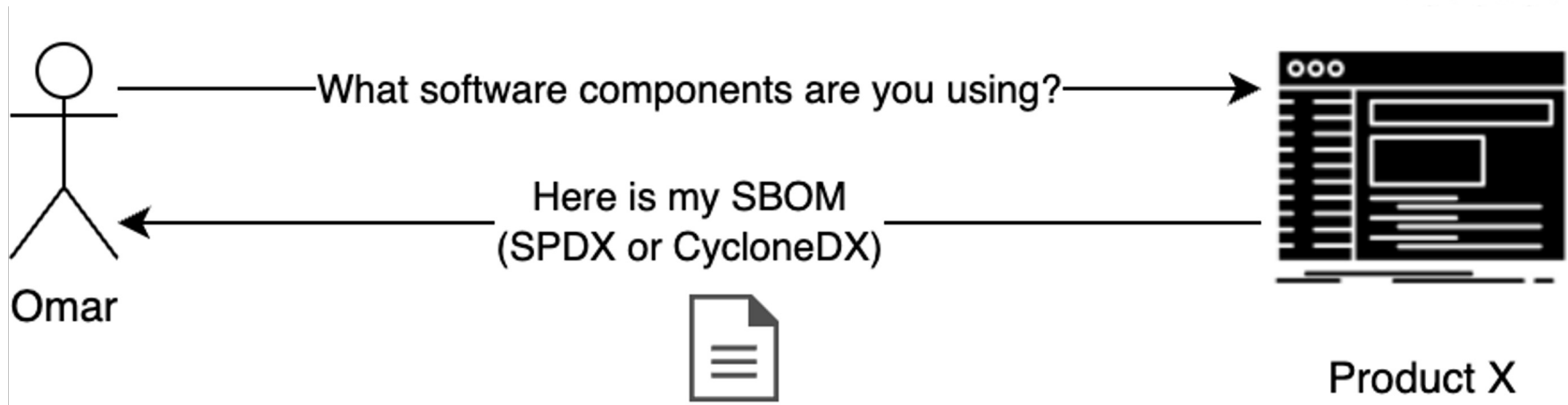
# Recap on SBOM Standards

The two “most popular” or “widely-adopted” SBOM machine readable formats are:

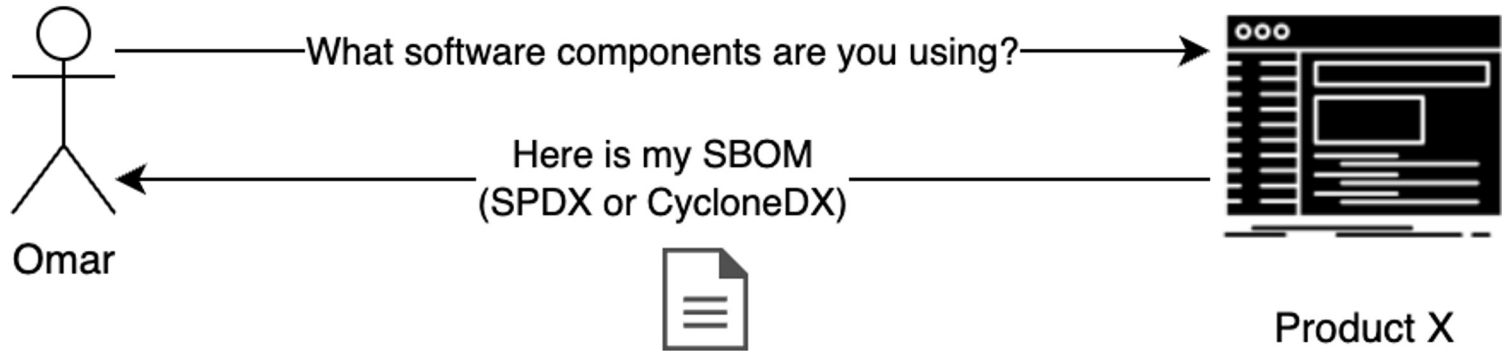
- Software Package Data Exchange (SPDX®): an ISO/IEC standard introduced as a Linux Foundation Project.
- CycloneDX: a lightweight SBOM specification and an open-source OWASP standard.

**Note:** Check out the “Survey of Existing SBOM Formats and Standards”, created by the NTIA and other collaborators, to learn more about how these standards (along with others) are used in the industry.

# How Does This Work?

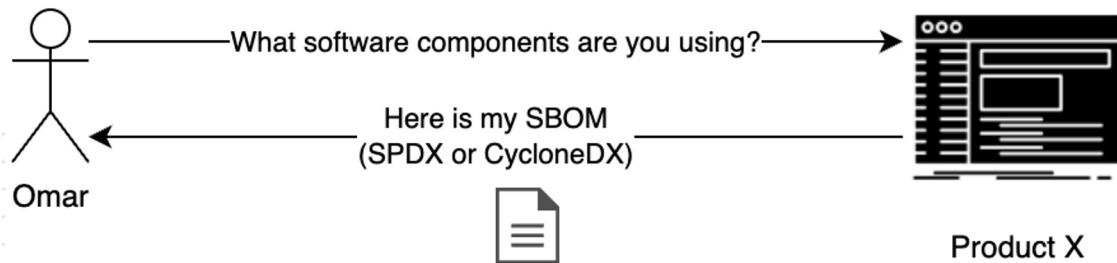


# How Does This Work?



What security vulnerabilities affect those components or are fixed?

My SBOM includes the list of affected, under investigation, and fixed vulnerabilities (as of today) using the Vulnerability Exploitability Exchange (VeX)



What security vulnerabilities affect those components or are fixed? →

← My SBOM includes the list of affected, under investigation, and fixed vulnerabilities (as of today) using the Vulnerability Exploitability Exchange (VeX)

But, that's "point-in-time"... new vulnerabilities are disclosed on a regular basis... →

← No worries, you can use the Common Security Advisory Framework (CSAF) VeX documents...

# CSAF in SPDX and CycloneDX

- CSAF is Supported in SPDX and CycloneDX

**SPDX 2.3:** <https://spdx.github.io/spdx-spec/v2.3-RC1/how-to-use/>

```
"externalRefs" : [ {  
    "referenceCategory" : "SECURITY",  
    "referenceLocator" : "https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/examples/csaf/csaf_vex/2022-evd-uc-01-a-  
001.json",  
    "referenceType" : "advisory" } ]
```

**CycloneDX:** <https://cyclonedx.org/capabilities/vex/#cyclonedx-and-third-party-advisory-formats> and <https://cyclonedx.org/use-cases/#security-advisories>

```
"externalReferences": [  
  {  
    "type": "advisories",  
    "url": "https://example.org/.well-known/csaf/advisory1.json"  
  }  
]
```

# VEX Statuses and Justifications

under\_investigation

known\_affected

fixed

known\_not\_affected

component\_not\_present

inline\_mitigations\_already\_exist

vulnerable\_code\_cannot\_be\_controlled\_by\_adversary

vulnerable\_code\_not\_in\_execute\_path

vulnerable\_code\_not\_present

VEX Justifications: [https://www.cisa.gov/sites/default/files/publications/VEX\\_Status\\_Justification\\_Jun22.pdf](https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf)



# Stakeholder-Specific Vulnerability Categorization (SSVC)



## **CISA Stakeholder-Specific Vulnerability Categorization Guide**

# SSVC Calculator

Dryad - SSVC Calc App (CISA Coordinator v2.0.3)

[Start Decision](#) [Clear All](#) [Show Full Tree](#)





<https://www.first.org/epss>

# Q&A