



# **Chapter 1.Introduction to Ethical Hacking LAB**

# Chapter 1. Sections and sectors

- **1.1 Introduction to Ethical Hacking**
  - Explain the characteristics and value of Ethical Hacking.
    - Define Ethical Hacking.
    - Explain why Ethical Hacking is profitable to hackers.
- **1.2 Kali Linux,**
  - Explain the characteristics and value of Kali Linux OS.
    - Describe Kali Linux OS.
    - Describe the impact of a security breach.
- **1.3 Burp Suite**
  - Explain Burp Suite for cybersecurity professionals.
    - Describe the characteristics of the Burp Suite application.
- **1.4 Penetration Tester . Who are they?**
  - What Does a Penetration Tester Do?

## 1.1 Introduction to Ethical Hacking

# What will you learn?

- ▶ Throughout this course, you will learn the importance of hacking ethically and practice using tools and techniques to identify vulnerabilities within a system.

After this course, you will be able to:

- ▶ Explain what Ethical Hacking is.
- ▶ Explain the different types of hackers.
- ▶ Explain the importance of hacking ethically.
- ▶ Use tools, technologies, and techniques to identify vulnerabilities within a system.

## 1.1 Introduction to Ethical Hacking

### What will you do?

- ▶ In this course, you will have demos that will allow you to practice being an ethical hacker. Here is a preview of the demos featured in this course:

### Intro To Bug Hunting

- ▶ In this demo, you learn and practice the process of hacking and bug hunting.

### Demo: Network Enumeration

- ▶ In this demo, you learn and practice network enumeration using Nmap, a free and open-source tool for network discovery and security auditing.

### Demo: Vulnerability Analysis & Exploitation

- ▶ In this demo, you will be ensuring that a system is free and protected from vulnerabilities.

### Demo: Packet Sniffing

- ▶ In this demo, you will view and log packets of data sent over a network for analysis.

# Definition

## Ethical hacking

- ▶ Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

# What is an ethical hacker?

- ▶ Also known as “white hats,” ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

## 1.1 Introduction to Ethical Hacking

# What are the key concepts of ethical hacking?

- ▶ Hacking experts follow four key protocol concepts:
  1. **Stay legal.** Obtain proper approval before accessing and performing a security assessment.
  2. **Define the scope.** Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
  3. **Report vulnerabilities.** Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
  4. **Respect data sensitivity.** Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

## 1.1 Introduction to Ethical Hacking

# How are ethical hackers different than malicious hackers?

- ▶ Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.
- ▶ An ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-test to ensure the vulnerabilities are fully resolved.
- ▶ Malicious hackers intend to gain unauthorized access to a resource (the more sensitive the better) for financial gain or personal recognition. Some malicious hackers deface websites or crash backend servers for fun, reputation damage, or to cause financial loss. The methods used and vulnerabilities found remain unreported. They aren't concerned with improving the organizations security posture.



## 1.1 Introduction to Ethical Hacking

# What skills and certifications should an ethical hacker obtain?

- An ethical hacker should have a wide range of computer skills. They often specialize, becoming subject matter experts (SME) on a particular area within the ethical hacking domain.
- All ethical hackers should have:
  - Expertise in scripting languages.
  - Proficiency in operating systems.
  - A thorough knowledge of networking.
  - A solid foundation in the principles of information security.
- Some of the most well-known and acquired certifications include:
  - [EC Council: Certified Ethical Hacking Certification](#)
  - [Offensive Security Certified Professional \(OSCP\) Certification](#)
  - [CompTIA Security+](#)
  - [Cisco's CCNA Security](#)
  - [SANS GIAC](#)
-

## 1.1 Introduction to Ethical Hacking

# What problems does hacking identify?

- ▶ While assessing the security of an organization's IT asset(s), ethical hacking aims to mimic an attacker. In doing so, they look for attack vectors against the target. The initial goal is to perform reconnaissance, gaining as much information as possible.
- ▶ Once the ethical hacker gathers enough information, they use it to look for vulnerabilities against the asset. They perform this assessment with a combination of automated and manual testing. Even sophisticated systems may have complex countermeasure technologies which may be vulnerable.
- ▶ They don't stop at uncovering vulnerabilities. Ethical hackers use exploits against the vulnerabilities to prove how a malicious attacker could exploit it.
- ▶ Some of the most common vulnerabilities discovered by ethical hackers include:
  - Injection attacks
  - Broken authentication
  - Security misconfigurations
  - Use of components with known vulnerabilities
  - Sensitive data exposure
- ▶ After the testing period, ethical hackers prepare a detailed report. This documentation includes steps to compromise the discovered vulnerabilities and steps to patch or mitigate them.

# What are some limitations of ethical hacking?

- **Limited scope.** Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it's not unreasonable to discuss out of scope attack potential with the organization.
- **Resource constraints.** Malicious hackers don't have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.
- **Restricted methods.** Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).

# Kali Linux



**Kali Linux** is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

## 1.2 Kali Linux

Kali Linux is not about its tools, nor the operating system. Kali Linux is a **platform**.

### Make Your Job Easier

You can take any Linux and install pentesting tools on it, but you have to set the tools up manually and configure them. Kali is optimized to reduce the amount of work, so a [professional](#) can just sit down and go.

### Kali Everywhere

A version of Kali is always close to you, no matter where you need it. Mobile devices, Containers, ARM, Cloud providers, Windows Subsystem for Linux, Pre-built Virtual Machine, Installer Images, and others are all [available](#).

### Customization

With the use of [metapackages](#), optimized for the specific tasks of a security professional, and a highly accessible and well documented [ISO customization process](#), it's always easy to generate an optimized version of Kali for your specific needs.

### Documentation

Whether you are a seasoned veteran or a novice, our [documentation](#) will have all the information you will need to know about Kali Linux. Multiple tips and “recipes” are available, to help ease doubts or address any issues. All documentation is open, so you can easily contribute.

### Community

Kali Linux, with its [BackTrack](#) lineage, has a vibrant and [active community](#). There are active Kali forums, IRC Channel, Kali Tools listings, an open bug tracker system, and even community provided tool suggestions.

# What is Kali Linux?

- ▶ Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

# Kali Linux History

- ▶ Kali Linux is based on years of knowledge and experience of building a pentest testing Operating Systems, which has spanned over multiple previous projects. During all these project's life-time, there has been only a few different developers, as [the team](#) has always been small. As a result, Kali has been years in the making and has come a long way.
- ▶ The first project was called **Whoppix**, which stood for **WhiteHat Knoppix**. As can be inferred from the name, it was based on Knoppix for the underlining OS. Whoppix had releases ranging from v2.0 to v2.7.
- ▶ This made way for the next project, **WHAX** (or the long hand, **WhiteHat Slax**). The name change was because the base OS changed from Knoppix to Slax. WHAX started at v3, as a nod towards it carrying on from Whoppix.
- ▶ There was a similar OS being produced at the same time, **Auditor Security Collection** (often getting shorted to just **Auditor**), once again using Knoppix, and efforts were combined (with WHAX) to produce [BackTrack](#). BackTrack was based on Slackware from v1 to v3, but switched to Ubuntu later on with v4 to v5.
- ▶ Using the experience gained from all of this, **Kali Linux** came after BackTrack in [2013](#). Kali started off using Debian stable as the engine under the hood before moving to [Debian](#) testing when Kali became a rolling OS.

# Kali linux Features

- **More than 600 penetration testing tools included:** After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either simply did not work or which duplicated other tools that provided the same or similar functionality. Details on what's included are on the [Kali Tools](#) site.
- **Free (as in beer) and always will be:** Kali Linux, like BackTrack, is [completely free](#) of charge and always will be. You will never, ever have to pay for Kali Linux.
- **Open source Git tree:** We are committed to the open source development model and our [development tree](#) is available for all to see. All of the source code which goes into Kali Linux is available for anyone who wants to tweak or rebuild [packages](#) to suit their specific needs.
- **FHS compliant:** Kali adheres to the [Filesystem Hierarchy Standard](#), allowing Linux users to easily locate binaries, support files, libraries, etc.
- **Wide-ranging wireless device support:** A regular sticking point with Linux distributions has been support for wireless interfaces. We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.



# Kali linux Features (cont.)

- **Custom kernel, patched for injection:** As penetration testers, the development team often needs to do wireless assessments, so our kernel has the latest injection patches included.
- **Developed in a secure environment:** The [Kali Linux team](#) is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.
- **GPG signed packages and repositories:** Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.
- **Multi-language support:** Although penetration tools tend to be written in English, we have ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
- **Completely customizable:** We thoroughly understand that not everyone will agree with our design decisions, so we have made it as easy as possible for our more adventurous users to [customize Kali Linux](#) to their liking, all the way down to the kernel.
- **ARMEL and ARMHF support:** Since ARM-based single-board systems like the [Raspberry Pi](#) and [BeagleBone Black](#), among others, are becoming more and more prevalent and inexpensive, we knew that [Kali's ARM support](#) would need to be as robust as we could manage, with fully working installations for both [ARMEL and ARMHF](#) systems.

# What's different about Kali Linux?

- ▶ Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflect these needs:
- 1. **Network services disabled by default:** Kali Linux contains systemd hooks that disable network services by default. These hooks allow us to install various services on Kali Linux, while ensuring that our distribution remains secure by default, no matter what packages are installed. Additional services such as Bluetooth are also blocklisted by default.
- 2. **Custom Linux kernel:** Kali Linux uses an upstream kernel, patched for wireless injection.
- 3. **A minimal and trusted set of repositories:** given the aims and goals of Kali Linux, maintaining the integrity of the system as a whole is absolutely key. With that goal in mind, the set of upstream software sources which Kali uses is kept to an absolute minimum. Many new Kali users are tempted to add additional repositories to their **sources.list**, but doing so runs a *very serious risk* of breaking your Kali Linux installation.

# Summary

- So, after having read this you should have figured out if **Kali Linux** is the distribution you were looking for or at least got an idea about your choice.
- If still you have not figured it out, here is a summary that will hopefully remove your remaining doubts:
  - Kali Linux is made with **pentesters** and **pentesting** in mind so, expecting it to fit with your necessity *might* not be as simple even though it's completely possible.
  - If you are new to **Linux** or have less experience with **command line** you might find Kali Linux to be not so user-friendly, even though our developers try to make it as user-friendly as possible some things might be intimidating to you if you are new.
  - The developers always try to make Kali Linux as much hardware compatible as possible but, still some hardware/s *might not work as expected or not work at all*. So, its better to **research hardware compatibility** beforehand rather than breaking your computer later.
  - If you are installing Kali Linux for the first time, it is recommended to install first in Virtual Machine then, after getting familiar with it, you can install it in your own hardware.

## 1.2 Kali Linux

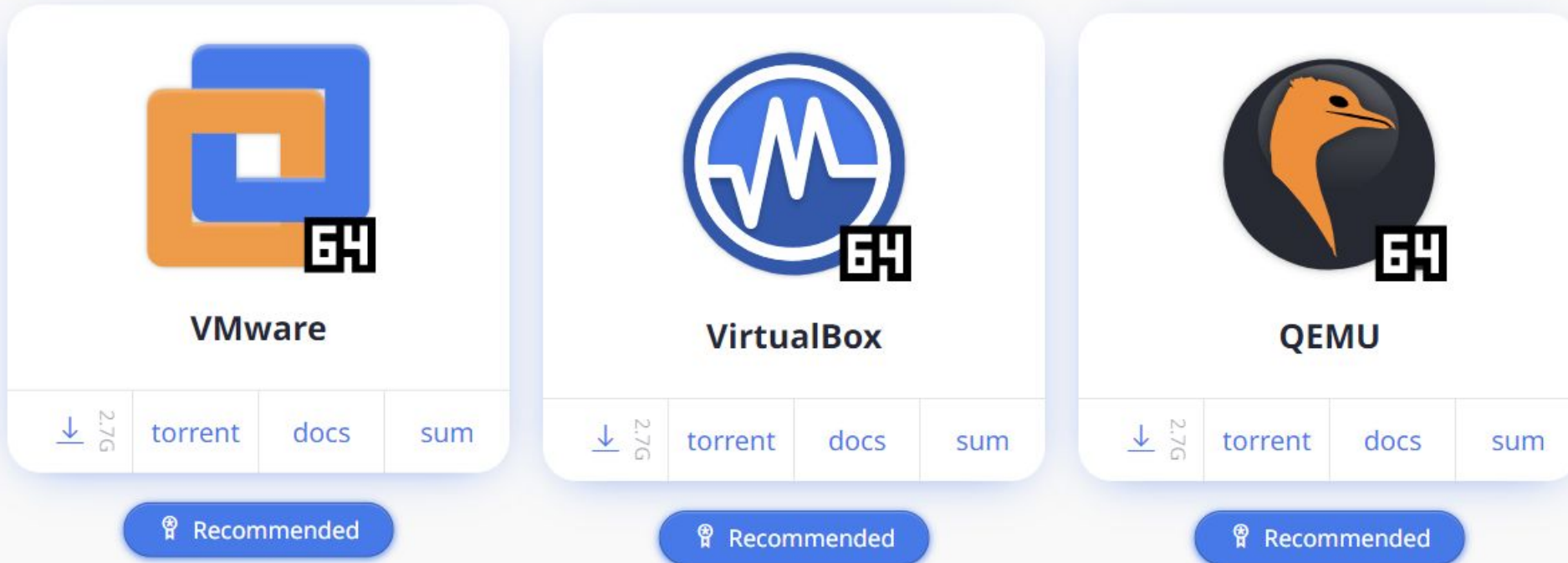
# Installation Kali Linux

- Kali is a rolling Linux distribution, meaning as soon as we have an update, we ship it. Would-be users have a variety of images to choose from.



# Virtualization Kali Linux

- Kali Linux [VMware](#) & [VirtualBox](#) images are available for users who prefer, or whose specific needs require a virtual machine installation.



# Kali ARM History

- ▶ When [BackTrack ARM](#) first came out, it was one image, for a Motorola Xoom. The work was done on the Xoom itself by [@muts](#). He started from an Ubuntu image for it, built all of the packages for BackTrack on it, then installed them. [@steev](#) then took the work and expanded it to support 3 or 4 different ARM devices he had, following a similar procedure. @steev showed @muts the work he'd done and @muts was as excited about it as @steev was.
- ▶ When Kali came about, we retooled everything, including build servers for armel, armhf, and arm64. No more building packages manually on the ARM devices themselves. So everything was in place, but the images for ARM devices were still being built manually. Putting out an updated image meant downloading the last release, writing it to an sdcard, booting the device, running updates, building the kernel, installing the new kernel, cleaning up the logs and apt cache, then powering the system off, plugging the sdcard back into my other system, and creating a dd image of the sdcard, putting it on to a server. This was very error prone due to the nature of sd cards from different manufacturers having different actual sizes.
- ▶ We wanted to make it so anyone could, starting from a Kali amd64 installation, build an image that would work on any of our supported ARM devices, end up with exactly what we put out, and most importantly, customize it for their needs. So we created the [kali-arm build scripts](#) - they are not fancy, but they're easy to read, follow and modify.



# Kali NetHunter History

- ▶ Kali NetHunter is a custom OS for Android devices. This takes Kali Linux desktop and makes it mobile.
- ▶ Kali NetHunter is made up of three parts:
  - ROM
  - App (and AppStore)
  - Kali Chroot
- ▶ Kali NetHunter was first released in September 2014 with v1.0, supporting just Nexus devices (5,7 and 10). There was a minor release of Kali NetHunter v1.1 in January 2015, and at the same time device support started to appear, such as OnePlus One and Nexus 4.
- ▶ Kali NetHunter v3 was the next major release in January 2016, which was a complete NetHunter app rewrite, allowing for more control and actions to be performed from it, build scripts and Android 5 and 6 support. Nexus 6 device also became supported.
- ▶ Kali NetHunter then joined the **rolling release** with 2019.2 release in May 2019, where 13 devices were supported, with a mixture of Android 4 to 9. From this point, Kali NetHunter matched the release points of Kali Linux, with each of them adding more devices support, image and overall features.



## 1.3 Burp Suite

Burp Suite is an integrated platform and graphical tool for performing security testing of web applications, it supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

### Burp Suite Enterprise Edition

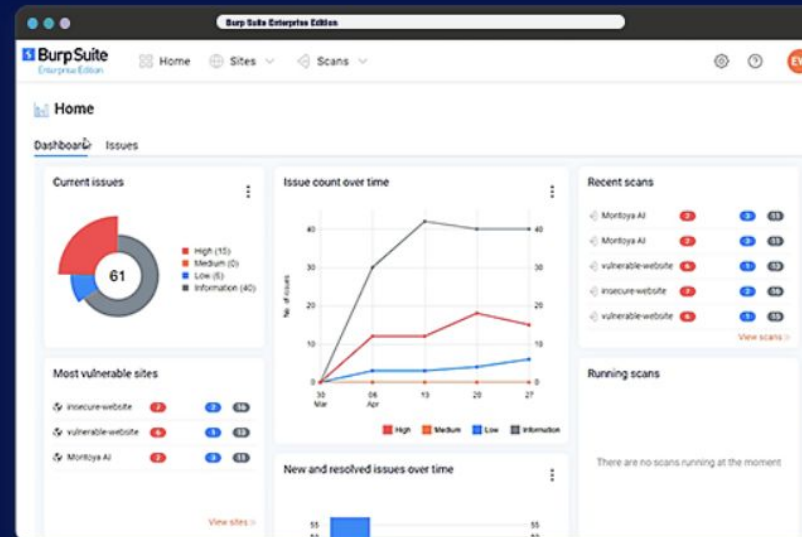
**More secure  
shouldn't mean  
less agile**

Scan it all. With the enterprise-enabled  
dynamic web vulnerability scanner.

TRY FOR FREE

PRICING AND PLANS

Got a question? [Contact us →](#)



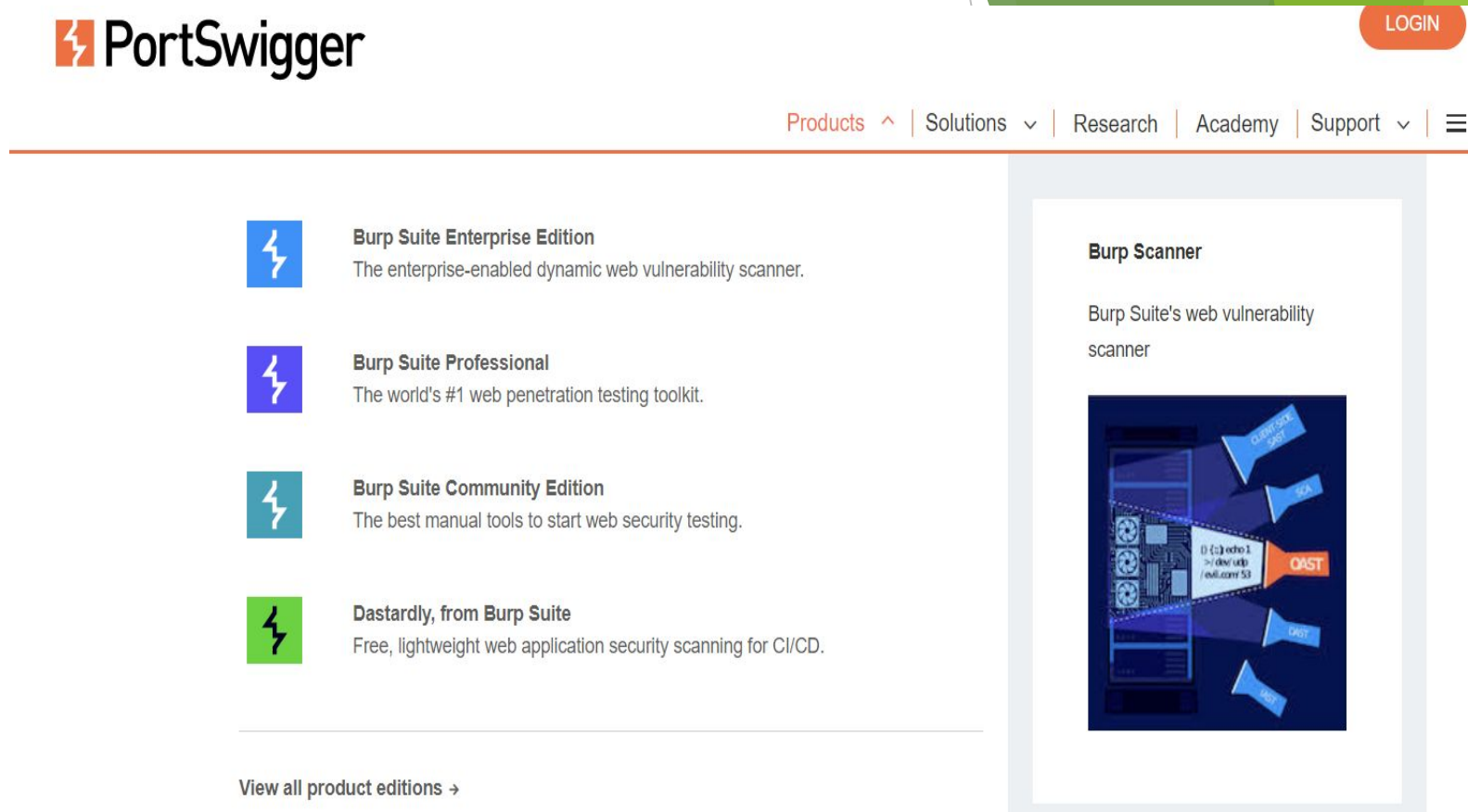
[Live demo →](#)

<https://portswigger.net/burp/enterprise>



## 1.3 Burp Suite

- ▶ The tool is written in Java and developed by PortSwigger Web Security.
- ▶ The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. The Community edition has significantly reduced functionality.
- ▶ It intends to provide a comprehensive solution for web application security checks.



The screenshot displays the PortSwigger website's product page. At the top, the PortSwigger logo is on the left, and a 'LOGIN' button is on the right. A navigation bar below the logo contains links for 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main content area lists four products, each with a lightning bolt icon and a description:

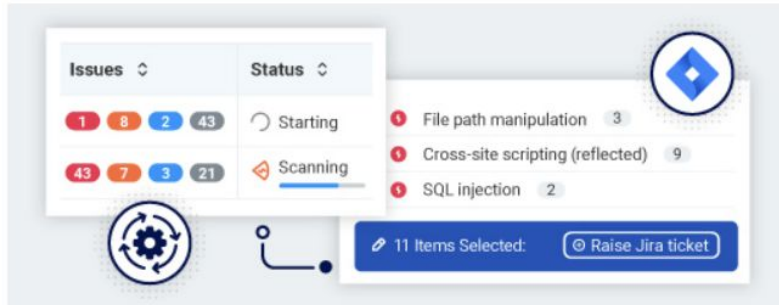
- Burp Suite Enterprise Edition**: The enterprise-enabled dynamic web vulnerability scanner.
- Burp Suite Professional**: The world's #1 web penetration testing toolkit.
- Burp Suite Community Edition**: The best manual tools to start web security testing.
- Dastardly, from Burp Suite**: Free, lightweight web application security scanning for CI/CD.

At the bottom of the product list is a link: 'View all product editions →'. On the right side of the page, there is a highlighted box for 'Burp Scanner', which includes the text 'Burp Suite's web vulnerability scanner' and an image of the scanner's interface showing various tool icons and a terminal window with the command 'D {c} echo 1' and its output '1'.

## 1.3 Burp Suite

# What do you want to do with Burp Suite?

### Automated dynamic scanning



Secure your whole web portfolio, integrate security with development, and free time for AppSec to do more - with automated dynamic scanning.

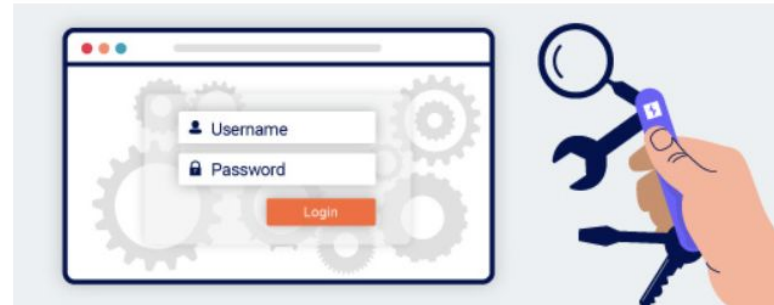
 **Burp Suite Enterprise Edition →**

The enterprise-enabled dynamic web vulnerability scanner.

 **Dastardly, from Burp Suite →**

Free, lightweight web application security scanning for CI/CD.

### Enhanced manual testing



Find more vulnerabilities faster, and be part of the world's largest web security community - with the dynamic testing toolkit designed and used by the industry's best.

 **Burp Suite Professional →**

The world's number one penetration testing toolkit.

 **Burp Suite Community Edition →**

The best manual tools to start web security testing.

# Burp Suite Features



Secure your whole  
web portfolio



Integrate security  
with development



Free time for  
AppSec to do more



## 1.3 Burp Suite

# Burp Suite Features

### Deploy with ease, report with simplicity

Perform recurring dynamic scans across thousands of applications. Point and click; all you need is a URL.

### Achieve full visibility of your enterprise security posture

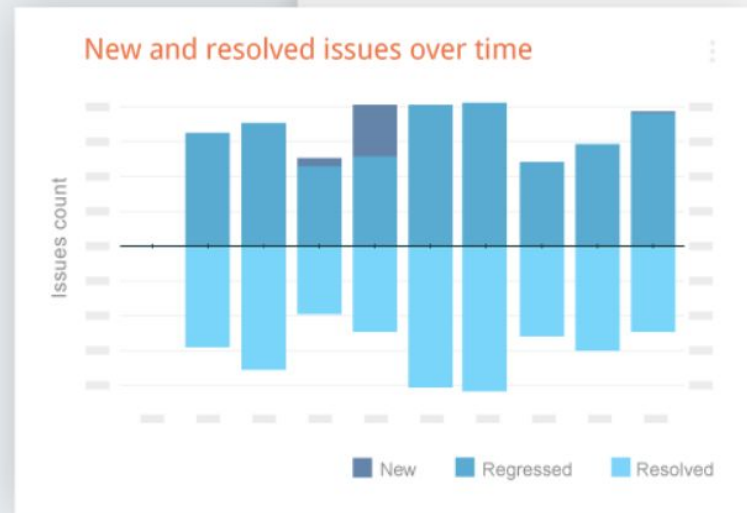
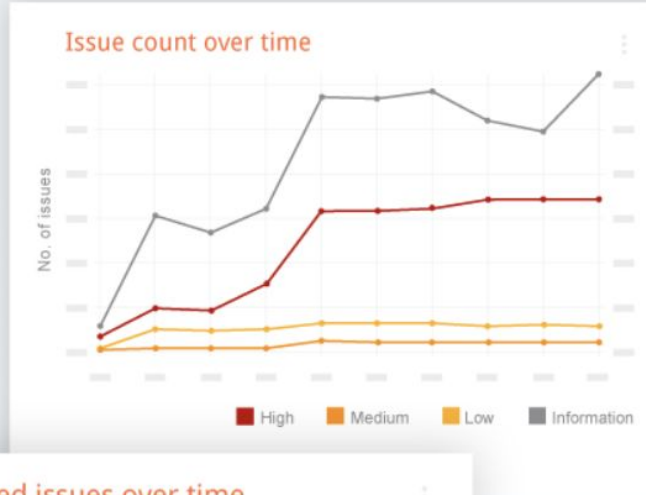
Intuitive security reporting dashboards, role-based access control, and scan reports by email.

### Empower DevSecOps

Out-of-the-box integration with ready-made CI plugins, native Jira support, and a rich API, to easily incorporate security within your existing software development processes.

### Reduce risk without increasing costs

A pricing model that allows you to scan at scale across thousands of applications, for maximum ROI with no strings attached.



# Burp Suite Features



**Powered by Burp Suite technology trusted at over 16,000 organizations worldwide**





# History of Penetration Testers

In the 1960s, computer systems became capable of exchanging data across communication networks. Security experts quickly realized these data exchanges were vulnerable to external attacks.

The increasing role of computers in government and business made it necessary to create effective safeguards.

In 1967, more than 15,000 computing experts and public and private sector officials met at the Joint Computer Conference. They discussed the issue of network penetration, a concept that would become known as penetration testing.

Early efforts by the RAND Corporation helped create a systematic approach to penetration testing. Advanced computer security systems like the Multiplexed Information and Computing Service (Multics) then emerged. Multics functioned as the industry's gold standard until about 2000.

Since that time, penetration testing has become increasingly complex and specialized. Today, pen testers draw on various advanced tools to identify and close off system vulnerabilities. Penetration testing has also become a big business, with 2021 estimates placing the value of the global cybersecurity industry at \$217.9 billion.

# The Importance of Pentesters:

- ▶ Pentesters are becoming increasingly relevant in the modern world. This is primarily because the average cost of a data breach has reached an all-time high (\$3.86 million), and companies know that they can no longer take cybersecurity lightly. It seems more prudent and cost-effective to hire a consultant for thousands, than to incur millions in losses, after being compromised.



# Resources for Penetration Testers

- » **Information Systems Security Association International:** This collaborative professional network unites cybersecurity professionals worldwide through training programs, workshops, and career services. ISSA also maintains a fellows program for ambitious professionals.
- » **(ISC)2:** This leading nonprofit cybersecurity organization features a membership base of more than 150,000 professionals. It offers respected certifications, exam preparation resources, career services, and many other perks.
- » **Comp-TIA:** Another respected global leader in cybersecurity, the Comp-TIA organization offers specialized training programs, continuing education, and certifications. Members also gain access to an exclusive career center.
- » **ISACA:** This enterprise-oriented organization offers benefits including members-only career fairs and job boards, international conferences, and more than 200 local chapters that host training workshops and events. ISACA offers student, recent graduate, and professional membership levels.

# What Kind of Vulnerabilities does a Pentester look for?

- ▶ There can be many different kinds of vulnerabilities within a system; including missing data encryption, OS command injection, SQL injection, missing authentication, missing authorization, reliance on untrusted inputs, buffer and stack overflows, etc. Depending on the level of freedom that the company gives to the pentester, the type and number of scanned and exploited vulnerabilities can differ. If there are no limits imposed by the client, a pentester has the liberty to go to any lengths; from performing a social engineering attack, to using a Wi-Fi sniffer, to making a denial-of-service attack.

## 1.4 Pentester

# What Kind of Vulnerabilities does a Pentester look for?

**Pentest-Tools**
7879 Credits
TOOLS +
FEATURES
PRICING
SERVICES
LEARN +
CAREERS +

My Scans ▾ | New Scan | Rescan | Current workspace: New workspace ▾

- Dashboard
- Workspaces
- Targets
- Scans
- Findings
- Reporting ▾
- Scheduler
- Admin panel

## Website Vulnerability Scanner Result

http://testing1.pentest-tools.com/dwva/

**Summary**

Overall risk level:

**High**

Risk ratings	Count
High	5
Medium	3
Low	2
Info	8

**Scan information:**

Start time: 2023-06-24 08:07:56  
 Finish time: 2023-06-24 09:11:22  
 Scan duration: 2 min, 36 sec  
 Tests performed: 18/20  
 Scan status: Finished

### Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-7958	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4.23
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4.23
●	7.2	CVE-2019-3211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non Unix systems are not affected.	N/A	http_server 2.4.23

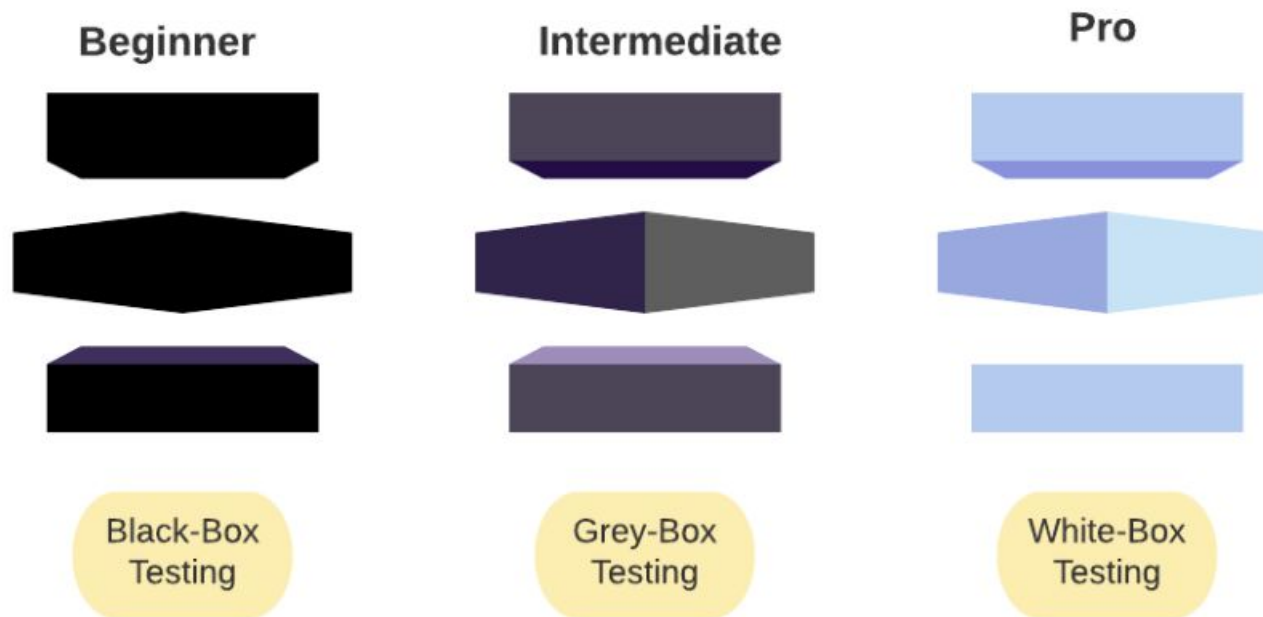
[Details](#)

### Cross-Site Scripting

Vulnerable Page	Vulnerable Parameter	Method	Attack Vector
/showlogin.php	username	POST	http://testing1.pentest-tools.com/dwva/login.php POST Data: username=<(script></script>)<script>-</script>
/dwva/vulnerabilities/bnuto/	username	GET	http://testing1.pentest-tools.com/dwva/vulnerabilities/bnuto/Login?Login&password=ZAP&username=%27%22%3Cscript%3Ealert%281%20%3B%3C%2Fscript%3E
/dwva/vulnerabilities/sql/	id	SQL	http://testing1.pentest-tools.com/dwva/vulnerabilities/sql/?Submit=Submit&id=427%22%3Cscript%3Ealert%281%20%3B%3C%2Fscript%3E
/dwva/vulnerabilities/xss_r/	name	GET	http://testing1.pentest-tools.com/dwva/vulnerabilities/xss_r/?name=%3C%2Fpre%3E%3Cscript%3Ealert%281%20%3B%3C%2Fscript%3E%3Cpre%3E

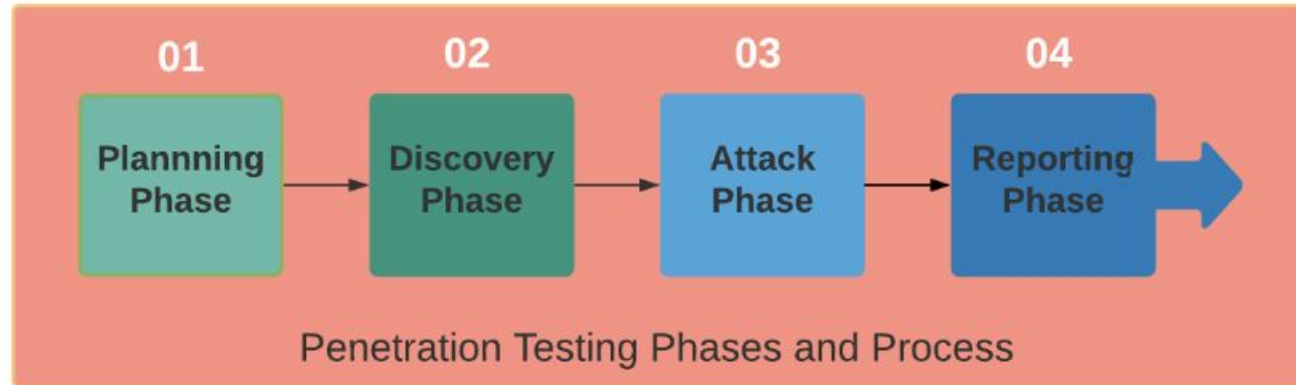
# Types of Penetration Testing

- There are three main types of penetration testing: *Black box testing*, *white box testing*, and *grey-box testing*. Which one you should choose typically depends on the extent of information you are willing to share with the pentester. Let's take a look at all three in more detail:



# Stages of Penetration Testing

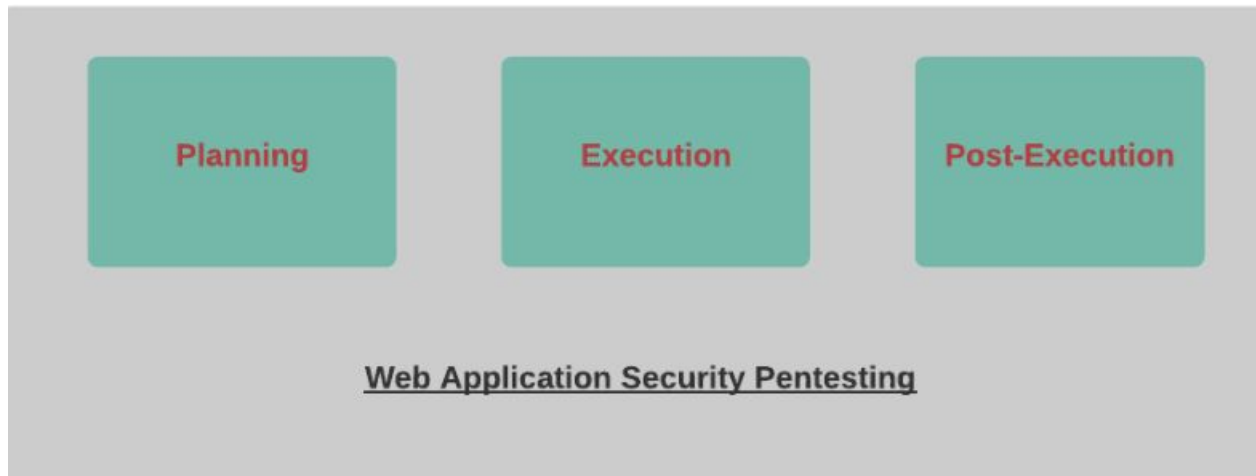
There are four main stages of any penetration testing effort



- **Planning:** Scope and strategy of the project is decided and documented.
- **Discovery:** At this stage, the pentester scans the system rigorously and repeatedly to find any useful information, like usernames, passwords, encryption keys, etc. This process is also known as fingerprinting. These days, a lot of fingerprinting tools are used for this purpose, e.g. [BlindElephant](#) and [Wappalyzer](#). In addition to this, the pentester also identifies any potential vulnerabilities during this stage.
- **Attack:** The pentester simulates a bunch of relevant attacks on the system during this stage.
- **Reporting:** Finally, audit reports are compiled, documenting security flaws and suggestions that can help revamp system security.

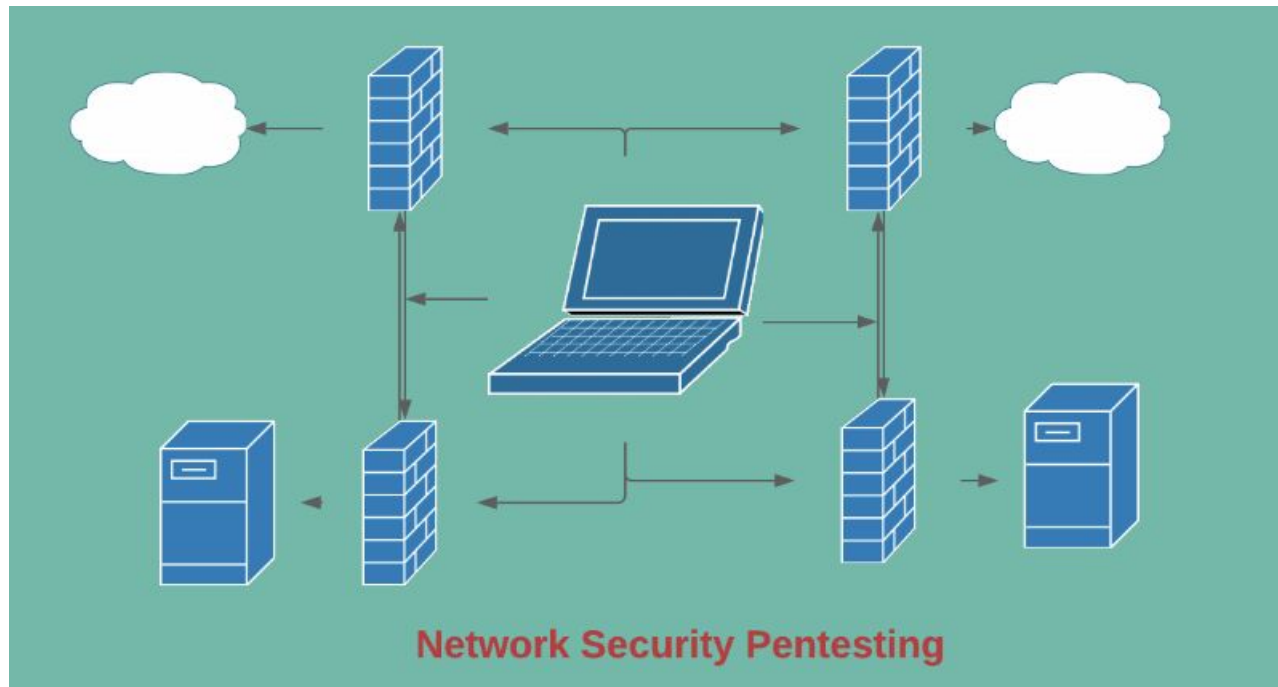
# How to Become a Pentester

- ▶ **Web App Security Pentesting:** As most of our software and applications became versatile and can be accessed via a browser, becoming an expert in web app security can be a great start. We may think companies on the internet are secure. Let me tell you, they are not. Nothing is 100% secure. We are not influencing to crackdown sites and services but giving hope that it is possible to gain the skillset.



# How to Become a Pentester

- **Network Security Pentesting:** A network security specialist or pentester has the task to figure out network access and weakness even if it is secure. Companies and industrial networks constantly need to figure out loopholes and ways to fix them. Carrying out a network pen-testing is a bit different from web app pentesting, as the pentester needs to listen to a spoofed network protocol and act accordingly.





# How to Become a Pentester

- **Script Scrambling for Pentesting:** Getting hands-on a script or code, a **pentester** should be able to read it like a book and find the errors like grammatical mistakes. As a beginner, it's not going to work like that. So, we need practice. Reviewing codes in C, C++, JavaScript, Python, and other languages should become an instinct regarding the target platform.

```
Executable File | 140 lines (105 sloc) | 3.04 KB
```

```
#!/usr/bin/python3  
  
# I don't believe in license.  
# You can do whatever you want with this program.  
  
import os  
import sys  
import socket  
import argparse  
from colored import fg, bg, attr  
from threading import Thread  
from queue import Queue  
from multiprocessing.dummy import Pool  
  
def banner():  
    print("""  
          _  
   --_--_--_|_|_--_--      -_-_-_-_  
| / \ v _/_\_/ \ \ \ // \_\_ |' \ \ ||| | | |
|| | _/\ \ \ \_) |\ \//\_ \| ) | | | |  
| | \ ||_/\_/_|\_/ \ \ \ \_) |./ \_|  
                                     |_| |_/  

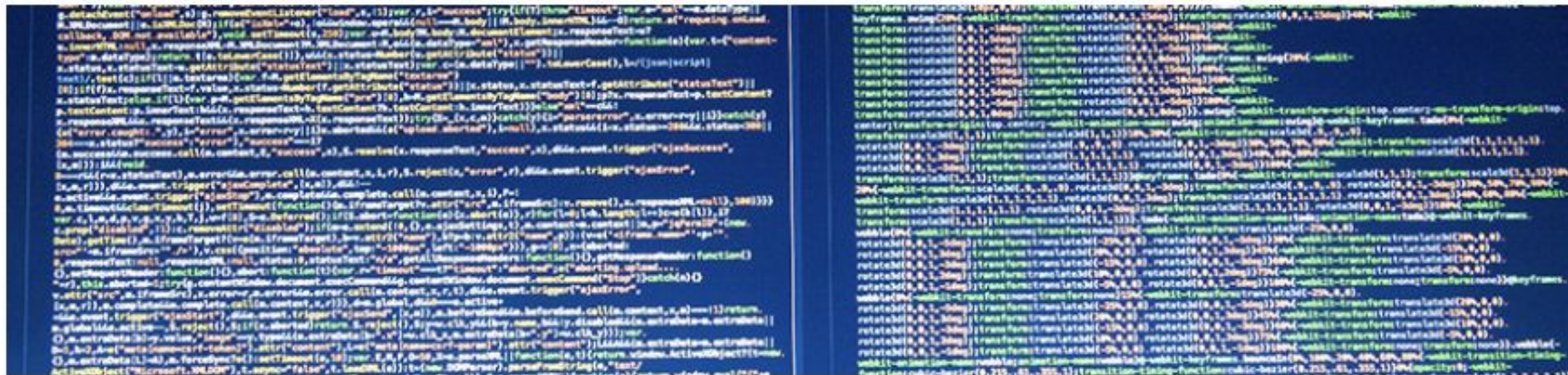
```



## 1.4 Pentester

# How to Become a Pentester

- **Physical/Hardware Pentesting:** Sometimes pen testing requires taking a physical device apart and trying to scope out ways to pentest. Electronic devices have many architectures (like ARM) and a pentester should be familiar with its work methodology. Also, SPI, FPGA, UART, JTAG are great tools to tweak. Architecture like x64 and x86, flash memory alongside connected scripts help understand embedded or hardware devices pen-testing.



## 1.4 Pentester

# Similar Specializations and Career Paths

DESCRIPTION	REQUIRED EDUCATION	REQUIRED EXPERIENCE	MEDIAN ANNUAL SALARY (2021)	
<b>Information Security Analyst</b>	Security analysts plan and implement strategies to protect their employer's computers and networks from intrusions and attacks.	Bachelor's degree or higher in computer science, computer programming, information technology, or cybersecurity  Some companies prefer candidates with specialized MBAs in information systems	Multiple years in a related position, such as database security or systems administration	\$102,600
<b>Security Software Developer</b>	These professionals specialize in developing software-based tools for enhancing organizational computer and network security.	Bachelor's degree or higher in computer science, software development, information technology, computer engineering, or mathematics	Previous experience in quality assurance (QA) testing or a related position may be an asset	\$109,020
<b>Security Architect</b>	Computer network architects design, implement, and monitor the security features used in communication network infrastructure.	Bachelor's degree or higher in computer science, computer engineering, or a specialized information systems discipline	5-10 years in IT roles such as systems analysis or database administration	\$120,520

# Summary

**Penetration testing has also become a big business, with 2021 estimates placing the value of the global cybersecurity industry at \$217.9 billion.**

An experienced pentester can help a company in identifying vulnerabilities that can otherwise cause a lot of reputational and financial damage. Regardless of whether you want to simulate an insider attack, or one made by an experienced external hacker, a pentester can do the job for you!