Top 30 Best Penetration Testing Tools – 2023

By **Cyber Security News Team** - April 15, 2023

In this article, security experts from **Cyber security News** have extensively researched and listed the top 30 best penetration testing tools.

When we talk about penetration Testing, we all know very well that the first thing that comes to mind is the threat.

These tools allow penetration testers to perform **scans, reconnaissance, information gathering, analysis, and exploit** the network and suggest a fix to secure it from cyberattack.

When you are reading this article, it is clear that you want to know about Penetration testing.

This is simulated with a cyber-attack where ethical hackers who are professionals search for the flaws in the corporate network and break this before the attacker break.

This is like the movie Sneakers, where hacker consultants break the corporate network and find the weakness.

This is similar to a **simulated cyber-attack** where ethical hackers use the tool and technique that malicious hackles can use.

This shows you how malicious attackers can hack your network; it also gives you an idea so that before they do anything, you implement that and make your business safe.

Basically, you will mitigate the weakness before the attacker comes to know.

We all know very well that we use penetration testing software to **recognize security vulnerabilities in a network, server, or web application.**

Generally, all these tools are very beneficial since they enable you to distinguish the "**unknown weakness**" in the software and in any networking applications that can create a security break or whole.

Hence, **(Vulnerability Assessment and Penetration Testing) VAPT Tools** strike your system inside the network and outside the web as if a hacker would strike it.

If unauthorized access is conceivable, the system undoubtedly has to be changed.

While apart from these things, **common thing penetration testing is used by companies** simply because it is one of the best procedures for companies and individuals to defend against cyber-attacks.

In the old days, hacking was very difficult to recognize and perform because it required a lot of manual bits fiddling.

According to the research, every company has its weaknesses, and attackers can exploit them.

Every company has a 93% chance that an attacker with the attack, but this tool will not allow them to attack. More than 71% of the company's unskilled hackers penetrate the internal network.

But today, it is quite possible because of these pentesting tools. Well, we can say that there is no doubt now that the threat aspect is regularly growing.

You must use penetration software to make the attacker fail and find the solution as a businessman.

Here you will get the **online security professional tool** list which helps you to find the loopholes and exploit the target.

Thus as we mentioned above that, it is one of the best methods, especially for businesses and corporations, to **protect themselves with the help of Penetration Testing or Pen Testing.**

Hence, this article will overview Pen Testing, its benefits, and the most commonly used tools today.

However, apart from all these things, **there is still a lot of confusion in the industry concerning the differentiation between vulnerability scanning and penetration testing;** these phrases are usually interchanged applications.

But the fact is that both their purposes and implications are quite different.

Hence if we talk about the vulnerability assessment, it directly classifies and reports noted weaknesses. On the other hand, a penetration or pen test tries to utilize the vulnerabilities to decide whether unauthorized access or other malicious exercise is conceivable.

Thus **Penetration testing generally comprises network penetration testing and application security testing** as well as directs and processes nearby the networks and applications and should occur from both outside and inside the network that is trying to come in.

Penetration Testing is now an integral part of every major security strategy due to the increasing frequency and severity of cyberattacks.

Some people may find the concept difficult to grasp if they are unfamiliar with the term.

Therefore, we have made an effort to describe the process and tools of Penetration Testing in this post. Those interested in learning more are encouraged to keep reading.

What are you going to learn Penetration Testing Tools article?

What is Penetration Testing?

> **Penetration testing also called pentesing or security testing**, is a method of simulating the attack by scanning, testing, and identifying the vulnerability in the authorized computer **system or network to prevent it by patching the vulnerability system.**

Penetration testing is automated by the Penetration Testing Tools, which is generally used to identify weak spots so that they can be cured with the help of these tools.

We can also say that Penetration testing tools are utilized as a part of a penetration test or pen test to automatize some specific tasks, develop testing productivity, and explore issues that might be challenging to find using manual analysis methods alone.

The two essential penetration testing tools are static analysis tools and dynamic analysis tools.

Moreover, for example, let us take Veracode, which performs both dynamic and static code analysis and finds different security weaknesses, including wicked code and the loss of functionality that may lead to security breaks.

For a better understanding, we can say it's like in the movies, where hacker consultants burst into your operating networks to find vulnerabilities before attackers do.

Thus it's a hidden cyber-attack where the pentester or decent hacker uses the tools and methods accessible to disclose the ill-disposed hackers.

> **Penetration Testing, also known as "Pentesting", is a form of security testing in which a professional "Ethical Hacker" or "Penetration Tester" simulates a cyber attack on a computer system or network to find vulnerabilities and flaws in the system before a malicious hacker can take advantage of them.**

Penetration Testing aims to discover and fix vulnerabilities before malicious hackers or bad cybercriminals exploit them.

Benefits of Penetration Testing

Penetration testing has numerous advantages. Among the most important are the following:

- **Maintaining compliance:** The Payment Card Industry Data Security Standard (**PCI DSS**) and the Health Insurance Portability and Accountability Act (**HIPAA**) are two laws and regulations requiring periodic penetration testing for many organizations.

- **Prevent cyberattacks:** Discovering vulnerabilities is a significant advantage of conducting a penetration test. This allows for fixing the issues before hackers use them.

- **Prevent expensive incidents:** The results of penetration tests can be used to strengthen a company's security measures. When businesses invest in regular penetration testing, they become less vulnerable to cyber attacks, ultimately saving them money.

- **Keeping cybersecurity experts up to date:** As a penetration tester, staying current on industry developments is crucial. Cybersecurity professionals can benefit from routine penetration testing because it keeps them abreast of new vulnerabilities and countermeasures.

What are the Skills needed for Penetration Tester?

The importance of Penetration Testing has only grown as cyber criminals have developed increasingly sophisticated methods of attacking organizational digital infrastructures, such as social engineering, ransomware, and others.

The first step in mounting an effective defense is honestly assessing the capabilities. A Penetration Tester requires the following skills:

- The fundamentals of networking (TCP/IP address, protocols)
- Expertise in learning and utilizing computer systems such as Windows, Linux, and macOS
- Understanding of different kinds of **penetration testing tools.**
- Knowledge of programming language
- Ability to convey ideas clearly and concisely in writing, especially in technical situations.

What are the Methods of Penetration Testing?

There are three main approaches for penetration testing, each of which depends on the depth of knowledge the tester has about the target system.

- **Black Box Penetration Testing**
- **White Box Penetration Testing**
- **Grey Box Penetration Testing**

Black Box Penetration Testing

- External penetration testing is another name for black box penetration testing.
- In this method, the pen tester needs to learn about the organization's IT infrastructure.
- This process seems more like an experiment of a real-world cyber threat to test the system's vulnerabilities.
- In this method, the pen testers pretend to be cyberattackers and try to exploit the device's vulnerabilities.
- This typically takes a long time and can take up to six weeks to finish.

White Box Penetration Testing

- Internal penetration testing, clear box, and even glass box penetration testing are other names for white box penetration testing.
- This penetration testing method gives the pen tester full access to the environment, source code, and IT infrastructure.
- It is a comprehensive and in-depth pen test examining every aspect, including the application's fundamental structure and code quality.
- Furthermore, completing this kind of pen-testing approach typically takes two to three weeks.

Grey Box Penetration Testing

- The pen tester has limited access to information about the target system's architecture and source code in this penetration testing method.
- Since the pen tester has limited information about the internal network or web application to work with, they can concentrate on finding and exploiting any vulnerabilities they find.

What all the Role of Coding in Penetration Testing?

Learning hacking techniques is necessary to improve one's penetration tester or cybersecurity analyst skills. If anyone is interested in understanding how penetration testers think, they need to acquire the same set of abilities they do.

While programming expertise is unnecessary to perform penetration tests, it can improve a tester's efficiency and effectiveness. A tester's success is not dependent on their familiarity with programming languages, but it is helpful.

> ***According to Ubuntu Pit, penetration testers utilize a wide range of cyber tools and programming languages to gain unauthorized access to networks or to reveal security vulnerabilities in specific pieces of software.***

The following are some of the languages for developing penetration testing software.

- **Python:** SQLMap, SimplyEmail, W3af, and Wfuzz
- **JavaScript:** Netsparker
- **C:** Hashcat, John the Ripper, Aircrack and Aircrack
- **Java:** Hydra, Xray, and ZAP
- **Ruby:** Metasploit

How to Perform Penetration Testing?

The penetration testing is performed in five phases which are:

- **Reconnaissance**
- **Scanning**
- **vulnerability assessment**
- **Exploitation**
- **Reporting**

Phase 1: Pre-engagement (planning and scoping)

Since every penetration test is different, the first step is always to establish the scope and objective of the test.

Everything about the procedure, including testing procedures, allowed systems, and more, is decided upon here.

The goals of each penetration test are established before the evaluation, and the tests are conducted accordingly.

Phase 2: Information gathering

During this phase, the penetration tester or Ethical Hacker collects as much data as possible about the target system. Similar terms include fingerprinting and reconnaissance.

Phase 3: Vulnerability Assessment

After gathering information about the target, the penetration tester assesses vulnerability to learn more about that system.

Knowing how the target application will respond to different attempts to get in is also helpful.

Ethical hackers or penetration testers use automated tools like **Nessus, and Rapid7**, for vulnerability assessment.

Phase 4: Exploitation

Penetration testers use their skills to attack and exploit target options to find security flaws.

They use techniques like cross-site scripting, SQL injection, social engineering, and security holes to get into the target and stay there.

It helps figure out what kind of damage a vulnerability could cause.

Phase 5: Post-exploitation

In this step, the Penetration Tester removes any malware, rootkits, codes, records, tools, etc., implanted or made during penetration testing.

They use their weaknesses to get what they want, including installing malware, changing it, or misusing its functions.

Phase 6: Reporting

This concludes the penetration testing phase. At this point, the penetration testers present their conclusions and suggestions for resolving security issues.

Organizations can use this information to strengthen their security.

What is the Role of Penetration Testing Tools?

Penetration testing tools are used to identify and test vulnerabilities in the system. Penetration testing tools enable authorized, ethical (white-hat) hacking of production-level applications.

These simulated cyberattacks by testers assist organizations in identifying vulnerabilities that hackers may exploit and determine the potential risk related to vulnerabilities. **Penetration testing tools** are used in different ways, including:

- Forensic and anti-forensics
- Gathering information and exploitation
- Password and wireless attacks
- Web applications and shells
- Surface-level vulnerabilities
- Reverse engineering

When do you need to do Penetration Testing?

Theoretically, all software and devices should be examined with reference to being used in manufacturing.

Therefore, penetration testing should typically be performed just before a system is put into manufacturing once it is no longer undergoing continuous development.

Additionally, frequent penetration testing should be conducted at least once a year.

Why are Penetration Testing Tools Essential?

Well, after knowing what Penetration Testing Tools are all about, some of you might be thinking about why these penetration tools are essential.

As we discussed above, these tools are used to find the weak points and areas to help you overcome those attacks.

Thus, these Best Penetration Testing Tools are used by companies and organizations so that they can protect their operating system through these tools and stop hackers from those who are stealing their companies' private information.

Testers generally perform these penetration tests, some network specialists, or by security specialists.

Performing these **penetration testing** software also has some advantages. Those are like it will provide the IT team with a distinct prospect on encouraging their lines of protection.

Next, it always provides honest feedback, and lastly, it's a vast and significant application as it is not just bounded to the hardware.

However, you must choose the right tools to perform and achieve a prosperous Pen Test.

Generally, we all know very well that if you are entirely new to this world or this phrase, then let me clarify that pentesting can be a complicated and intricate task, as it can take hours literally, and not only that even sometimes it also takes days as well if it all had to be done by hand.

Hence, in this article, we tried our best to provide you with the top **10 best penetration Testing tools** available on the internet, which will help you choose the best among all and help you complete your task as per your need and demand.

How do We Pick the Best Penetration Testing Tools?

We analyzed the industry with the requirement to protect digital assets and discussed the respective industries' needs with the experts based on the following Points.

How effectively are the Penetration testing tools performing for the following operations?

- How does the software test the vulnerabilities
- How **easy is it to deploy** in the environment
- How deep does it scan your network or application to find the vulnerabilities?
- Updated with Latest Vulnerabilities.
- Whether the software can automate the verification of vulnerabilities?
- Whether the software is updated to exploit recently patched vulnerabilities
- Whether the software **combines automated & manual pentest** feature

So, now without wasting much time, let's get started and explore the whole list that we have mentioned below.

Penetration Testing Tools Features

22 Best Penetration Testing Tools (Free)	Key Features
1. WireShark	**1**. It analyzes network traffic. **2**. Inspect network protocol. **3**. Troubleshoot network performance problems. **4**. Decrypt protocols. **5**. Collect real-time data from Ethernet, LAN, USB, etc.
2. Metasploit	**1**. Bunch of many tools. **2**. Quickly execute tasks. **3**. Automatic reporting.
3. NMAP/ZenMap	**1.** OS Detection **2.** Target specification **3.** Port Scanning **4.** Firewall/IDS Evasion and Spoofing **5.** Host discovery **6.** Scan techniques **7.** Script scan **8.** Service or version detection **9.** Evasion and spoofing
4. BurpSuite	**1.** Intercepting browser traffic **2.** Break HTTPS **3**. Manage recon data **4**. Expose hidden attack surface **5**. Speed up granular workflows **6**. Test for clickjacking attacks **7**. Work with WebSockets **8**. Assess token strength **9**. Manually test for out-of-band vulnerabilities
5. sqlmap	**1**. Powerful testing engine. **2**. capable of carrying out multiple injection attacks. **3**. Supports MySQL, Microsoft Access, IBM DB2, and SQLite servers.
6. Intruder	**1**. Security testing tool for businesses. **2**. There are security features that banks and the government can use.
7. Nessus	**1**. Nessus can check the system for over 65,000 vulnerabilities.

	2. Facilitate efficient vulnerability assessment. **3**. Nessus is constantly updated with new features to mitigate emerging potential risks. **4**. It is compatible with all other tenable products.
8. Zed Attack Proxy	**1**. Compatible with Mac OS X, Linux, and Windows. **2**. Capable of identifying a wide range of vulnerabilities in web applications. **3**. An interface that is easy to use. **4**. Pentesting platform for beginners. **5**. Many pentesting activities are supported.
9. Nikto	**1**. Identifies 1250 servers running out-of-date software. **2**. Fully compatible with the HTTP protocol. **3**. Templates can be used to make custom reports. **4**. Several server ports scan simultaneously.
10. BeEF	**1**. Solid command-line tool. **2**. Fantastic for checking up on any suspicious activity on the network through the browser. **3**. Comprehensive threat searches. **4**. Good for mobile devices.
11. Invicti	**1**. Fully automated. **2**. Bunch of many tools. **3**. System intelligence. **4**. Fast scanning. **5**. Automatic assessment report.
12. Powershell-Suite	**1**. Powershell-Suite works with macOS, Linux, and Windows. **2**. pipeline for command chaining and an in-console help system. **3**. Post-exploitation, infrastructure scanning and information gathering, and attacks.
13. w3af	**1**. Assembled tools available. **2**. Covers everything about known network vulnerabilities. **3**. Enables reusing test parameters.
14. Wapiti	**1**. Proxy support for HTTP, HTTPS, and SOCKS5. **2**. Variations in Verbosity. **3**. Modular attack systems that can be activated and deactivated quickly and easily.

	4. A Customizable number of concurrent HTTP request processing tasks. **5**. A payload can be added as easily as a line. **6**. Can provide terminal colors to highlight vulnerabilities. **7**. It is a command-line application.
15. Radare	**1**. Multi-architecture and multi-platform. **2**. Highly scriptable. **3**. Hexadecimal editor. **4**. IO is wrapped. **5**. Filesystems and debugger support. **6**. Examine the source code at the basic block and function levels.
16. IDA	**1**. It has a multi-processor interactive, programmable, extensible disassembler with a graphical interface on Windows and console interfaces on Linux and Mac OS X.
17. Apktool	**1**. Decode APK resources. **2**. Reformatting the binary APK from the decoded resources. **3**. Putting together and taking care of APKs that use framework resources. **4**. Using automation for repetitive tasks.
18. MobSF	**1**. Information gathering. **2**. Analyze security headers. **3**. Find vulnerabilities in mobile APIs like XXE, SSRF, Path Traversal, and IDOR. **4**. Monitor additional logical issues associated with Session and API.
19. FuzzDB	**1**. For the purpose of fault injection testing, FuzzDB provides exhaustive lists of attack payload primitives. **2**. By providing a comprehensive dictionary structured by framework, language, and application, FuzzDB reduces the impact of brute force testing. **3**. FuzzDB stores dictionaries of regular coding sequences that can be used to explore and investigate server feedback. **4**. FuzzDB has regular expressions for various data types, including credit cards, social security numbers, and common server error messages.

20. Aircrack-ng	**1**. Password cracking **2**. Packet sniffing **3**. Attacking **4**. OS Compatibility
21. Retina	**1**. Multi-tiered architecture: Each report is structured differently depending on the details of the target system. **2**. Threat analytics dashboard: This lets you put Cyber threats in order of how dangerous they are and how likely they are to expose you. **3**. Resource planning: This lets the team create specific "what-if" scenarios to plan for the right way to use resources during the real pen testing cycle. **4**. Retina has over 270 customizable reporting templates that can be changed to fit your client's needs and accurately show the collected information and data. 5. Compliance reporting: Ensure the customer complies with federal laws like HIPAA, Sarbanes-Oxley, etc. 6. Heat maps: In seconds, anyone can show the client where their IT system is most susceptible to attack.
22. Social Engineering Toolkit	**1.** open-source penetration testing framework **2.** Phishing Attacks **3.** pretexting **4.** Tailgating and CEO fraud analysis **5.** Web jacking attack **6.** Credential Harvester Attack
23. **Hexway**	**1.** Custom branded docx reports **2.** All security data in one place **3**. Issues knowledge base **4**. Integrations with tools (Nessus, Nmap, Burp, etc.) **5**. Checklists & pentest methodologies **6**. API (for custom tools) **7**. Team collaboration **8**. Project dashboards **9**. Scan comparisons **10**. LDAP & Jira integration **11**. Continuous scanning **12**. PPTX reports **13**. Customer support

24. **Shodan**	1. Cyber security Search engine **2**. Network Monitoring **3**. Shodan crawls the entire Internet **4**. Looking up IP Information **5**. Internet routers. **6**. Enterprise Security **7**. Academic Research **8**. Market Research
25. Intruder	**1**. Ongoing attack surface monitoring **2**. Intelligent results **3**. Cloud Security. **4**. System Security. **5**. Application Security. **6**. Confidentiality. **7**. Data Security. **8**. Email Security. **9**. Endpoint Protection. **10**. Identity Management.
26. Dnsdumpster	**1**. Actions. Automate any workflow. **2**. Security. Find and fix vulnerabilities. **3**. Copilot. Write better code with AI. **4**. Manage code changes. **5**. Issues. Plan and track work. **6**. Discussions. Collaborate outside of code.
27. Hunter	**1**. Email searches & verifications **2**. Link tracking **3**. Find emails while surfing the web **4**. Searching or verifying lists of email addresses **5**. Domain Tracking
28. Skrapp	**1**. Account-Based Marketing. **2**. Content Marketing. **3**. Conversion Rate Optimization. **4**. Customer Data Platform (CDP) **5**. Demand Generation. **6**. Event Management.
29. **URL Fuzzer**	**1**. Fuzz url set from an input file. **2**. Concurrent relative path search. **3**. a Configurable number of fuzzing workers. **4**. Configurable time wait periods between fuzz tests per worker.

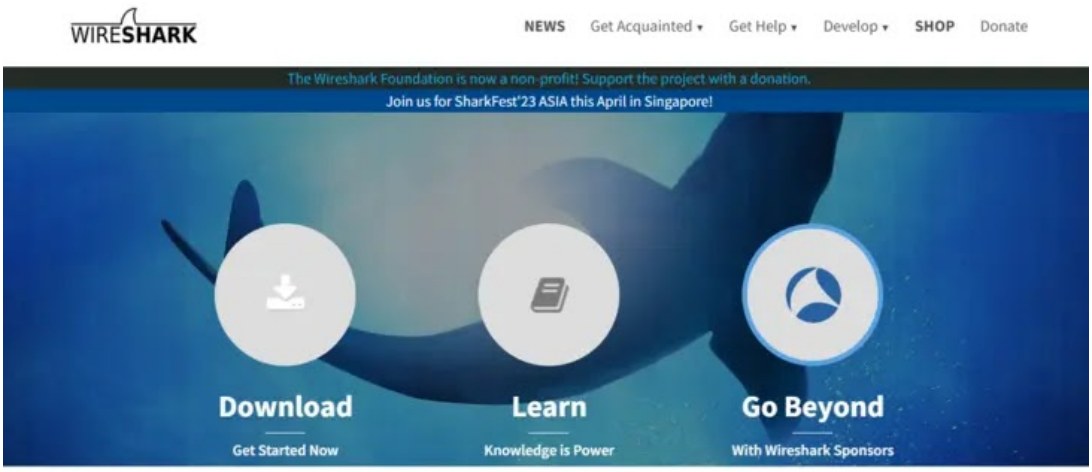
	5. Custom HTTP headers support. **6**. Various HTTP methods support.
30.**Pentest Tools**	1. Find, exploit & report common vulnerabilities 2. Save time for creative hacking 3. Eliminate the cost of multiple scanners 4. offensive security testing 5. network penetration testing 6. Templates for scans, findings, reports, engagements

30 Best Penetration Testing Tools 2023

- **Wireshark**
- **Metasploit**
- **NMAP/ZenMap**
- **BurpSuite**
- **sqlmap**
- **Intruder**
- **Nessus**
- **Zed Attack Proxy**
- **Nikto**
- **BeEF**
- **Invicti**
- **Powershell-Suite**
- **w3af**
- **Wapiti**
- **Radare**
- **IDA**
- **Apktool**
- **MobSF**
- **FuzzDB**
- **Aircrack-ng**
- **Retina**

The list of best penetration testing tools used in different tasks follows.

1. WireShark



WireShark

Next, we have the Wireshark, as it is a universal tool to know the traffic crossing across your network.

Thus it is generally used to **penetrate your everyday TCP/IP** connection problems.

This tool supports the analysis of the number of protocols (around a hundred), including real-time investigation and decryption assistance for many of those protocols.

Moreover, suppose you want to capture data packets. In that case, it will allow you to examine the different features of individual packages, such as where they are getting from, their purpose, and the protocol they have used.

With all this information, you can effortlessly recognize security Vulnerabilities in your network.

Hence, If you're new to pen testing, Learn Wireshark tool online.

This penetration testing tool is primarily a network protocol analyzer, famous for giving the finer details about the internet protocols, packet information, decryption, etc.

It can be used on many different systems, including **Windows, Linux, OS X, Solaris, FreeBSD, NetBSD,** etc. It is a well-known open-source penetration testing tool primarily used to examine network protocols.

With this tool, you can monitor network activity at a very small scale. WireShark is one of the best penetration testing tools because thousands of security engineers worldwide work to improve it.

Notably, WireShark is not an Intrusion Detection System (IDS). As a protocol analyzer, it helps users to visualize malformed packets, but it cannot detect malicious activity on the network and raise the alarm.

Wireshark Demo Video:

Learn Master in **Wireshark Network Analysis** complete online course.

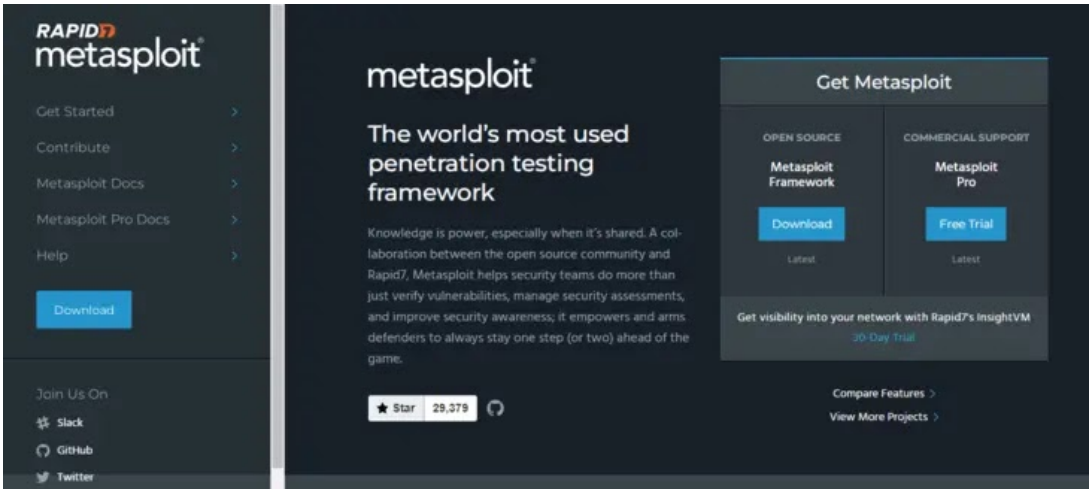
Pros	Cons
Freely available	Does not provide alerts in real-time for any intrusions.
Real-time network traffic analyzer	Capable of information analysis but not transmission.

Download

You can download the Wireshark tools from the below link.

Wireshark – Download

2. Metasploit



Metasploit

First, we will discuss Metasploit; it is a famous collection among all several Penetration Testing Tools.

As per the Cybersecurity specialists and other IT experts, this tool is very beneficial as it has been there for years to achieve various intentions and tasks.

Moreover, it discovers weaknesses, conducts security evaluations, and formulates a defense technique.

Furthermore, you can use the **Metasploit framework** **on different servers, like online-based applications**, networks, and other places.

Suppose if a new security weakness or abuse has arrived, then the utility will recognize it.

Well, if you need to estimate the security of your foundation upon older weakness, Metasploit will be the right choice for you because it is the **most advanced and successful framework** among all the penetration tools; in short, we can say that it's a commercial product.

Metasploit is a great tool because it includes many penetration testing services.

One of the great things about it is that it keeps changing and growing to keep up with the advancements that are always happening.

Metasploit is a PERL-based tool that can be used to practice various **penetration testing scenarios**.

You can use the features to determine which prepackaged vulnerabilities to use and then tweak and configure those exploits for a specific IP and remote port.

Moreover, Metasploit includes a tool called Meterpreter that showcases all outcomes when a vulnerability happens, allowing you to analyze and interpret results and formulate strategies more efficiently and easily.

Metasploit Demo

Pros	Cons
Currently, one of the most widely-used security frameworks	If you're starting out, you probably shouldn't go with Metasploit because it's geared toward more advanced users.
Supported by one of the largest user bases, making it ideal for ongoing maintenance and feature updates	
A free version and a paid commercial version are both made available.	
Extremely adaptable and packed with free software	

Download

You can download the Metasploit tool from the below link.

Metasploit – Download

3. NMAP/ZenMap

NMAP/ZenMap

After Metasploit, we now have the NMAP, also known as network mapper, a free and open-source tool for examining your systems or networks for different weaknesses.

This tool is also useful if you want to carry out other activities, like monitoring host or service uptime and working mapping of network assault surfaces.

This tool generally runs on all the major operating systems and is proper for scanning large and small networks.

With this tool, you can also understand the different features of any target network, including the hosts accessible on the network, the operating system working, and the type of container filters or firewalls in the area.

Hence, NMAP itself is legal to use, and not only that, it's a handy and helpful tool.

NMAP is an acronym for Network Mapping. It aids in network mapping by inspecting ports, exploring operating systems, and establishing an inventory of services and equipment.

This suite is excellent for network penetration testing. NMAP sends packets with different structures for each transport layer protocol.

The packets come back with IP addresses and other data. You can use this information to find servers, find out about OS fingerprints, services, and check for security vulnerabilities.

NMAP is a robust program that can map a massive network with thousands of accessible ports.

Using NMAP, network administrators can compile a list of all the hardware, software, and services currently connected to a network, thus identifying potential security vulnerabilities.

NMAP Demo

> **Learn here the complete NMAP tutorials.**

Pros	Cons
Open-source software is, therefore, readily accessible and easily verifiable.	Utilization requires extensive knowledge.
Easy to navigate	Limited scanning depth
Lots of networking features	Utilized by both malicious hackers and security professionals

Download

You can download the NMap tool from the below link.

NMAP/ZenMap – Download

4. BurpSuite

BurpSuite

Now we will discuss the Burp Suite; this is one of the essential scanners with a limited “intruder” tool for attacks, although many protection testing experts swear that pen-testing without this tool is unbelievable.

Hence, this tool is not free but very cost-effective and efficient. This tool works and surprises with tasks like intercepting proxy, dragging content and functionality, web employment scanning, and much more.

Moreover, you can also use this tool on all the major platforms like Windows, Apple Mac OS X, and Linux environments for performing these types of tasks.

Burp Suite Demo

Learn complete **Burp Suite tutorials**.

Download

You can download the Burp Suite tools from the below link.

Burp Suite Download

5. SQLmap

SQLmap

Lastly, we will discuss Sqlmap, it is a fantastic open-source Pen-testing tool, which is mainly used for identifying and exploiting SQL injection effects in an application and hacking over different database servers.

Apart from all these things, it comes with a command-line interface. Hence it supports all the major platforms.

And all the versions of this tool are available for free of cost, which means you can easily download them if you want.

> ***Well, basically this tool is essentially used for identifying and utilizing SQL injection issues in an application and hacking over different database servers.***

Moreover, as we told earlier, it appears with the command-line interface and is available for various platforms like Linux, Apple Mac OS X, and Microsoft Windows.

Most importantly, all versions of this tool are free for download; as we told you earlier, it is an **open-source tool**; hence, you can easily download it and use it for your use.

sqlmap is a useful open-source penetration testing tool. The primary purpose of this tool is to locate SQL injection vulnerabilities in an application and exploit those vulnerabilities to gain access to the database servers that house the application's data.

It included a command-line interface. It's compatible with Linux, Mac OS X, and Windows.

SQLMap is an automated penetration testing tool for finding and exploiting SQL injection vulnerabilities and taking control of database servers.

SQLMap's features entail compatibility with a wide range of injection methods, database fingerprinting, enumeration of essential data like password hashes and users, and a detection engine.

Pros	Cons
Open-source pentesting tool.	No GUI
Uses automated methods to find different kinds of SQL injections.	Producing false positives and requiring human verification of vulnerabilities.

Demo Video

Learn complete SQmap tutorials.

Download

You can download the SQLMAP from the below link.

sqlmap – Download

6. Intruder

Intruder

The intruder is an effective penetration testing tool that finds security vulnerabilities in the virtual estate, describes the threats, and helps you fix them before an infringement occurs.

It is the perfect tool to help you optimize penetration testing. With more than 11,000 security screenings, Intruder makes organization vulnerability scanning

available to organizations of any size.

Its security checks look for misconfigurations, missing fragments, and common web-based problems like SQL injection and cross-site scripting.

It saves time by putting results in order of importance based on their context and scanning the systems for new vulnerabilities before attackers do.

Pros	Cons
Easy to navigate	There is no zero false positive assurance.
Alerts that are easy to handle	Services for manual penetration testing are not available at all
	The reporting format is challenging to understand

Demo Video

Download

You can download the Intruder tool from the below link.

Intruder – Download

7. Nessus

Nessus

Nessus is one of the world's most common and widely used vulnerability scanners.

Hence, it has obtained first place in the world rankings in 2000, 2003, and 2006 as the best network security tool available on the internet.

Basically, this tool prevents network attacks by identifying the weaknesses and configuration errors that can be used for attacks.

So, Nessus is the worldwide standard for **preventing network attacks, identifying vulnerabilities, and detecting configuration problems** hackers use to enter the network.

> **Apart from all these things, this well-known tool, of course, Nessus, has been used by more than 1 million users worldwide, which makes it the leader in vulnerability assessment, security configuration, and compliance with security standards.**

Moreover, we all know very well that mobile phones, the cloud, and the internet are the future technologies, and it is really important to secure them properly.

As all these new technologies change the assumptions we have used in the past for security technology.

Hence, now it is time to evolve to security 2.0, it's not a next-generation security product; basically, it's a collection of critical capabilities integrated together in a complete solution.

Its specialties include compliance audits, sensitive data searches, IP scans, website scans, and other services.

Nessus aims to make vulnerability assessments easier and facilitate resolving threats or vulnerabilities.

It works on a lot of different platforms and has a lot of various features.

Pros	Cons
It has a free version	The free version does not have more features
It identifies vulnerability accurately	The commercial version is expensive

Demo Video

Download

You can download the **Nessus** tool from the below link.

Nessus – Download

8. Zed Attack Proxy

Zed Attack Proxy

OWASP offers Zed Attack Proxy, or ZAP, open-source penetration testing software.

The OWASP Zed Attack Proxy is the most popular free web security tool in the world, and it is developed and maintained by teams of volunteers from across the globe.

Demo Video

Pros	Cons
Freely available and maintained by OWASP	The tool is difficult to set up.
Easy to learn	Inconvenient in comparison to other tools.
Both beginners and security experts can use it.	Some functions call for additional plugins.
Both beginners and security experts can use it.	

Download

You can download the **Zed Attack proxy** tool from the below link.

Zed Attack Proxy – Download

9. Nikto

Nikto

Nikto is a web application scanner that proclaims itself loudly and proudly.

It's free and includes valuable tools like a web server scanner, a database of known malicious files, and a configuration verification tool.

Nikto isn't undetectable and doesn't try to be, but it still works.

This free penetration testing tool can thoroughly scan web servers and detect threats from nearly 7,000 malicious files and data databases.

Pros	Cons
Freely available for users	It does not have a community platform
Available in Kali Linux	It does not have GUI

Demo Video

Download

Nikto – Download

10. BeEF

BeEF

After that, we will discuss the BeEF, and the BeEF stands for the Browser Exploitation Framework.

Thus it's a penetration testing tool that concentrates on the web browser, which implies that it takes advantage of the point that it's an open web browser into a target system and creates its attacks to go on from this point.

Moreover, this tool has a GUI interface and operates on all major platforms like **Linux, Apple Mac OS X, and Microsoft Windows**. And apart from all these things, it is a wide open-source web application.

The Browser Exploitation Framework is what BeEF stands for. It focuses on the web page.

This means it exploits the evidence that an open web browser serves as a window (or crack) into a target system and bases its attacks on this.

In light of the increasing number of **web-based attacks targeting clients, including mobile clients, BeEF enables professional penetration testers** to evaluate the actual state of security in a target environment by focusing on potential entry points.

BeEF will hijack one or more web browsers and use them to launch facilities for additional attacks against the system using directed command modules.

Demo Video

Pros	Cons
A simple CLI tool for quickly assessing network threats	Only for web browsers; not a tool for everything.
The source code is available on GitHub.	
Compatible with	
Open-source tool	

Learn BeEF – **Browser Exploitation Framework**.

Download

You can download the BeEF tools from the below link.

BeEF – Download

11. Invicti

Invicti

Invicti is a high-accuracy automated scanner that identifies SQL Injection and Cross-Site Scripting vulnerabilities in web applications and web APIs.

Invicti authenticates the known vulnerabilities, demonstrating that they are genuine and not fraudulent claims.

Another thing that makes this tool so prominent is that it lets pen testers scan up to 1,000 web apps simultaneously and lets users configure security scans to make the process powerful.

It exploits vulnerabilities in a read-only manner, and the potential effects are immediately available.

This proof-based scanning works because it produces compliance reports and has other great features, like collaborating with multiple members, and making sharing findings easier without setting up anything additional.

Pros	Cons
A high-quality graphical user interface, perfect for use by pen-testing groups, network operations centers, or even single administrators.	Invicti is a professional security tool with a lot of features. It is not a good choice for home users.
Teams can use color coding and automatic threat scoring to prioritize remediation efforts.	
Runs all the time, so you don't have to schedule scans or run checks manually.	
Comes in different packages so that any size organization can use Invicti.	

Demo Video

Download

You can download the tool from the below link.

Invicti – Download

12. Powershell-Suite

Powershell-Suite

The PowerShell suite is a group of PowerShell scripts that can get details about Windows machines' handles, processes, DLLs, etc.

Putting specific tasks into a script lets you quickly move around a network and see which systems are simple to penetrate.

> **Users can use the declarative configurations and custom scripts, apply the configuration settings, and install the configuration using the push or pull models due largely to the configuration management's convenient features.**

Other features, such as a built-in help system and a pipeline for chaining commands, are also included in the shell.

Pros	Cons
Allowing individuals to investigate multiple attack potentials, aiding in establishing effective login methods, and integrating with WinRM to eliminate the use of Remote Desktop Protocol (RDP) exposes users to severe attacks.	Because it is easy to use, attackers can change the operating system, get into the network without using external files, or use the tool to hide an invasion.

Demo Video

Download

You can download the tool from the below link.

Powershell-Suite – Download

13. W3AF

w3af

Now we will discuss the W3AF, a web application attack and inspection framework.

Moreover, It has three varieties of plugins, discovery, audit, and charge, that interact with each other for any weakness in the site; for illustration, a discovery plugin in W3AF seems for different URLs to test for deficiency and deliver it to the audit plugin which then utilizes these URL's to hunt for several vulnerabilities.

It can be configured to run as a MITM proxy, and this request can be caught.

Thus, you could be transferred to the demand generator, and then manual web application testing can be implemented by using mutable parameters.

Therefore, it also has features to employ the vulnerabilities that it obtains.

This toolkit for penetration testing was developed by the same people who made Metasploit.

It aims to discover, evaluate, and manipulate any vulnerabilities in websites and web-based systems.

User-agent spoofing, modifying request headers, DNS cache poisoning/spoofing, and many other attack methods are all included in this comprehensive package.

The fact that parameters and variables can be saved quickly into a Session Manager file makes W3AF such a complete tool.

As a result, you won't have to re-enter all the key parameters each time you need to use them for another pen test on a web app, saving you a tremendous amount of time.

Furthermore, graphical and textual representations of test outcomes are provided for the user's convenience.

Demo Video

Pros	Cons
Designed for auditors and security testers	Made for experts in the field of security, not ideal for personal networks.
Offers a set of tools that cover vulnerabilities and how to take advantage of them.	
Works as a small utility.	

Download

You can download the tool from the below link.

w3af – Download

14. Wapiti

Wapiti

Users can check the confidentiality of the websites or web apps with **Wapiti**.

It does "black-box" scans of the web application, which means it doesn't look at the source code. Instead, it slinks the pages of the deployed web app, looking for scripts and forms it can use to implant data.

Wapiti acts like a script by injecting payloads into a script to see if it is vulnerable once it has a list of URLs, forms, and their inputs. Wapiti can be used to attack using both the **GET and POST HTTP** techniques.

It can also handle multivolume forms and add payloads to file types (upload). A warning is sent when something mysterious is found, like 500 errors or timeouts. Wapiti can tell the difference between permanent XSS vulnerabilities and reflected ones.

Demo Video

Download

You can download the tool from the below link.

Wapiti – Download

15. Radare

Radare

Radare is a reverse engineering framework. It can disassemble and assemble for many different architectures and debug with local native and remote debuggers as follows:

- gdb
- rap
- WebUI
- r2pipe
- winedbg
- windbg
- Run on Linux
- BSD, Windows
- OS Android, iOS, Solaris, and Haiku

perform forensics on filesystems and data carving, be **scripted in Python, Javascript, Go, and other languages,** and support collaborative analysis using the built-in web server.

The Radare program began as a forensics tool, a scriptable command-line hex editor that could read files from discs.

Later, it added features for analyzing binaries, disassembling code, debugging programs, and connecting to remote gdb servers.

Demo Video

Download

You can download the tool from the below link.

Radare – Download

16. IDA

IDA

In the business world, IDA is the most popular software for reverse engineering.

It can decompile the five most common architectures (x86, x64, ARM, PowerPC, and MIPS), disassemble over a hundred rare architectures, and debug most.

It will help users to take apart that Microsoft update to find the bugs they fixed without telling the user about them or look at a server binary more closely to figure out why the malicious code isn't working.

There are a lot of debuggers out there, but IDA has become the standard for looking at obfuscated code and finding security vulnerabilities.

Demo Video

Download

You can download the tool from the below link.

IDA – Download

17. Apktool

Apktool

Apktool analyzes Android apps and discovers how they work behind the scenes (APK).

It is possible to make on-the-fly changes to the source code and recompile the decoded resources back into APK with the help of Apktool, which allows us to decode APKs to nearly their original form.

Its project-based layout makes it simple to use. With some modifications, it can decode and reassemble resources to nearly their original form. **The endeavor file system and automation of repetitive jobs, such as building an apk**, make it simpler to work with an app.

Demo Video

Download

You can download the tools via the following link.

Apktool – Download

18. MobSF

MobSF

The Mobile Security Framework (MobSF) is a comprehensive, automated, cross-platform (Android/iOS/Windows) mobile software pen-testing, malware detection, and security evaluation framework.

Whether you use a **CI/CD or DevSecOps pipeline, MobSF** can be easily integrated due to its support for mobile app binaries (APK, XAPK, IPA, and APPX) and zipped source code, as well as its REST APIs.

Runtime security analysis and interactive, integrated testing are simplified with the Dynamic Analyzer's aid.

Demo Video

Download

You can download the tools via the following link.

MobSF – Download

19. FuzzDB

FuzzDB

An open-source repository of attack patterns, common resource names, regular expressions for pinpointing enticing server feedback, and related documentation can be found in FuzzDB.

Its primary function is to verify the safety of web applications, but it also has many other potential applications. FuzzDB was made to make it easier to find security bugs in applications by using dynamic application security testing.

It is the first and most complete open dictionary of fault detection structures, dependable resource locations, and regular expressions for corresponding server responses.

Demo Video

Download

You can download the tools via the following link.

FuzzDB – Download

20. Aircrack-ng

Aircrack-ng

Next, we have one of the most comprehensive tools, which is Aircrack ng, it offers a good collection of utility tools for examining the vulnerabilities in a WiFi network.

This tool enables you to watch over the security of your WiFi network by seizing data packets and transporting them to text files for additional analysis.

Moreover, You can also check the execution of WiFi cards through capture and injection. Furthermore, this wifi security auditing tool is free to use.

However, the fact is that cracking wifi today is often possible because of the sparse arrangement, bad passwords, or outmoded encryption protocols. Thus Aircrack is one of the best choices for many users.

It was developed in 2010 and is used to test wireless networks that adhere to the 801.11 standards.

A pen tester can use Aircrack-ng to concentrate on specific aspects of **Wi-Fi security, such as tracking, exploiting, evaluating, and cracking.**

Packer Collecting and converting data to text files for examination by any third-party tool is part of tracking.

Examples of threats include replay attacks, de-authentication, evil-twin cyberattacks, and packet insertion attacks.

Based on the capture and injections, testing encompasses the **Wi-Fi cards and driver abilities. Finally, Cracking allows you to decrypt WEP and WPA PSK keys.**

Several operating systems, including **Linux, FreeBSD, macOS, OpenBSD, Android, and Windows,** are compatible with Aircrack-ng.

A third-party Wi-Fi card that supports monitoring mode is required for Aircrack-ng attacks.

Aircrack-ng Features

- WEP and WPA PSK password weaknesses can be identified using the wireless network testing program Aircrack-ng.
- Aircrack-ng can monitor a specific WiFi network. Data packets are captured and then exported to text files for additional network analysis.
- Aircrack-ng, like any other pen test tool, can perform replay attacks, create bogus entry points, and implant packets into the network.
- Aircrack-ng was made to work on Linux OS when it was first released. This has grown to include more things, like Windows OS.

Demo Video

Learn here the complete **Aircrack-NG** Tutorials.

Download:

You can download the tools via the following link.

Aircrack-ng – Download

21. Retina

Retina

The retina network scanner supports a wide variety of operating systems. It also enables the tester to conduct its own audits and implement automatic fixes.

It protects the business network against every major vulnerability, so the tester can relax knowing. Every session begins with a fresh database, so the tester can trust it to provide accurate results.

A penetration tester can scan up to 256 targets simultaneously with Retina's queuing system, which lets the tester scan in parallel.

Retina Network Security Analyzer is a great system that can find, characterize, and evaluate all the assets on a company's network.

With Retina Network Security Device, clients can quickly find, rank, and fix known vulnerabilities like missing patches and weak configurations.

It is a marketable product and is more of a vulnerability management tool than a Pen-Testing tool. It works by having tests at set times and showing the results.

After the free trial of Retina ends, you'll need to contact them to get an accurate quote for using the software.

Demo Video

Download

You can download the tool via the following link.

Retina – Download

22. Social Engineering Toolkit

Social Engineering Toolkit

Next, we will discuss the Social-Engineer Toolkit (SET); it is a unique tool in sequences that detects the attacks that are targeted at the human element than on the system component.

Further, it has incredible features that let you send emails, java applets, and many more, including the attack code.

Well, this tool must be practiced carefully and only for 'white-hat' purposes.

While now, if we talk about its availability, let me clarify that this tool has a command-line interface and **runs on Linux, Apple Mac OS X, and Microsoft Windows**. And not only that even it is an open-source tool.

Demo Video

Learn the complete Social-Engineer Toolkit tutorials.

Download:

You can download the tools via the following link.

Social Engineering Toolkit – Download

23. Hexway

Hexway provides users with 2-workspace self-hosted environments made for penetration testing (PTaaS) and vulnerability management.

It's created to normalize and aggregate data from pentest tools (**like Nmap, Nessus, Burp, and Metasploit**) to work with it fastest and most conveniently.

Hexway is made for pentesters who know that time is extremely valuable — that is why **Hive & Apiary** has a wide toolkit to work with security data and present work results in real-time.

Also, Hexway isn't just about pentest reports or data aggregation – it's about enhanced workflow and useful methodologies that can speed up testing and bring more profit to the company.

Demo Video

Download:

You can download the tool via the following link.

Hexway – Download

24. Shodan

As a customer, we can completely trust Shodan, which gives you detailed information. How Google is one search engine, the same way Shodan is also a search engine.

It helps to search the invisible part of the information from the internet, which is best for cybersecurity.

Suppose you want to know the perfect number in anything that also Shodan will show you. You need to put the question in the search bar, and you will get the specific result.

If you are looking for an online exploit search tool, then this tool is the best one.

Demo Video

Download

You can download the tool here.

Shodan – Download

25. Intruder

It is one of the online automated penetration testing platforms that finds cybersecurity vulnerabilities, it includes the process of simulating real cyber-attacks against your own systems.

The **tools check systems for vulnerabilitie**s, including web-layer security problems, infrastructure weaknesses, and other security misconfigurations.

The tools also include an Email Verifier, which completely checks for the email address to let you confidently send your emails.

Demo Video

Download:

You can download the tool via the following link.

Intruder – Download

26. Dnsdumpster

This is one domain research tool that discovers the subdomain and targets that.

It works to find a subdomain that includes Shodan and Maxmind.

As a user, you are not allowed to search unlimited numbers there is a limit to it.

If you want to try out with more limits, then you need to opt for a domain profiler.

This domain profiler is a little similar to Dnsdumpster because it also performs domain.

The domain profiler has much additional information, and it's not free. You need to have a membership plan for it.

This online tool is mainly used for commercial purposes and for finding the subdomain user need.

It also gives you a clue to search the subdomain, and it will perform as an **IP lookup**. There are many more subdomain finders available in the market.

You also need to **find the email address where the company** is vulnerable to phish. You need to find the email address of the target company.

Demo Video

Download:

You can download the tool via the following link.

Dnsdumpster – Download

27. Hunter

This is one of the best email finder services where anyone can search email addresses through the email finder method or domain search method.

Since this domain is only for searching, you must put the email address with a domain name in the search bar.

The tools also include an Email Verifier that checks the email address to let you confidently send your emails.

Demo Video

Download:

You can download the tool via the following link.

Hunter – Download

28. Skrapp

It is best for email finder tool to search email addresses with domain search features.

Why send single mail, you will have a bulk email finder, and it helps you do your work less by importing CSV files on employees and company names. It also supports it if it is in bulk.

Many users prefer to search the email address programmatically for the API available.

This API domain performs so that it gives an extensive lookup of your domain in real-time. This provides correct technical information to the end-user with complete security.

You will get the option to explore more through the email finder tool.

You need to know which files or folders will give you sensitive information like administrator passwords, web servers, and GitHub keys.

Demo Video

Download:

You can download the tool via the following link.

Skrapp – Download

29. URL Fuzzer

This is one of the best online services given by the Pentest tool, and you can also do the customization, where you can even discover hidden files and directories.

This can handle more than 1000 common names and everything it keeps safe.

This is mainly used to keep safe your hidden resource via a light or full scan. The registered user is allowed for full scan mode.

This tool includes more than 20 tools best for information gathering, **infrastructure scanning tools** checking systems for vulnerabilities, and much more.

This technology profiler gives real-time information by targeting **domain API and live domain API.** Domain API provides technical information like the embedded plugin, framework, analytics service, and libraries.

It also relies on the database, which can provide current information related to the target. If you search in the search bar, you will get a few pieces of information from the API domain.

This software helps to extract the information where the technology got stuck. If you want to know about CMS and its target, then you have to use this framework. This will analyze the tool which has operated.

There are different ways to use this tool to access the information using the Lookup API. To secure product security, engineers and developers use Wappalyzer technology.

As a user, you can browse this extension in Firefox, Chrome, and Edge.

Demo Video

Download:

You can download the tool via the following link.

URL Fuzzer – Download

30. Penetest Tools

One of the best online tools to quickly discover and report vulnerabilities in websites and network infrastructures.

The website offers 25+ tools to run automated testing sequences and also provides customizable report templates.

It is one of the best tools for **performing black-box external network security assessments** and reports allowing pentesters to identify and quickly respond to potential issues.

Demo Video

Download:

You can download the tool via the following link.

Penetest Tools – Download

Final Thoughts

With how quickly technology changes, your risk is being outdone by an opponent whose products have many more features and the best security in their class.

In today's digital world, customers need security, confidentiality, and better optimization for every program, software, website, etc. However, it would be best to do security testing to protect your products.

Penetration testing is one type of security check that can be done on IT products.

When you conduct penetration testing, you gain insight into your network security from a hacker's perspective.

Experts complete the task and then apply what they learn to strengthen cybersecurity at the company.

As a result, penetration testing can help you find vulnerabilities and strengthen your defenses if you have the time and resources to invest in one.

If you want to know how secure your organization is and how to fix any vulnerabilities you find, thorough penetration testing is the way to go.

Therefore, penetration testing has become an increasingly popular security strategy among organizations in recent years.

Conclusion

Well, this article is a brief summary of what a penetration tool is, how it works, why it is essential, and what is the top tool among all, as well as we have also mentioned the critical principles that should be taken into account while choosing the right tool to be used.

Eventually, we have also discussed the top 10 Penetration Testing Tools used today frequently.

And it is essential to note that the tools studied are all open-source, suggesting that you can easily download them for free.

And not only that, even if you want then, you can easily modify or enhance the nature of these tools, or if you want, then you can also contact the team or community of the particular tool to request any addon to fit the needs of the particular test, which are to be taken out.

Moreover, there is an excellent advantage of utilizing **open source Penetration Testing** software, as they are continually being perfected by subscribers and other cybersecurity experts to guarantee that they stay at the lead of the ever-changing threat landscape.

While now, if we talk about the list, let me clarify that this list is not independent, as here in this list, we tried our best to suggest the most preferred ones.

Several other advanced Penetration Testing software **are also available for any Security-based conditions.**

So, we hope that you liked this post; if you liked this post and if this post is beneficial to you, then do not forget to share this post with your friends and family, on your social profiles, and with those who are facing these types of problems.

Moreover, if you have any other queries regarding the Penetration Testing Softwareor the list we mentioned above, please do not hesitate to share your query, suggestions, or addon in the comment section below.

Frequently Asked Questions

Is Kali Linux best for penetration testing?
One of the most widely used security distribution functions, Kali Linux provides access to numerous exploits and penetration testing tools.
Furthermore, new features and tools are consistently added to Kali Linux, making it an indispensable asset for any penetration tester.

1. There are many reasons why Kali Linux is a fantastic penetration testing tool.
2. Many security tools are installed, so performing a penetration test is straightforward.
3. New capabilities and utilities are routinely added to Kali Linux.
4. The process of using it is simple.
5. It's free to use and works on several different systems.

Is penetration testing a good career?
We now live in a digital era where the increasing complexity of cyberattacks has grown alongside the advancement of technology.

Companies need skilled penetration testers to identify vulnerabilities and improve their overall security.

It's a lucrative field that rewards those proficient in computers, IT, and finding

solutions. According to Glassdoor, the average salary for a penetration tester in the United States is $1,02,405.

Also, Read

Best UTM Software (Unified Threat Management Solutions)

Best Android Password Managers

Vulnerability Assessment and Penetration Testing (VAPT) Tools

AWS Security Tools to Protect Your Environment and Accounts

SMTP Test Tools to Detect Server Issues & To Test Email Security

Online Penetration Testing Tools for Reconnaissance and Exploit Search

Best Advanced Endpoint Security Tools

10 Best SysAdmin Tools

Dangerous DNS Attacks Types and The Prevention Measures

Best Security Incident Response Tools

Mobile App Security Scanners to Detect Vulnerability

Cyber Security News Team

Work done by a Team Of Security Experts from Cyber Security News