Infiltr8: A Linux Terminal-Based Pentesting Tool

Streamline your ethical hacking workflow with a powerful, terminal-based toolkit.

What is Infiltr8?

Terminal-Based

Infiltr8 is designed for use within the Linux terminal environment. This offers flexibility and portability for security professionals.

Ethical Hacking Toolkit

It provides a comprehensive set of tools for conducting ethical penetration testing and security assessments.

Simplified Workflow

Infiltr8 is built with simplicity and efficiency in mind, making it suitable for both beginners and experienced security professionals.

Key Features

Information Gathering

Infiltr8 utilizes powerful tools like Amass, Sublist3r, WPScan, Nmap, and Gobuster to gather crucial information about a target network. These tools can perform subdomain enumeration, network scanning, and web vulnerability discovery.

Vulnerability Scanning

Once you have gathered initial information, Infiltr8's vulnerability scanning tools come into play. Tools like SQLmap, Nikto, Wapiti, and CVE Search are used to detect vulnerabilities in web applications and network configurations, providing actionable insights for exploitation.

Exploitation

Infiltr8 empowers ethical hackers to simulate real-world attacks by leveraging tools like Metasploit Framework, Commix, XXE Injector, and SSRFMap. These tools allow for exploiting identified vulnerabilities and understanding potential security risks.

Additional Tools

Denial of Service

Hamster & Ferret tools simulate DoS attacks, allowing you to test system resilience against potential disruptions.

Web Application Attacks

XSStrike is a tool for testing web applications for cross-site scripting (XSS) vulnerabilities, which can be exploited by attackers to inject malicious scripts.

How It Works

1

Information Gathering

Start by identifying potential targets and collecting information about their network infrastructure, services, and vulnerabilities.

2

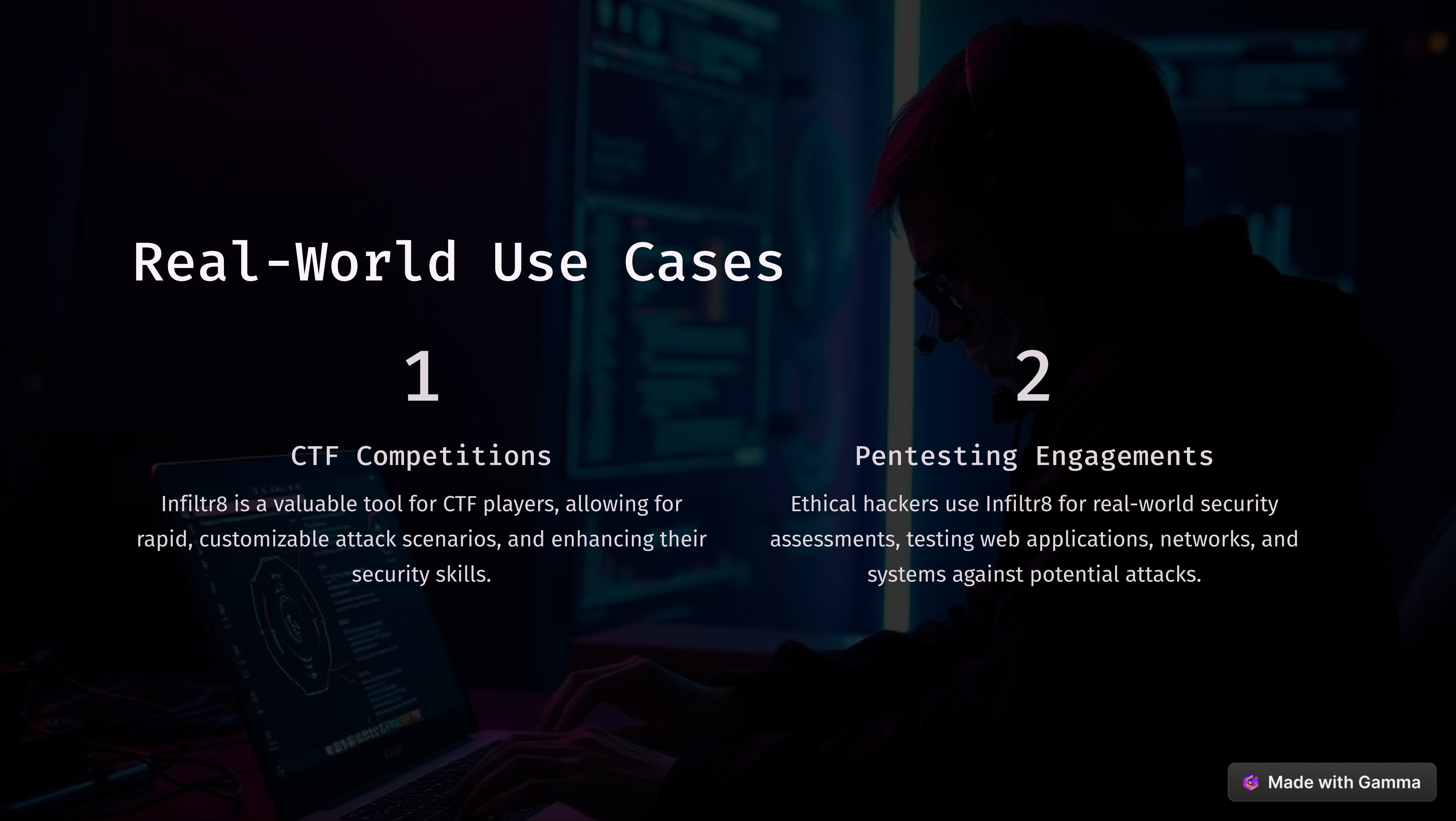
Vulnerability Scanning

Analyze collected data to identify potential vulnerabilities, such as weak passwords, outdated software, or misconfigured services.

3

Exploitation

Test and exploit vulnerabilities to gain access to systems and assess their security posture.



Real-World Use Cases

1

CTF Competitions

Infiltr8 is a valuable tool for CTF players, allowing for rapid, customizable attack scenarios, and enhancing their security skills.

2

Pentesting Engagements

Ethical hackers use Infiltr8 for real-world security assessments, testing web applications, networks, and systems against potential attacks.

Why Infiltr8?

1

Simplified Workflow

Infiltr8 streamlines pentesting with its intuitive terminal-based interface.

2

Powerful Tools

Infiltr8 integrates a powerful suite of security tools for comprehensive assessments.

3

Flexibility & Control

Enjoy full control and flexibility with both automated and manual testing options.