

Forum:[Hack Forums](#)

Thread: [A General Outline For Bypassing Firewalls - Ethical Hacking](#)

Koyote - January 25, 2023, 6:02 am

As an ethical hacker, you should always have written permission from the system or network owner before attempting to bypass firewalls. Here are some general steps for conducting ethical hacking and bypassing firewalls:

1. Identify the target: Determine the specific system or network that you have been authorised to test.
2. Information gathering: Collect as much information as possible about the target, including IP addresses, open ports, and firewall configurations.
3. Identify vulnerabilities: Use a tool like Nessus to scan the target for vulnerabilities.
4. Exploit vulnerabilities: Attempt to exploit any vulnerabilities that you have identified in order to gain unauthorised access to the target.
5. Bypass firewall: Attempt to bypass the firewall in place to gain access to the target system or network. This could include techniques such as port forwarding, VPN tunneling, or exploiting a vulnerability in the firewall software.
6. Report findings: Once you have completed the test, document your findings and report them to the system or network owner. Include detailed information about the vulnerabilities you found, how you exploited them, and any recommendations for fixes.

It is important to remember that ethical hacking is a complex and highly technical process. If you are not an experienced hacker, it is best to work with a professional ethical hacking service.

Please note that this guide is for educational purpose, It's illegal and unethical to perform unauthorised penetration test on any system or network without proper consent.

SIM-587985 - January 25, 2023, 8:54 am

What are some common vulnerabilities and how would you exploit them?

Is there any websites that help teach ethical hacking or bypassing firewalls?

Koyote - January 25, 2023, 9:53 am

(Jan 25, 2023 09:54 AM)Wardyn Wrote: [\[CITE\]](#) What are some common vulnerabilities and how would you exploit them?

Is there any websites that help teach ethical hacking or bypassing firewalls?

Thanks for your questions, [SIM-587985](#)

A few quick examples:

SQL Injection: SQL injection is a type of attack in which an attacker injects malicious SQL code into a web application's database, allowing them to gain unauthorized access to sensitive information. To exploit this vulnerability, an attacker would typically enter malicious SQL code into an input field in a web application, such as a login form or search bar.

Cross-Site Scripting (XSS): XSS is a type of attack in which an attacker injects malicious code into a web page that is then executed by a victim's browser. To exploit this vulnerability, an attacker would typically inject malicious code into an input field in a web application, such as a search bar or comment section.

Cross-Site Request Forgery (CSRF): CSRF is a type of attack in which an attacker tricks a victim into performing actions on a web application without their knowledge or consent. To exploit this vulnerability, an attacker would typically use social engineering tactics to trick the victim into clicking a link or submitting a form that performs an action on the web application.

File Inclusion: A file inclusion vulnerability is a type of vulnerability that allows an attacker to include a file on a web server through a script on a web page. This can lead to information disclosure, or even remote code execution if the attacker can manipulate the script in a way that allows them to include a file containing malicious code.

Weak Credentials: Weak or easily guessable credentials, such as default usernames and passwords, can also be exploited by attackers. To exploit this vulnerability, an attacker would typically use automated tools to try commonly used usernames and passwords on a web application or network.

Here are some good sites for people to get started with:

[Offensive Security](#) - Offers a variety of online courses and certifications, including the popular Penetration Testing with Kali Linux (PWK) course.

[SANS Institute](#) - Offers training courses and certifications, including the Certified Ethical Hacker (CEH) certification.

[Cybersecurity Ventures](#) - Offers a variety of cybersecurity training and certification programs.

[HackerOne](#) - Offers free online courses and resources for learning about ethical hacking and penetration testing.

[Hacktivist](#) - Offers online courses and resources for learning, with a focus on Indian cyber security.

[Udemy \(warez disallowed\)](#) - Offers online courses related to ethical hacking and penetration testing, including the "Ethical Hacking from Scratch to Advanced Technique" course.

[Coursera](#) - Offers related online courses, including the "Introduction to Cybersecurity" course.

Learning ethical hacking and firewall bypassing is a continuous process, so it's important to stay up-to-date with the latest tools, techniques, and best practices in the field.