Hacking

There are various ways to hack, and this topic is quite interesting. As a hobbyist White Hat Hacker, I find there is a lot of knowledge to learn in this field. Here, I will record some methods I've explored.

Default Passwords

Some websites, including those of government agencies, still use default passwords. While many companies or users change their default credentials, others fail to do so. Users are often lazy, and passwords like `12345678` are still commonly seen. This is especially true for older or niche systems.

nmap or Netcat

These tools are used to scan the ports of a server. Pay particular attention to commonly used ports such as 80, 22, and 443. For AWS instances, the default username is `ec2-user`. For Azure instances, it's `azure-user`. For Google Cloud instances, the default username is usually `ubuntu` or `google-cloud`. For other cloud instances, it's typically `root`.

Using the Browser Console

The browser console is useful for inspecting hidden information. Sometimes, critical data is embedded in the HTML or JavaScript code but not visible on the page itself.

Backdoors

In life, backdoors provide unauthorized entry into buildings, often unnoticed or unguarded, such as parking lots or side doors. Similarly, systems may have hidden backdoors that bypass normal security protocols.

Social Engineering

People's nicknames, birthdays, and social media posts can reveal a lot of personal information. Often, these details are used to construct weak passwords. For Wi-Fi networks, knowing someone's house number or other identifying details can help in guessing their SSID or password.

SQL Injection

For any input field, testing with `? 1=1` is a common technique to identify vulnerabilities and potential SQL injection points.

Actuator or Health APIs

For API servers, applications like Spring Boot offer an `/actuator` endpoint that provides machine and application health data. Other web frameworks also have similar functionality that can expose sensitive server details.

Traffic Monitoring

To understand how the frontend interacts with the backend, use proxy applications like Charles Proxy on macOS to record and analyze request logs. This can give you insight into the paths and data exchanges between components.

Limits and Edge Cases of APIs

It's important to test the limits and edge cases of an API or server. A Distributed Denial of Service (DDoS) attack attempts to overwhelm request limits. Additionally, edge cases are scenarios where APIs might allow access to restricted data. Testing these can help ensure proper access controls are in place.

Admin Panels

Sometimes, admin or internal panels are not adequately protected. It's worth trying to access paths like `/admin` or visiting subdomains like `admin.xx.com` to check if these areas are properly secured.