Top five hacking Tools for Security Assessments and Penetration Testing

Chey Cobb, CISSP

You're called to do a security assessment on a network for a client, and the obvious question arises: Which security assessment tools do you bring? Sadly, while there are literally hundreds of penetration testing and security assessment tools from which to choose, no single tool will do a complete job. Therefore, you need to assemble a catalogue of programs with individual specialties in order to conduct an extensive security assessment. What follows is a list of the most popular tools, their usage, and why they should be in your security assessment toolbox.

Nessus

- Available from Tenable Network Security
- Free for basic application or pay option available for full-featured program/Linux/Mac/Windows

This popular hacking tool is primarily a vulnerability scanner that queries servers on the network, identifies security vulnerabilities and rates them according to severity. The basic scanner is free, but the vulnerability database on the free version will not have the most current vulnerabilities, and updates to the database are limited. The paid version removes this restriction and provides a "live feed" in which the vulnerability database is constantly updated.

The Nessus security assessment tool can also search for sensitive information through the use of a configurable content scanner. If your company stores personal identity information, Nessus can help you identify where this information is kept so you can take appropriate measures to ensure this data is as safe as can be (this extra protection is a requirement of most compliance regulations). Nessus can look at access permissions on both sides of the firewalls, enumerate shares, and identify unnecessary services running on servers. Misconfiguration of permissions, shares and services are routes that hackers often use to gain access to a network.

Nmap

- Available from Insecure
- Free for Linux/Mac/Windows

Nmap is a powerful security assessment tool capable of scanning very large and complex networks. It identifies what services are running, what operating systems are in use and what type of packet filters/firewalls are employed. Nmap also works like a bloodhound to track down strange connections that might indicate an infection or security breach.

All of this is exactly the information a hacker needs to begin exploiting a network. It's like a robber casing a bank and discovering where the weaknesses are. In the case of a security audit, it's important that service providers and consultants have this information beforehand so they can take steps to hide information from prying eyes.

While vulnerability scanners are usually at the top of the list of important hacking tools, it's equally important to truly know the network for a complete security assessment.

Core Impact

Available from Core Security
Must pay for tool. Price varies for Windows only.

Since many companies store customer information on databases connected to Web-based applications, it's important to ensure that information cannot be drawn out of the database. Core Impact not only identifies Web servers, Web applications, ports and services, it simulates actual attacks to see if the Web servers/applications are vulnerable.

After checking for vulnerabilities the penetration testing tool completely backs out of the network by removing all code that was used to scan and attack. Because it's very easy to inadvertently upset a network during penetration testing, it's important to use a tool that prevents disruption of a client's network.

Kismet and Aircrack

- Kismet is available from Kismet Wireless
- Free for Mac/Windows/Linux
- Aircrack is available from Aircrack
- Free for Mac/Windows/Linux

Kismet is a wireless sniffer for detecting 802.xx networks and access points. Aircrack is a very fast wireless encryption cracker. These two security assessment tools are included as a pair here because it's not good enough just to find wireless networks -- you need to see if you can break the encryption to gain access.

In a proper security assessment you need to check that wireless networks cannot be accessed from outside the company. It's not uncommon for employees to bring in their own wireless access points and connect them to the corporate network without permission. Kismet finds these rogue access points so they can be disabled.

Conclusion

This list represents a very small sample of the tools available and your choices may vary. However, the list contains enough tools to get you started. We must note that it can take a while to fully understand the complexities and subtleties of the products mentioned. There are books available for most of these tools and there is also good online support through forums and documentation.