Web Attacks

Exercises

1. Experiment with Metasploit data gathering modules for Firefox, including post/firefox/gather/passwords, post/multi/gather/firefox\_creds, post/firefox/gather/history, and post/firefox/gather/cookies.
2. Try the Metasploit module to collect password data from Chrome, post/windows/gather/enum\_chrome.
3. Experiment with other data gathering Metasploit modules for Internet Explorer. Is it possible to obtain the target’s browser history?
4. Run Ettercap and dump the results to a log file. Use Etterlog to analyze the result. What switch can be used to extract just the password data?
5. What information is obtained by an attacker that intercepts SSL communication to an IIS web site that uses Windows authentication?
6. Run an sslstrip Ettercap attack against a website running IIS. Compare the results between basic authentication and Windows authentication.
7. Experiment with the NMap script http-brute to attack a password protected web site.
8. Experiment with the Metasploit module auxiliary/scanner/http/http\_login to attack a password protected web site.
9. Configure ModSecurity to block brute-force attacks.
10. Experiment with the Metasploit module auxiliary/scanner/http/http\_version.
11. The NMap script http-userdir-enum tries to determine valid usernames on an Apache web server that provide per-user directories. Run the script against an Apache server. The list of usernames checked by the script is contained in the file /usr/share/nmap/nselib/data/usernames.lst (on Kali).
12. What is the Slowloris attack? Is it still effective?