Firewalls: Supplement

Exercises

1. Configure an IPFire based network. Sniff the traffic between the IPFire system and the network gateway. What packets are observed? How often? Is there anything interesting about the contents of the packets?
2. (Advanced). IPFire is not the only reasonable choice for a network firewall. Another excellent choice is pfSense (<https://www.pfsense.org/>) which is based on FreeBSD rather than Linux. Build a network like mars.test using a pfSense firewall.
3. Replace the IPFire DHCP server with a Windows DHCP server in a network like mars.test.
4. What is the key size for the default key generated for the IPFire SSL/TLS key? How secure is it?
5. Suppose an administrator configures the web proxy and the outgoing firewall, but instead of blocking all HTTP and HTTPS traffic from the internal (GREEN) network, the administrator blocks HTTP and HTTPS traffic from all networks. What occurs?
6. The network mars.test described blocks most outbound requests from the domain controller and the internal file server. What are the implications for Windows Update?
7. How well does the Metasploit payload windows/meterpreter/reverse\_tcp\_allports work as a way of bypassing restrictive egress filtering? See <https://blog.rapid7.com/2009/09/24/forcing-payloads-through-restrictive-firewalls/>.
8. Another approach to mapping egress filter rules is the Metasploit module post/windows/recon/outbound\_ports. Compare this module to the method shown in the text.
9. Configure the IPFire webproxy to use local authentication. From a packet capture, verify that the proxy authentication base64 encodes the credentials but otherwise passes them in plain text. Extract the credentials from the packet capture.
10. Compare the module post/multi/manage/autoroute to the route command described in the text.
11. Test the attack exploit/linux/http/ipfire\_bashbug\_exec against IPFire.
12. Test the attack exploit/linux/http/ipfire\_proxy\_exec against IPFIre.
13. Test the attack exploit/linux/http/ipfire\_oinkcode\_exec against IPFIre.