Andrew Plum

Mr. Alves-Foss

Cyb 110

11/12/21

Ch. 11 Homework

1) Address space layout randomization is a security technique where the operating system makes it more difficult to tamper with the contents of memory in use by shifting the memory content around when it is in use. Each time the program is loaded, different addresses are used. Address space layout randomization makes it more difficult for an attacker to predict target addresses which hinders their ability to perform some security attacks specifically ones which require precise addresses.

3) Although they are similar, there is a difference between port scanners and vulnerability assessment tools. Port scanners check network ports for statuses and the network services running on a host. Vulnerability assessment tools try to find and report network services on host which have known vulnerabilities. Vulnerability assessment tools are more complex than port scanners because even though both scan network services running on hosts, vulnerability assessment tools can detect services that have known vulnerabilities.

4) In operating system security, there are several available avenues the attacker may take in order to attack your operating system. The total sum of all these avenues the attacker might take to attack your operating system is what is called your attack surface. The attacker is more likely to be successful in their endeavors the larger your attack surface is to your operating system. If you want to make it more difficult for attackers to successfully penetrate your defenses, you need to make your attack surface tinier. You can do this by hardening your operating system by removing unnecessary software, removing unneeded services, altering default accounts, using principles of least privilege, performing updates to your operating system, and implementing logging and auditing.

5) Using firewalls as well as intrusion detection systems both on your host and your network increases your layers of security. Although firewalls on hosts usually have less features than a full network firewall, they are typically capable of similar packet filtering and stateful packet inspection. Firewalls on your host can filter out specific traffic depending on the hosts preferences. Overall increased layers of security make your systems, and in this case individual hosts, more secure and difficult for the attackers to successfully to attack.

9) Principle of least privilege applies to operating system hardening because operating system hardening is all about making it more difficult for the attacker to successfully attack your operating system and you do that by reducing its attack surface, and principle of least privilege does that because it only gives to a party the absolute minimum permission needed for it to carry out its function. With very limited permissions given to a party, it is very difficult for that party to do more than what was intended with the limited granted permissions. This means it is more difficult for attackers to conduct certain attacks if their permissions limit them making your operating system more secure. This is why principle of least privilege applies to operating system hardening.

10) I downloaded Nmap from the link provided, conducted the basic scan of the website it told me to scan, and I found only four open ports. The ports I saw that were open from the scan were 22/tcp with

service “ssh”, 80/tcp with service “http”, 9929/tcp with service “nping-echo”, and 31337/tcp with service “Elite”. All of the rest of the ports from the scan were not open and were in the closed or filtered state.