Ryan Carey

4/25/2019

SRA 211

Theoretical Pen Testing

* Establish Security Posture of Assigned Workstation ( 25 points)

I would use backbox, which is based on ubuntu because I run a dual boot system at home that uses ubuntu. The backbox pen testing OS should have everything I need to identify some security issues. It’s also open source, so there should be no issues with licensing and any problems inadvertently caused can be dealt with more easily. The context of testing will determine which tools are actually used in this case. Since it’s a workstation, mainly I should be looking for settings that facilitate intrusion, like remote desktop being on, ports 22 and 23 forwarded on the router, mostly things like that.

* Interpret Security Posture Assessment ( 25 points)

This is impossible without having actual results to review, but let’s say during testing a lot of latency is present even from one workstation to another over ethernet. That would be a good indicator that a broadcast storm was occurring. If the workstation is receiving a lot of traffic on the telnet or ssh ports, that could mean someone is trying to bruteforce into the workstation. Same story with RDP. If the operating system is windows prior to 10, I expect my pen testing might reveal user passwords since the original NTLM is vulnerable.

* Develop a course of action ( 25 points)

What actions to take depend, again, on the results of testing. If the workstation is currently under siege any remote desktop, secure shell, or vnc services should be stopped and the firewall configured before starting them up again. If the issue is an outdated driver with known exploits, then the driver needs to be updated. If the issue is a broadcast storm, the source of the storm needs to be determined. If the issue is the security of NTLM, then the workstation OS should be upgraded if possible.

* Demonstrate your course of action was successful ( 25 points)

This step is as simple as running the pen testing tools again and verifying that the vulnerabilities have been sufficiently dealt with. If they haven’t, rinse and repeat.