Test Answers – Project C (CEH) Omer Libich

1. Name an exploit found on the webserver that would be considered critical or high?
   * The remote SSH host key has been generated on an Ubuntu system which contains a but in the random number generator of its OpenSSL library.
   * The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
   * An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a MITM attack.
   * SOLUTION: Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be regenerated.
2. Name an exploit found on the DNS server that would be considered critical or high?
   * Weak password for the root user “password”
   * A weak password is considered a critical exploit that would allow an attacker to make changes to the DNS table and potentially cause a DoS or setup a pharming attack for credentials.
   * SOLUTION: Change the root user password
3. Can you remotely connect to the webserver from outside of the network?
   * Yes, by entering the web address www.seclab.net you may access the webserver.
   * The pfSense firewall allows https traffic into the DMZ from outside of the network.
4. Can you remotely connect to the CEO’s computer from outside of the network?
   * No, I cannot remotely connect to the CEO’s computer from outside of the network.
   * The pfSense firewall security policy does not allow that traffic class to move from the DMZ to the internal VLAN.
5. What exploit can be used on the Windows 7 machine and does it work?
   * <https://www.youtube.com/watch?v=goUVgchVGB0>
6. What tools did you use to conduct the vulnerability assessment and why?
   * Nessus – because it is a comprehensive vulnerability assessment tool that references CVE and proposes solutions to the findings.
   * OpenVAS – for the same reason. It is comprehensive and references CVE nomenclature that will recommend action to mitigate or workaround any discovered vulnerabilities.
   * BurpSuite – was used for network mapping and node discovery
   * Nikto – used as a vulnerability scanner
   * nmap – used as a vulnerablility scanner
7. What tools did you use to conduct the exploit and why?
   * The tool that I used is the Metasploit Framework, it is the most comprehensive resource with abundant online tutorial and online community support.
   * I also used BurpSuite – it is a proxy tool that allows fine-tuned attacks to the webserver applications.
8. What users are located on the Windows Server 2008 machine?
   * I don’t know, we weren’t provided a VirtualBox image of a Windows Server 2008
9. What exploit was successful on the Windows Server 2008 machine?
   * <https://www.youtube.com/watch?v=tqLMjWgMd_U>
10. Where you able to exploit a Linux machine and which one worked?
    * Yes, I was able to exploit the webserver running Ubuntu. The exploit that worked for me is at following path: exploit/unix/irc/unreal\_ircd\_3281\_backdoor
    * I was able to establish a session and shutdown the server remotely-effectively denying service.