CPTR 427 Lab #10-11 Name

Network Sniffers & IDS

# Questions from reading:

Reading Material: NIST publications SP 800-X on security

* <http://csrc.nist.gov/publications/PubsSPs.html>
* Other web resources on WIFI

1. What is a SSID?
2. Name the different security (encryption) modes for wireless networks. For each mode, give the encryption algorithm and tell if the security mode is secure.

|  |  |  |
| --- | --- | --- |
| **Security Mode** | **Encryption Algorithm** | **Secure / Not Secure** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. In a default configuration from the factory of most wireless access points, what things would have to be changed to make an access point secure?
2. What is war-driving?
3. What elements should you report as part of an incident response report(see: <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>).
4. List three elements to help you collect good forensic data (same link see evidence gathering – think general items).
5. What should you do to analyze your forensic data?
6. Where would you find log files on Linux?
7. Where would you find log files on Windows?
8. What is dd and what do you use it for?
9. Research forensic tools on line and come up with a list for windows or Linux. Be prepared to discuss one on each system for the final exam.

# Lab OPs

1. You will need a WIFI SNIFFER such as Netstumbler or Kismet on your laptop.

# War Drive Collegedale

List places and SSIDs of any WIFI networks you find in the college campus area group them by secured vs non-secured. You will probably want to print this information/report from your sniffer software.