

Lab-3: Network Forensics

Digital Forensics
Spring 2004

Posted: February 12th
Due: Rolling Deadline

This is a week-long assignment on network forensics. In this assignment you will sharpen your knowledge of network forensics and get some hands on experience doing forensics on live network traffic. You need an account on a network forensic appliance installed in the University's network to complete the second part of the assignment.

1 Basic Network Forensics

Refresh your knowledge on networks and network protocols by answering *all* of the following questions:

1. What is a network sniffer? Give examples of sniffers.
2. What is port scanning?
3. Name at least 5 types of port scans?
4. For each type of scan listed above, if a network traffic dump is given, describe methods to identify packets that belong to the scans above.
5. Explain what a *distributed slow scan* is and how it is carried out?
6. Can a TCP connection be spoofed? If so, how? If not, why not?
7. Can a computer spoof a TCP connection to frame another computer in the same broadcast domain? If so, explain in detail how? If not, explain why not?

2 Firewall Forensics

To complete this part of the assignment you need an account in a log appliance installed in the University's network. Please contact Kulesh (kulesh@isis) if you need an account. The appliance simply logs all the alerts from a firewall installed at the edge of the University's network. Looking at the appliance logs please answer the following questions:

1. What kind of events does the appliance log?
2. Identify the top 5 threats (IP addresses) to our network and the types of threats? (You will have to look at the historic data for these threats using the query interface)
3. Pick any two of the top 5 threats and setup an alert using the log appliance. Report the alerts you receive during the period.
4. Identify any port scan activity in the network. Justify your conclusion as to why you believe these are port scans.