CS 6542, Fall 2015
Lab 5 – Network Security
Due 11/18/2015 Before Class

Demonstrate mastery of the tools discussed in class by implementing the tests described in the following exercises.

> Please note, all pcap files should be created using the following syntax and command line options:
>
> tcpdump -s 0 -w username_homework5_lab#.pcap

Deliverables for each test are listed below the test description.

1) Create custom scan of network using the Arbor Atlas top 10 services and adding TCP 1337, 12345, 1 and UDP 1337 and 53. You may include or exclude UDP at your choice. You must use hping, netcat or libnet to perform these scans and tcpdump to capture the scan traffic. You may not use nmap or other prebuilt scanning tools.

   You must submit the commands and IPs used to accomplish the scan and the attendant pcap file.

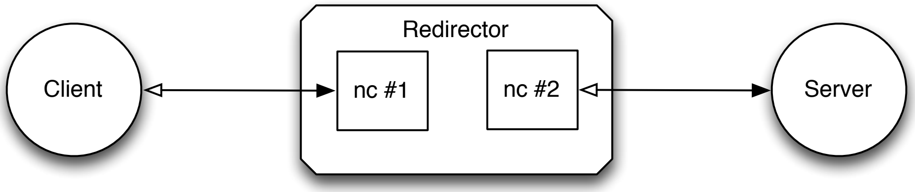
2) Determine and describe all ports that nmap attempts to access in a default scan. You may not simply quote the nmap man page or a webpage. For complete credit you must show the complete list of ports as described below and how you obtained it.

   Must submit the complete list of port/protocol pairs (e.g the table below - include all ports, not just open ports!), the

Proto	Port	Common Name
TCP	1	tcpmux
TCP	5	rje
...	...	
TCP	51206	

commands used to determine this information and the attendant pcap file.

3) Retrieve a webpage from a server redirecting through a netcat redirector (e.g. image below).



Must submit the commands, IPs used and attendant pcap file. For full points, pcap file must show both sides of the conversation, not just one side.

4) Write a program to generate and send 100 DNS query responses to 127.0.0.1 for a QType of A, a QClass of IN, for the domain z.tiwaz.net. The query responses should have random TxIDs and should also contain an authoritative NS glue record with the IP of 127.0.0.1.

You must submit your source code, a pcap file of traffic generated by your program, and a description of the traffic in the pcap.

***Hint**: Lookup the DNS specification. Run your network pcap capture from the same system as your program.

5) Evaluate the attached pcap (csci6542-signature-pcap-v1.pcap) to identify a pattern that can be used to *uniquely* identify this traffic. Once you have identified a potential pattern, create a valid snort signature or bro script to identify future instances of this traffic. The rules generated must uniquely identify the traffic - e.g. you may not simply match on the port and/or the source or destination IP addresses.

You must submit a description of your analysis, potential indicators discovered, and the rule(s) that you have written.

6) Optional (5 extra credit points). Determine the mechanism used to obfuscate the C&C traffic analyzed in the traffic identification (Snort/Bro rule) question. Provide the cleartext, un-obfuscated version of the data transferred.

You must submit any applicable source code, a description of the analysis process, and the un-obfuscated data transferred.

7) Optional (10 extra credit points). Write a program to monitor the network (on an interface set as promiscuous) for TCP traffic. When the program identifies a predefined string value it attempts to disrupt the TCP session.

You must submit your source code, a pcap file of traffic generated by your program, and a description of the traffic in the pcap.

8) Optional (10 extra credit points): Implement the DNS Man in the Middle attack discussed in the attached academic paper using libnet and libpcap.

Your code must listen for domain requests for two or more different domains that you specify (e.g. www.facebook.com, mail.google.com, …) and respond to the sender with a forged DNS response.

You must submit your source code, a pcap file of traffic generated by your program, and a description of the traffic in the pcap.