Offensive Network Security

Assignment 2
CIS 4930/5930
100 points
Due: 25 February 2014

1. Parse the Ethernet frame
    a. Label the different parts of the valid Ethernet frame (put DNE for a layer that is not used).
        i. Which bytes belong to the link-layer and what do they represent?
        ii. Which bytes belong to the network-layer and what do they represent?
        iii. Which bytes belong to the transport-layer and what do they represent?
        iv. Which bytes belong to the application-layer and what do they represent?
    b. Perform a reverse DNS lookup on the destination IP address. What is the returned PTR record?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
70	ca	9b	de	dd	00	a4	9c	0f	f5	c7	24	08	00	45	00
00	4c	00	01	00	00	40	11	ff	24	c0	a8	4b	3a	b8	16
b7	82	00	7b	00	7b	00	38	db	2c	1b	02	0a	00	00	00
00	00	00	00	00	00	7f	00	00	01	00	00	00	00	00	00
00	00	98	bf	2e	d2	00	00	00	00	00	00	00	00	00	00
00	00	ea	15	d9	fb	00	00	00	00						

2. Use `nping` to generate the following packet with specific `nping` options and send it to **three** remote servers of your choosing. Show the `nping` command that was used, and the results that were returned including what `nping` sent to the remote host. Is there a flag that is being sent that was not set by `nping` command-line values?
    a. TCP Probe mode
    b. TCP source port: 5567
    c. TCP destination port: your choosing
    d. TCP flags: RST, ACK
    e. TCP window size: 1

f. IP id: 31620

3. This question will survey the site `<URL emailed>`.
    a. What is the A record of the provided website?
    b. What is the PTR record of the returned A record? Is the PTR record the same as the provided website URL?
    c. Use `nmap` to run a TCP stealth-scan on the provided website. What ports are opened, filtered, and closed? For the filtered and closed ports, how is `nmap` determining the result? Try using `nping`, `Wireshark` (`tshark`), or `tcpdump` to see if nmap is using other packets to reach its conclusion. By default `nmap` does not display filtered and closed ports. Try changing the verbosity level to print these ports.
    d. Use `nmap` to run an OS detection on the site. What is the best guess for the OS?
    e. Use `ncat` to grab banners from the open ports. Does the port send a banner? If so what is the banner and can the service be determined by the banner? Does the returned banner indicate that `nmap` guessed correctly for the service?
    f. Are there any services that seem like they should **not** be facing the outside world?

4. This question is dedicated to searching http://www.shodanhq.com. List the search term used and the results found.
    a. Search for different `Content-Length` HTTP header request values (i.e. `Content-Length: 2890`)
    b. Choose another HTTP request header (http://en.wikipedia.org/wiki/List_of_HTTP_header_fields#Responses) and search for a specific value to see if Shodan returns any matches.
    c. What interesting services appeared in these results?

5. Home routers have been in the news recently due to backdoors being found by reversing the firmware. One such firmware allows a specific HTTP User-Agent full admin access to the router. Use http://www.shodanhq.com to search for routers vulnerable to this backdoor.
    a. Search value: “thttpd-alphanetworks/2.23 country: US”.
    b. The *magic* HTTP User-Agent: “xmlset_roodkcableoj28840ybtide”
    c. How many results were returned by shodan search?
    d. Make a HTTP request to the found IP without the *magic* HTTP User-Agent
    e. Make a HTTP request to the found IP with the *magic* HTTP User-Agent