# Offensive Network Security

Assignment 3
CIS 4930/5930
100 points
Due: 20 March 2014

1. The `nping` tool utilizes Echo Mode to allow users to see how packets change from host to remote machine. Use this option to answer the following questions. (Hint: read the man page section titled Echo Mode for `nping`)
    a. Does this option utilize a custom protocol defined by `nping`? If it does, what is it?
    b. Does this mode allow `nping` to act as a sniffer, a packet generator, or both?
    c. What information can a user determine, troubleshoot, or interpret by using this mode?
    d. Use the echo-client to determine the external IP of your WAN (only first two octets of IP)? Write the `nping` command used to determine this IP.

2. We've covered the use of the TCP stealth-scan (SYN flag set) but what happens if a user sends initial packets with other flags set (ACK, RST, PSH, URG, FIN, etc.)?
    a. Search Shodan for a variety of Operating Systems (search filter 'os'). Pick out a few IPs and make sure they have a web server running. Write all the shodan search queries used to locate these systems.
    b. Use Scapy to generate packets that perform different TCP scans to these systems. Write the code used to perform these scans.
    c. Did these systems return any error codes or packets to help determine if their ports are open?
    d. Does the TCP RPC (RFC 793) indicate that specific TCP flags should send back error messages?

3. Use Scapy to craft a packet to force a remote server to send an ICMP time-exceeded packets to a "spoofed" host.
    a. Write the Scapy code used to generate and send this packet.
    b. Will the attacker receive any confirmation of a successful attack?
    c. What rule of TCP is the attacker manipulating to perform this attack?

4. Use Scapy to generate the following packets.
    a. Create, send an NTP (Network Time Protocol) packet; capture the result (Choose a remote NTP server).
    b. Create, send, DHCP discover packet; capture the result (Perform on your LAN).
    c. Create, send, DNS A-record request to a remote DNS server; capture the result.

5. An attack was performed to determine which computers were talking to a video surveillance camera. It was determined that a computer at a security desk is polling this

camera for real-time images. The camera and computer utilize HTTP to send and receive images. Craft an attack using Scapy that will force the victim computer to **not** poll the camera but poll a separate computer.

a. Write this crafted attack used to fool the victim computer.
b. Can the attacker send spoofed images to the Victim computer pretending that the camera is still functioning properly?
c. An attack was utilized to determine which computers were talking to the camera. How was this attack performed? Use Scapy to craft a packet that will allow an attacker to determine which computers are talking to the camera without interrupting any communication between the camera and the devices.

| | | |
|---|---|---|
| Security desk computer | 192.168.23.56 | 12:55:A9:90:BB:00 |
| Surveillance Camera | 192.168.23.100 | 11:AA:BB:CC:22:00 |
| Attacker | 192.168.23.20 | 22:33:BC:CD:90:12 |