Network Security
6CCS3NSE / 7CCSMNSE

Prof. Luca Viganò

Department of Informatics
King's College London, UK

Second term 2017/18

Practicals 5

Nmap

In case you find a vulnerability (or something suspect), you should report it immediately to the lecturers.

- At the command prompt, type “nmap” and press Enter to see available nmap scan types and options.
- Browse `http://nmap.org` to get yourself acquainted with nmap.
- Which is the option to determine whether a host is online or not?
- Find out the Network Address of your machine and at command line, type “nmap -sP [Network Address].*” and press Enter.
  - * at the end of the network address means to scan every possible IP address on that network.
  - -sP option tells Nmap to only perform a ping scan (host discovery), then print out the available hosts that responded to the scan.
  - This will take some time, please be patient.
    You can press Enter to check the progress of the scan.

  Ask yourself whether possible problems might depend on your subnetwork.

- Now search 137.73.113.0/24 (NMS server subnet) and try to obtain as many informations as possible: open ports, OS and services versions.
- Try to look for web servers (TCP/80, TCP/443), pop3 (TCP/110) and Windows file services (TCP/445), for example.

  Run “nmap -sT -O <target-IP>”
- Run “nmap -sU -v <target-IP>”. What kind of scan is this?
- Now let’s look in detail at the operational behavior of nmap.

  Wireshark will reveal it, so run Wireshark (or tcpdump) in a window on the side.
- Recall the standard “3-way handshake” by which TCP establishes a fresh conversation with another machine. Client sends a packet with “syn” flag set, server sends back a packet with “syn” and “ack” flags set if the port is open, or with “rst” flag if not. To complete the connection, client confirms by sending a packet with “ack” set.
- “nmap -sT" is nmap’s TCP connect scan. Read its description in the nmap man page.

- Choose one of the ports that is open on the target computer and run nmap's connect scan against just that port. For example, if that's port 80, run "nmap -sT -p 80 <target-IP>".

  That causes a volley of 4 packets. Identify them in Wireshark and relate them to the 3-way handshake.

- nmap also has a version called TCP SYN scan, slightly different. Read its description in the nmap man page. Now run it against an open port, for example maybe port 80, if it's open:

  "nmap -sS -p 80 <target-IP>"

  This time there are 3 packets. For an open port, how would you describe the difference between the -sT and -sS scan versions in terms of normal TCP operation to start conversations?

- Now consider a port known to be closed and run both

  "nmap -sT -p <closedport> <target-IP>"

  "nmap -sS -p <closedport> <target-IP>"

  How many packets result from these? For a closed port, is there an operational difference between them?

- You can see that nmap's various scan types involve some minor but deliberate differences in behavior. These are designed to elicit different, known, responsive behavior from the target.
  - Possibly to identify the target operating system.
  - Or to minimize the likelihood of scan detection by the target, should it be running intrusion detection software.
- Look at the man page again: there are several scan variants you could try, e.g. -sN, -sF, -sX, -sA, -sW, -sM.
- Play with a couple of these a little. Take a look at the packets they generate and the results nmap reports when you run them.
- Perform operating system "fingerprinting":

  "nmap -O <target-IP>"
- Decoy scan:

  "nmap -sS -p 80 -D 207.192.16.206,66.158.250.44 <target-IP>"

  Read about decoy scans in the man page. Judging from what you captured in Wireshark, the target will experience contact from how many machines? What machines are they??
- Finally, browse `http://sectools.org`.