Module 20
(Service Discovery)

- At the end of this module, you should know a bit more about what typical services might be provided by a machine, how nmap discovers services, and where to get information on installing the OpenVAS network service auditing tool.
What are these Services?

• The services one would like to discover are provided by programs running on servers (devices running a service).

• A service will listen for incoming connections on a well-known port.

• When a connection is received, the service will satisfy both some application program interface (API) requirements likely specified by an Internet Engineering Task Force (IETF) Request for Comment (RFC). The RFCs specify how a client and server are to communicate.

• Taking ftp as an example, the ftp protocol is defined by RFCs. Any ftp server will provide access to manipulate the server's collection of files remotely from an internet client.
Is There a List of Services?

• You can find many of these. One such list is available at http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

• These are just lists of ports that are conventionally used for particular services.

• In fact, a machine can provide any service on any port in the range 1-65,535. (Port 0 is reserved and is usually used in programs to represent some arbitrarily selected available port, saving the programmer from having to write code to find an available port.)
Nmap Version Scanning

• Consider this scan:
  
  ```
  nmap -sS target.com -p 82
  ```

  vs. this scan:

  ```
  nmap -sV target.com -p 82
  ```

• In the first case, nmap uses a table to tell it the likely service on port 82. In the second case, nmap actually communicates with port 82 to figure out what service it's running.

• What happens if we try to do a banner grab on this machine?
One way to do a Banner Grab

- Use netcat on kali:
  
  nc 192.168.0.6 80

- No banner is immediately printed.

- Try some input. How about ? ?

- Response is interesting:
  
  HTTP/1.0 400 Bad Request
  Content-type: text/html
  Date: Tue, 17 Sep 2013 12:15:26 GMT
  Connection: close

  <HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD>
  <BODY><H1>400 Bad Request</H1>
  Unsupported method
  </BODY></HTML>

  .
What are the Most Common Services

- Fyodor gives this list:
  - 80 (http)
  - 25 (smtp)
  - 22 (ssh)
  - 443 (https)
  - 21 (ftp)
  - 113 (auth)
  - 23 (telnet)
  - 53 (domain)
  - 554 (rtsp)
  - 3389 (MS-Term-Server)
Automated Scanners

- Nessus, Nexpose, and OpenVAS are the most popular commercial network audit tools.
- If there is no need for stealth in a penetration, you can discover services (in particular vulnerable services) using these tools.
- Typically, these operate as client/server applications. The client asks the server to scan machines/networks/etc. The server does the scanning.
- Your Kali VM would normally act as both client and server. (You communicate to the server with a web browser.)
Set up OpenVAS on your Machine

- You can find an excellent tutorial on setting up OpenVAS at
  https://www.youtube.com/watch?v=0b4SVyP0lql

- Install OpenVAS on your kali VM.
- We'll start using it very soon.