**DNS**

* DNS server hold various kinds of records, most common of them are :
  + NS contains the authoritative server hosting the DNS records of a domain.
  + A contains the IP address
  + MX Mail Exchange record contains names of the server responsible for handling email for the domain.
  + PTR Pointer Records are used in reverse lookup zones and used to find the records associated with an IP.
  + CNAME
  + TXT
* **dnsrecon -d megacorpone.com -t axfr** Does all kinds of lookup for different records. Also checks for DNS zone transfer.
* **dnsrecon -d megacorpone.com –D filename.txt –t brt** brute forces subdomain based on the file provided.

**SCANNING**

* **IPTABLES :**
  + –I means input rule . INPUT/OUTPUT followed by the rule number.
  + –s/-d to specify source/destination address.
  + –j Accept to accept the traffic
  + –L to list all existing rules
* **NMAP :**
  + When sudo not used, nmap can’t use raw sockets hence will do connect scan ( Full 3-way handshake).
  + nmap --script-help dns-zone-transfer can be used to find out information about the NSE script.
* **NETBIOS:**
  + NetBios listens on 139/TCP and several other ports on UDP.
  + NetBios and SMB are two separate protocol.
  + NetBios is an independent session layer protocol and service that allows computers on local network to communicate with each other.
  + SMB modern implementation can work with/without netbios.
  + NetBios/TCP is required for backward compatibility and is often enabled together.
  + NBTSCAN can be used to identify NetBios information
  + sudo nbtscan -r 10.11.1.0/24, -r specifies the use of UDP 137 port.
* **SMB:**
  + nmap -v -p 139,445 --script=smb-vuln-ms08-067 --script-args=unsafe=1, this will definitely crash the targeted system.
  + Enum4linux to explore.
  + Smbclient to explore.
* **NFS :**
  + Both Portmapper and RPCbind run on TCP port 111. Both of them tie services to port and direct the client to the correct port number.
  + RPC process notify rpcbind when they start, registering the port they are listening on and the RPC program numbers they expect to serve.
  + mount -o nolock 10.11.1.72:/home ~/home/ , in the older version of NFS, -o nolock is used to disable file locking.
* **SMTP :** 
  + VRFY,EXPN commands can be used to identify login names from smtp server.
* **SNMP :**
  + UDP based protocol. Hence best for IP spoofing and stateless attacks.
  + SNMP 1,2,2c offers no encryption, hence credentials can be easily intercepted over local network.
  + The SNMP Management Information Base (MIB) is a database containing information usually related to network management.
  + The database is organized like a tree, where branches represent different organizations or network functions.
  + The leaves of the tree (final endpoints) correspond to specific variable values that can then be accessed, and probed, by an external user.
  + 1.3.6.1.2.1.25.1.6.0 System Processes
  + 1.3.6.1.2.1.25.4.2.1.2 Running Programs
  + 1.3.6.1.2.1.25.4.2.1.4 Processes Path
  + 1.3.6.1.2.1.25.2.3.1.4 Storage Units
  + 1.3.6.1.2.1.25.6.3.1.2 Software Name
  + 1.3.6.1.4.1.77.1.2.25 User Accounts
  + 1.3.6.1.2.1.6.13.1.3 TCP Local Ports
  + Onesixtyone –c <file-to-use> -I IPs, can be used to brute force community string.
  + Snmpwalk –c public –v<specif-version-of-snmp> -t IP , Snmpwalk attempts to enumerate all the MIBs using the provided community string.
  + snmpwalk -c public -v1 10.11.1.14 1.3.6.1.4.1.77.1.2.25, enumerate windows users.
  + snmpwalk -c public -v1 10.11.1.73 1.3.6.1.2.1.25.4.2.1.2, enumerate windows process.
  + snmpwalk -c public -v1 10.11.1.14 1.3.6.1.2.1.6.13.1.3, enumerate open TCP ports.
  + snmpwalk -c public -v1 10.11.1.50 1.3.6.1.2.1.25.6.3.1.2, enumerate installed software
  + snmpcheck is similar to snmpwalk.