DNS Enumeration:

DNSRECON:

syntax: root @kali~# dnsrecon -t <type of record> -d <domain name>

DNS dictionary attack

syntax : root@kali~# atk6-dnsdict -d46 <domain name>

it'll have a wordfile with 1400+ words in it and will try to gather information about that domain.

DNS enumeration with Fierce :

syntax: root@kali~# fierce -dns <domain name>

this is similar to DNSDICT attack but you have 2280 key words in the database to resolve the DNS queries.

CRUNCH:

Syntax: root@kali~# crunch <min word length> <max word length> <parameters/options> -o <file name/ path with filename>

to create a random wordlist file with given parameters

CUPP:

Common User Passwords Profiler

open a browser go with github.com

search for CUPP and open up mebus/CUPP (a tool that runs on python)

click on clone or download (copy the link shown by clicking on the clip board)

open a new terminal and use the command

root@kali~# git clone <the link you copied earlier>

navigate into the directory that's cloned.

root@kali~# python3 cupp.py -i

follow on screen instructions.

Installing NESSUS

Open browser go with nessus home download on a google search

find tennable website and locate the downloads tab.

in downloads find NESSUS

find for suitable operating system and download the file

if in kali linux:
root@kali~# dpkg -i <Nessus File Name>

root@kali~# service nessusd start

open a browser go with https://127.0.0.1:8834 (because Nessus runs on port 8834)

for the first time accept the security risk and proceed to the site.

install nessus essesntials using onscreen commands. (Use trashmail if possible)

How to use Nessus

In next class