July,2021

HAcker Playbook Labs

# Setting up Kali

### Passwd – chage default password

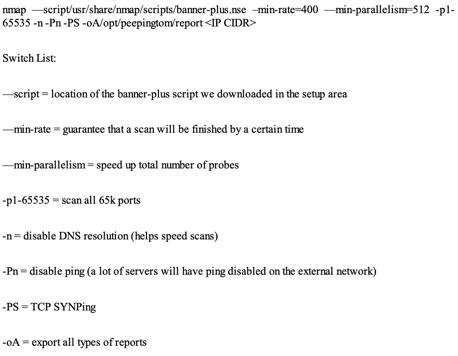
### Apt-get update

### Apt-get dist-upgrade

# Passive Discovry

* Cd /opt
* git clone https://github.com/leebaird/discover.git
* ./discover.sh
* DOMAIN \_ PASSIVE \_ exemple.com
* if you need to dive deeper **Recon-ng**
* firefox/root/[domain]/index.htm

# Active Discovry

* Network Scanning
  1. OPENVAS
  2. NMAP(OS AND SERVICE SCANNER)
     + Quick scan for all ports
     + Scan differences
     + Scan script(The banner-plus.nse will be used for quicker scanning and smarter identification)
     + cd/usr/share/nmap/scripts/
     + wget https://raw.github.com/hdm/scan-tools/master/nse/banner-plus.nse

nmap —script/usr/share/nmap/scripts/banner-plus.nse –min-rate=400 —min-parallelism=512 -p1- 65535 -n -Pn -PS -oA/opt/peepingtom/report <IP CIDR>

* 1. Screen Capturing PeepingTom for taking snapshot (check <https://bitbucket.org/LaNMaSteR53/peepingtom/src/master>)

cat report.gnmap | ./gnmap.pl | grep http | cut -f 1,2 -d “,”| tr “,” “:” > http\_ips.txt

create a list of ip addresses from the last nmap result

check <https://github.com/Rainism/peepingtom/blob/master/README>