PROOF OF CONCEPT

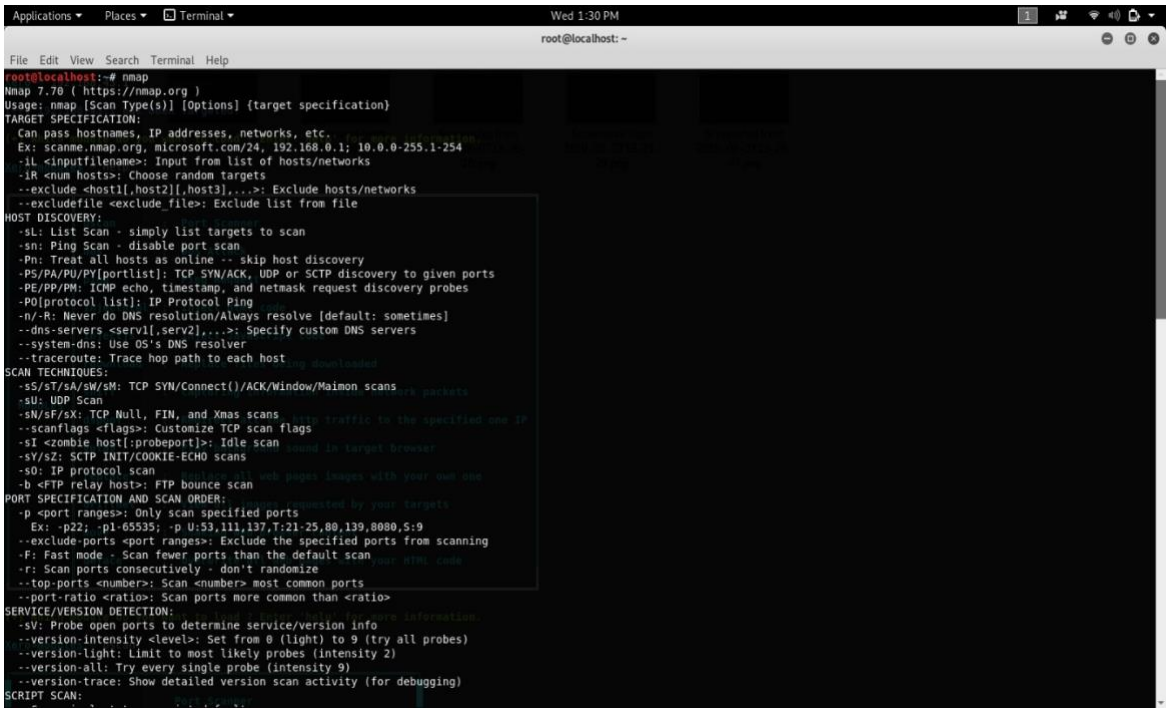
By V.R.Devanand 181MC117

Nmap: Nmap or Network Mapper is a free and open source built-in tool in Kali Linux which allows us to map the users in our network and consists of various utilities such as host discovery, operating system detection, service detection etc..

Nmap is a pre-installed tool in Kali Linux and thus doesn't require installation

To launch Nmap just type nmap in terminal

Major arguments/commands in Nmap:



-p --> port

--top-ports -->scans for top ports

-iL --> read from txt file

-O --> os detection

-sV --> service detection

-sT --> send tcp packets

-sS --> send tcp SYN (half open scanning)

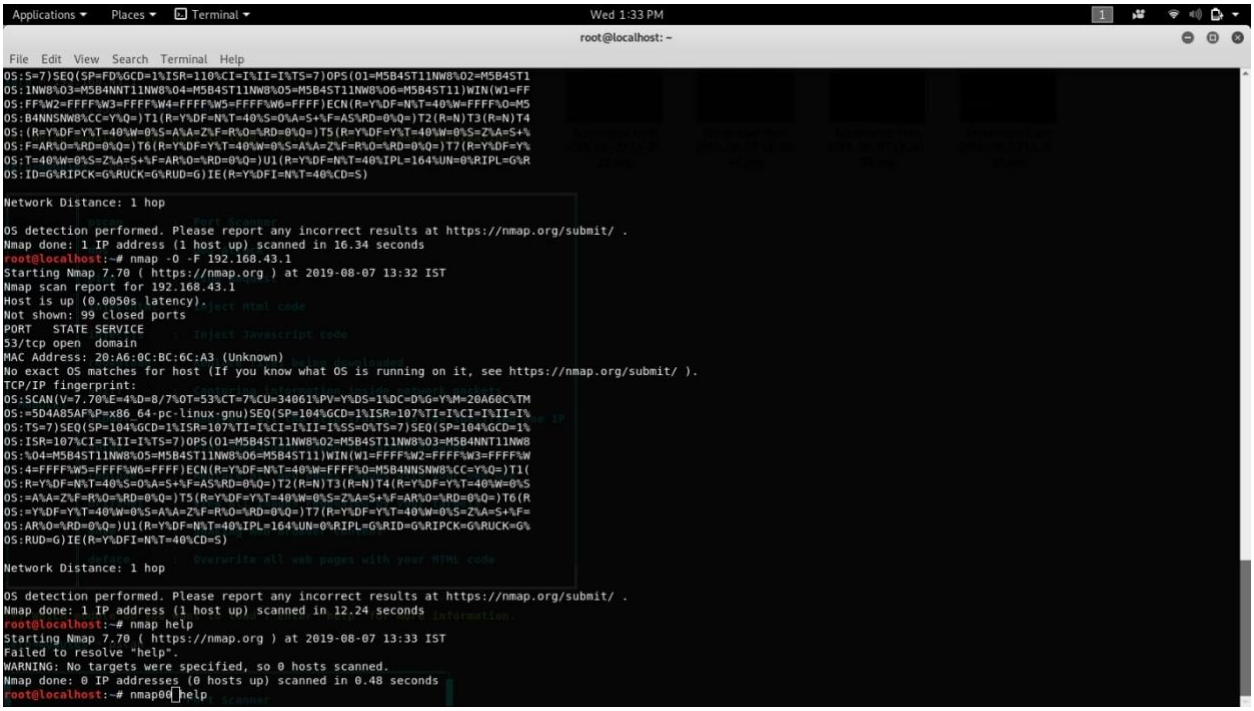
-sU --> send udp packets

--script --> use its scripting engine.

-A --> aggressive scan (os detection,version detection)

Usage: nmap -arguments (victims' ip)

By this way Nmap is used as a Information gathering tool to find the



vulnerabilities in victims' machine to use the apt exploits.