Act 3

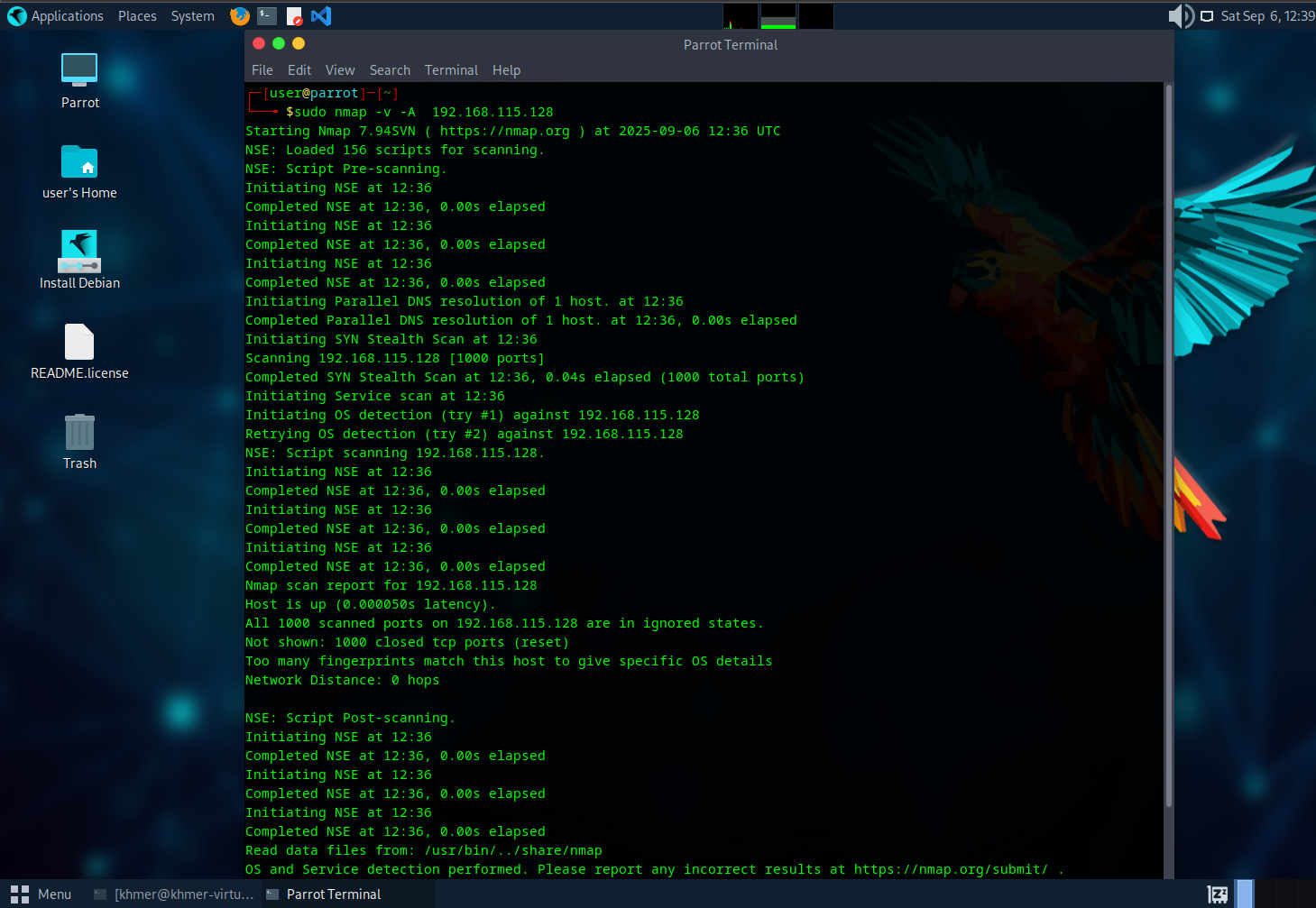
Q1. Notice the open ports on all 3 devices (the attacker notebook, the target

notebook, and the target Linux VM). Does anything look suspicious, i.e., some ports

that you are not aware of that are open on the VM or on your notebooks?

ANS

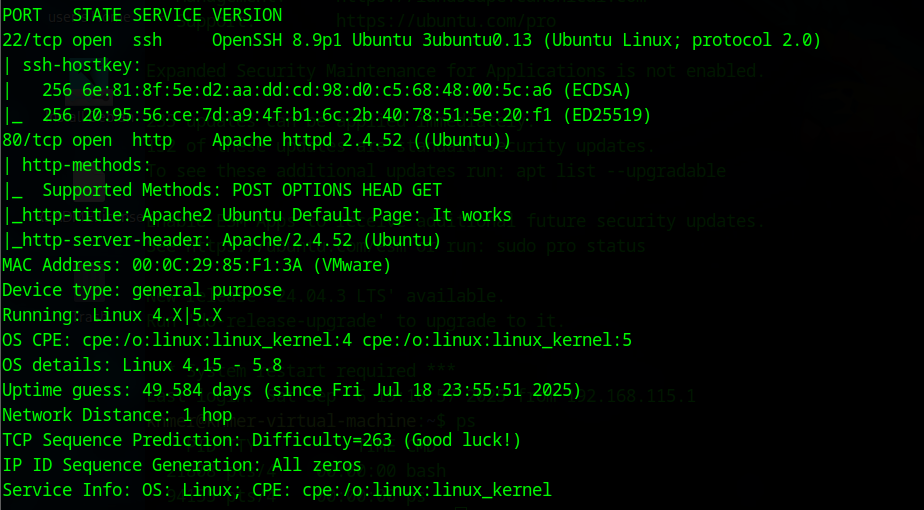
Attacker: *all ports closed*.



Target VM: Open ports: 22/tcp (SSH) and 80/tcp (Apache). Running Linux

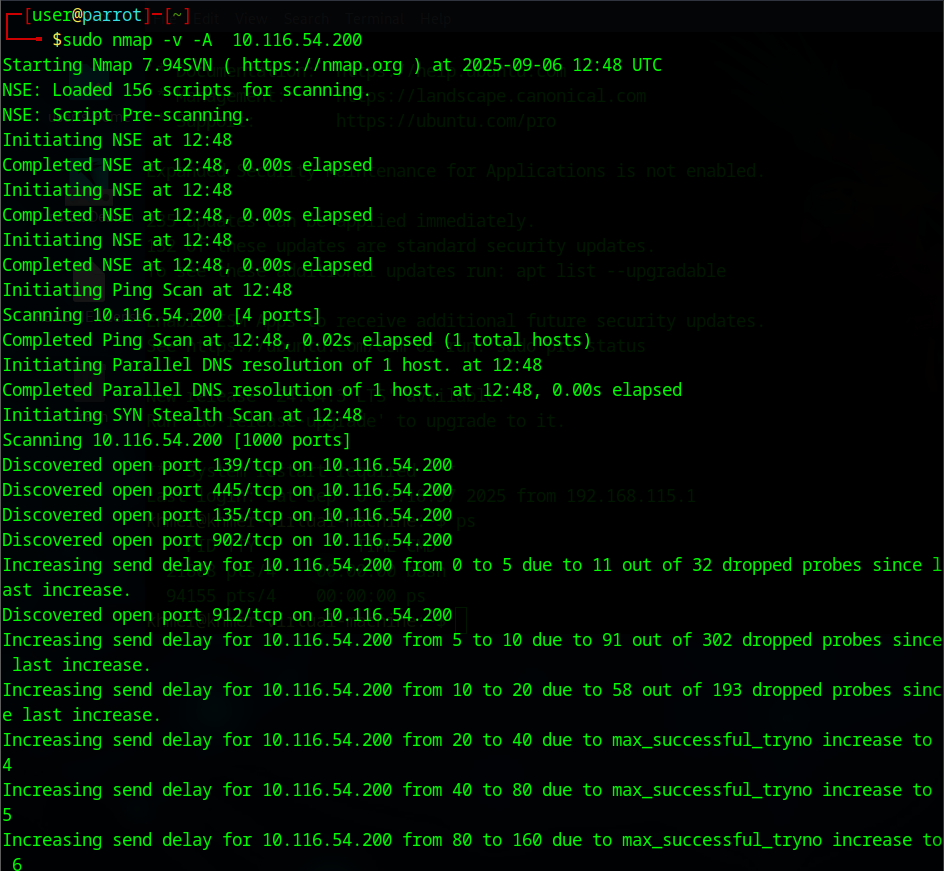








Target notebook: port 139, 445, 135 opened (These are Windows services (SMB, RPC, etc.).)



Q2. Look at the information provided by nmap about your OS's on all 3 devices. Is

the information correct? Why is it or why is it not correct?

ANS Yes. The information is correct.Nmap can guess the information of the target from the target’s response and using Nmap’s database(Nmap has a **database** of known OS fingerprints. Each entry in this database contains the characteristic responses of a particular OS. Nmap compares the observed responses from the target against this database.)

Q3. What do you think about the information you can get using nmap? Scary?

ANS - nmap can reveal: Which ports are open, Which services are running, Software versions,

Sometimes even the OS type.

- Yes, attacker can identify possible attack points from the information.

Q4. Look at the access.log file for the web server in your Linux VM. What IP

addresses do you see accessing the web server? Which devices do these IP addresses

belong to?  
ANS 192.168.115.134 is target notebook VM, 192.168.115.128 is attacker notebook.

Q5. Find the nmap scan in the web server log. Copy the lines from the log file that

were created because of the nmap scan.

ANS

khmer@khmer-virtual-machine:/var/log/apache2$ cat access.log

192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:130.0) Gecko/20100101 Firefox/130.0"

192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:130.0) Gecko/20100101 Firefox/130.0"

192.168.115.134 - - [06/Sep/2025:19:13:26 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:130.0) Gecko/20100101 Firefox/130.0"

192.168.115.134 - - [06/Sep/2025:19:15:31 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:130.0) Gecko/20100101 Firefox/130.0"

192.168.115.134 - - [06/Sep/2025:19:15:31 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.115.134/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:130.0) Gecko/20100101 Firefox/130.0"

192.168.115.128 - - [06/Sep/2025:19:32:31 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /nmaplowercheck1757161953 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "PYOW / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:32:33 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:42 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /nmaplowercheck1757162383 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "SZTO / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:39:43 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:05 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /nmaplowercheck1757162886 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "KBCU / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:19:48:06 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:34 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /nmaplowercheck1757166995 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PEEZ / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:20:56:35 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

Result of iptables -L  
root@khmer-virtual-machine:~# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

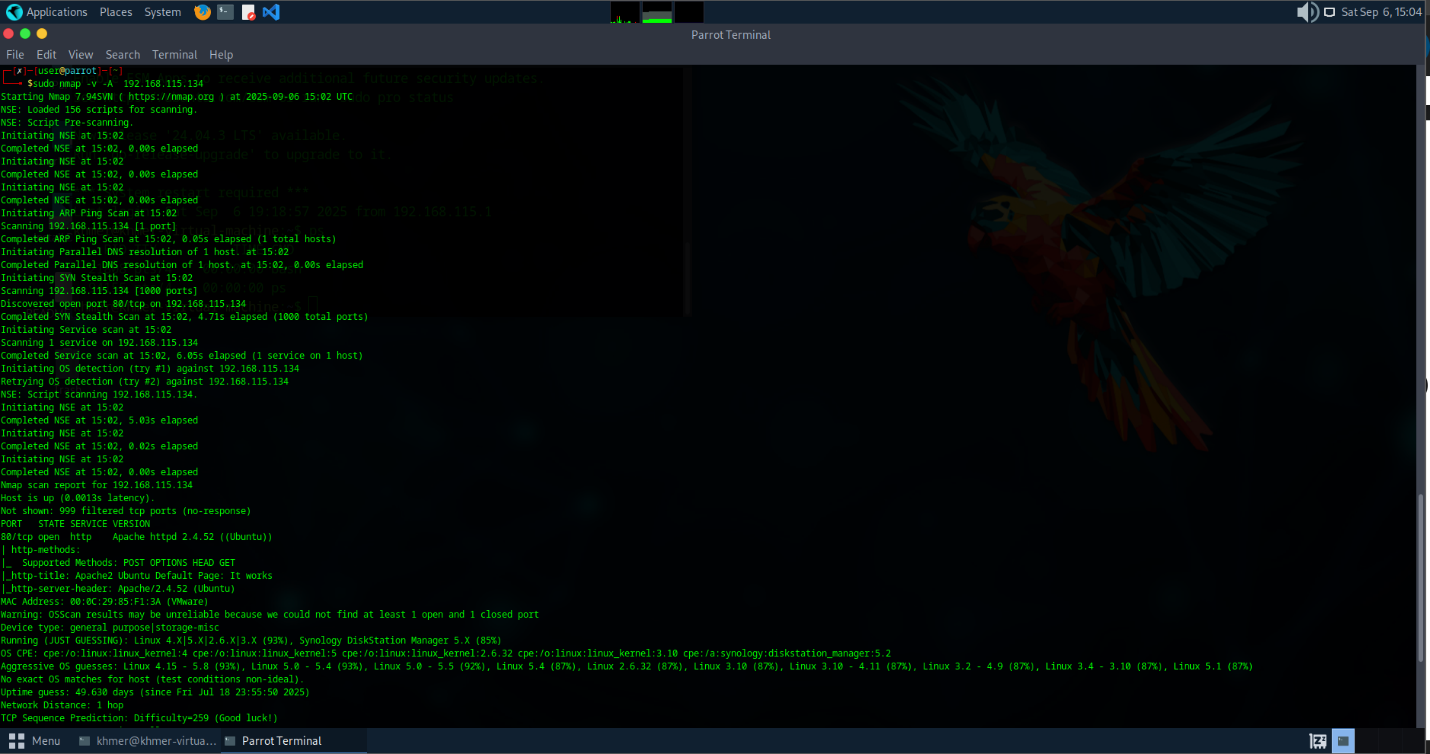
Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Q6. After you successfully install your iptable rule(s), how do the reported results

from your new nmap scan compare to your previous scan before using iptables?

Look to see if OS detection, port open results, etc. have changed. Something(s) have

definitely changed.  
ANS found only port 80 and OS(but just guessing) look at the arrows.



Q7. Notice that nmap can still figure out you have Apache httpd running. Look at

the access.log file for the web server in your Linux VM. Are the logs the same as in

Part II?

ANS nmap can still figure out. No the logs are not the same as in PartII.

192.168.115.128 - - [06/Sep/2025:22:02:43 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "POST /sdk HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /nmaplowercheck1757170967 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /.git/HEAD HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /robots.txt HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "POST / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "SGWI / HTTP/1.1" 501 500 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "PROPFIND / HTTP/1.1" 405 525 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /favicon.ico HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET /evox/about HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "GET / HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:47 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:48 +0700] "OPTIONS / HTTP/1.1" 200 181 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"

192.168.115.128 - - [06/Sep/2025:22:02:52 +0700] "GET / HTTP/1.0" 200 10945 "-" "-"

192.168.115.128 - - [06/Sep/2025:22:02:52 +0700] "GET / HTTP/1.1" 200 10926 "-" "-"

Q8. Explain whether or not you could prevent nmap from reaching the web server

while still allowing legitimate clients to get service. Will a firewall be sufficient for

this? Or do you need some other device? Please think critically about this.

ANS

You can't fully prevent Nmap from reaching an open web server while still allowing legitimate clients. A basic firewall isn't enough for this task.

A firewall like **iptables** works at a low level, filtering traffic based on port and protocol. THe rule to allow web traffic on port 80 opens a path for anyone. Since Nmap's reconnaissance probes use the same protocol as a regular web browser, the firewall lets them through.

To block Nmap's specific probing behavior, you need a more advanced security tool, like a **Web Application Firewall (WAF)**. A WAF inspects the actual content of the HTTP requests, allowing it to detect and block suspicious patterns and methods that a standard browser wouldn't use.  
  
Q9. What are your firewall rules? Run iptables -L on your VM and enter the output

here.  
ANS

