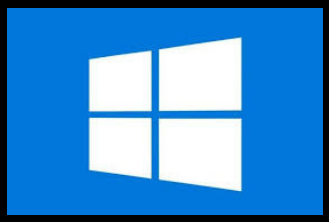
MAJOR PROJECT

CYBER SECURITY COURSE (VERZO)

NAME : PRAMOTH K J
E MAIL : PRAMOTHKJ751@GMAIL.COM

SCANNING MODULE USING NMAP TOOL

HACKER MACHINE : WINDOWS 10

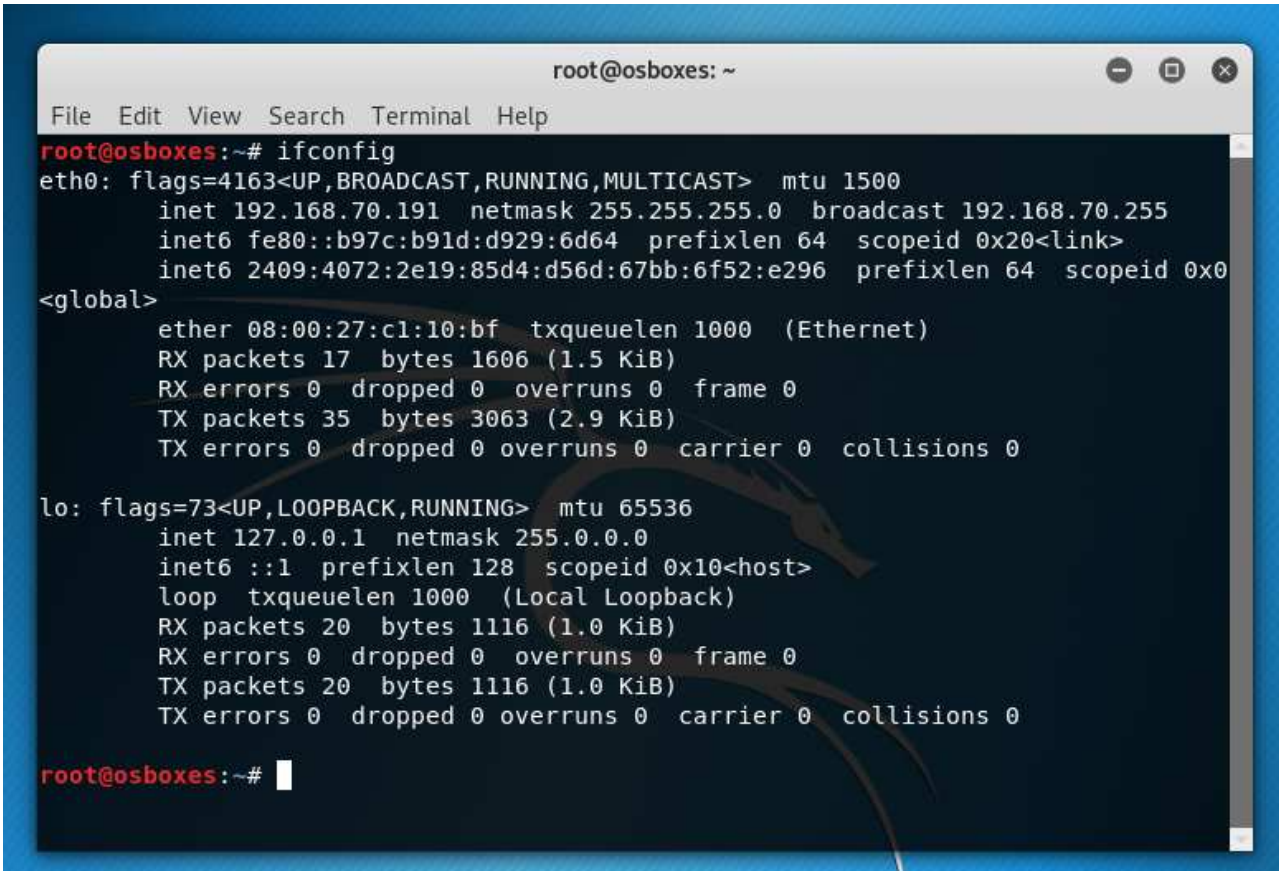


VICTIM MACHINE : KALI LINUX & WINDOWS 7

1.VICTIM MACHINE : KALI LINUX

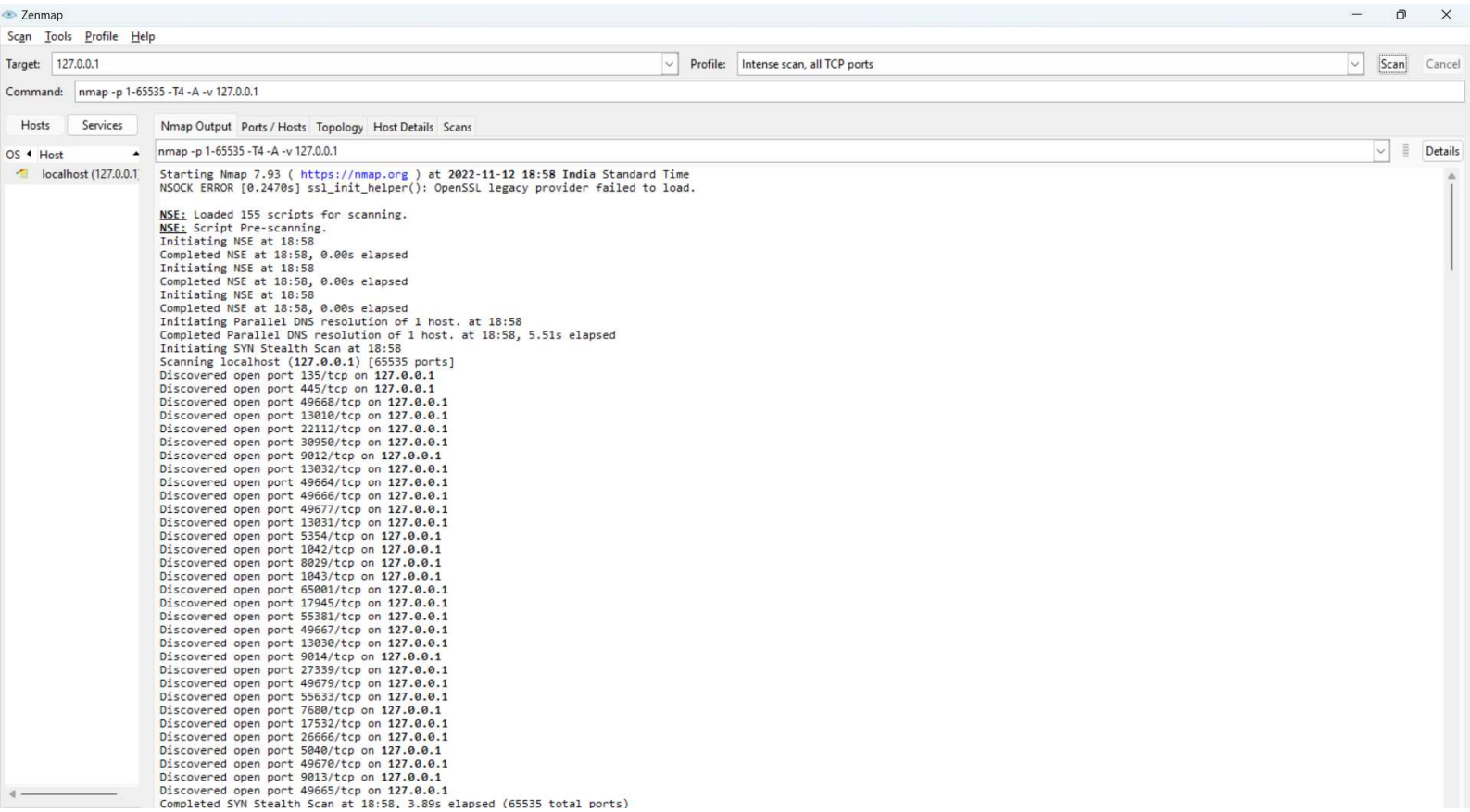
STEP 1:

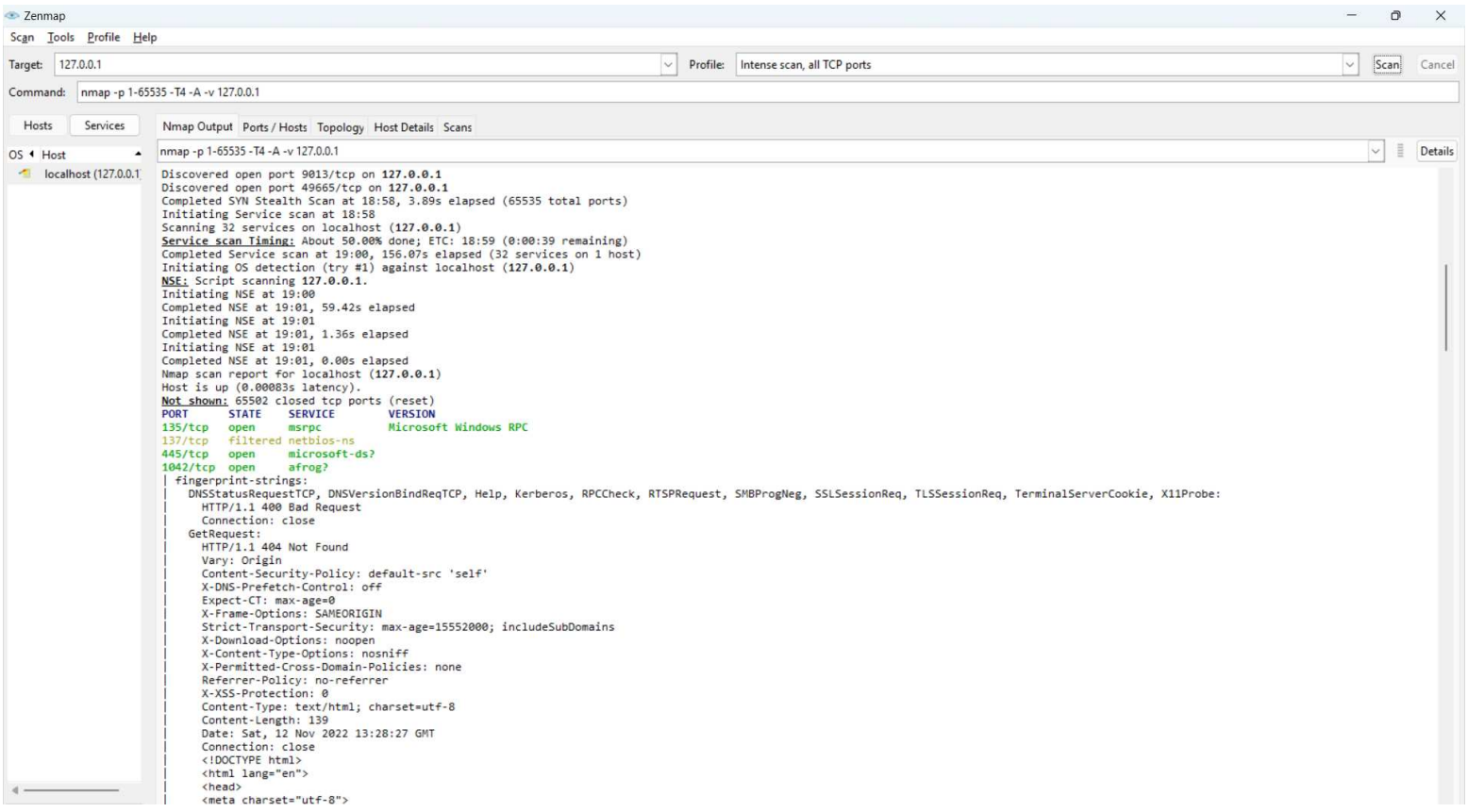
GET THE IP ADDRESS USING TERMINAL

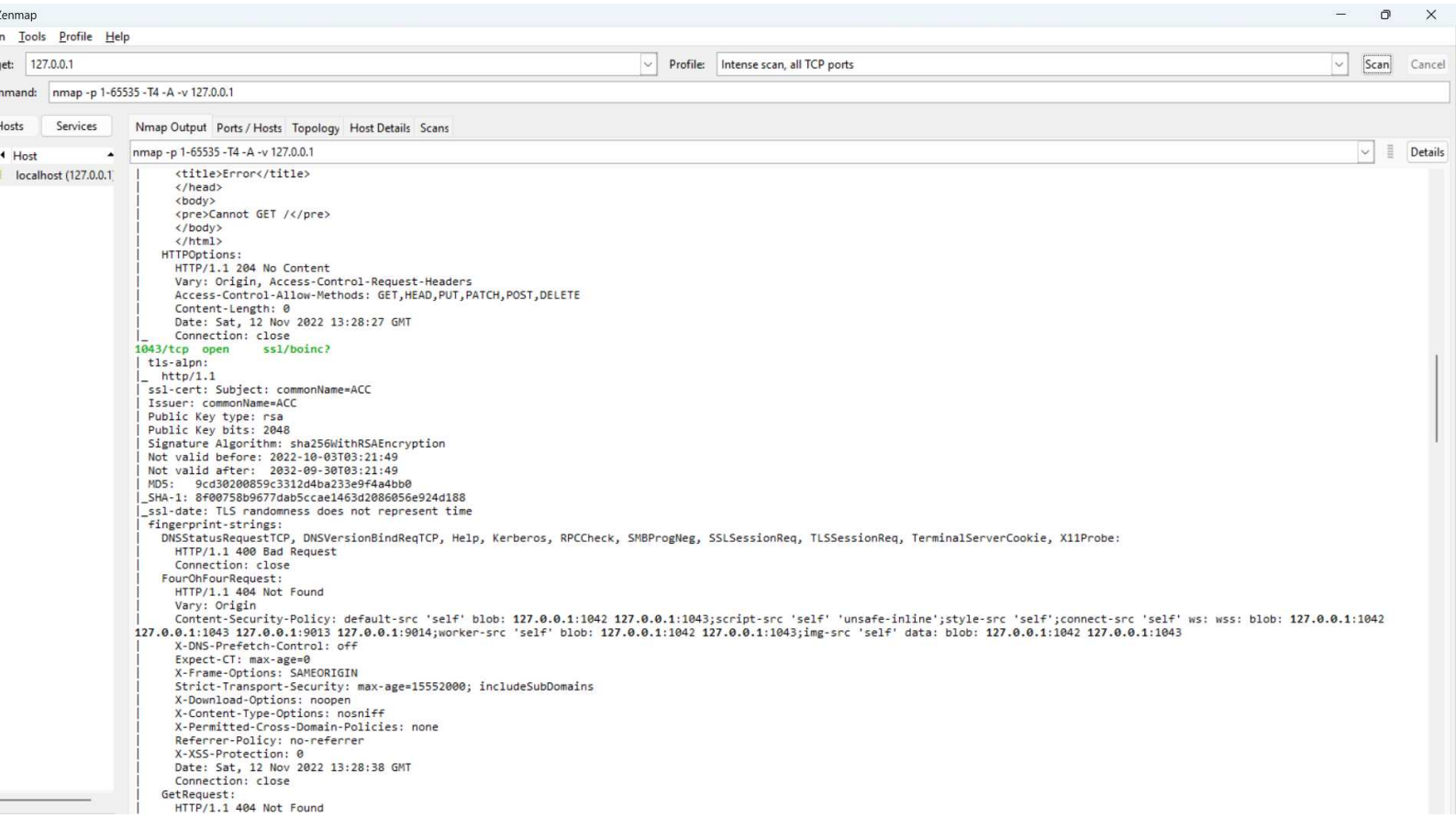


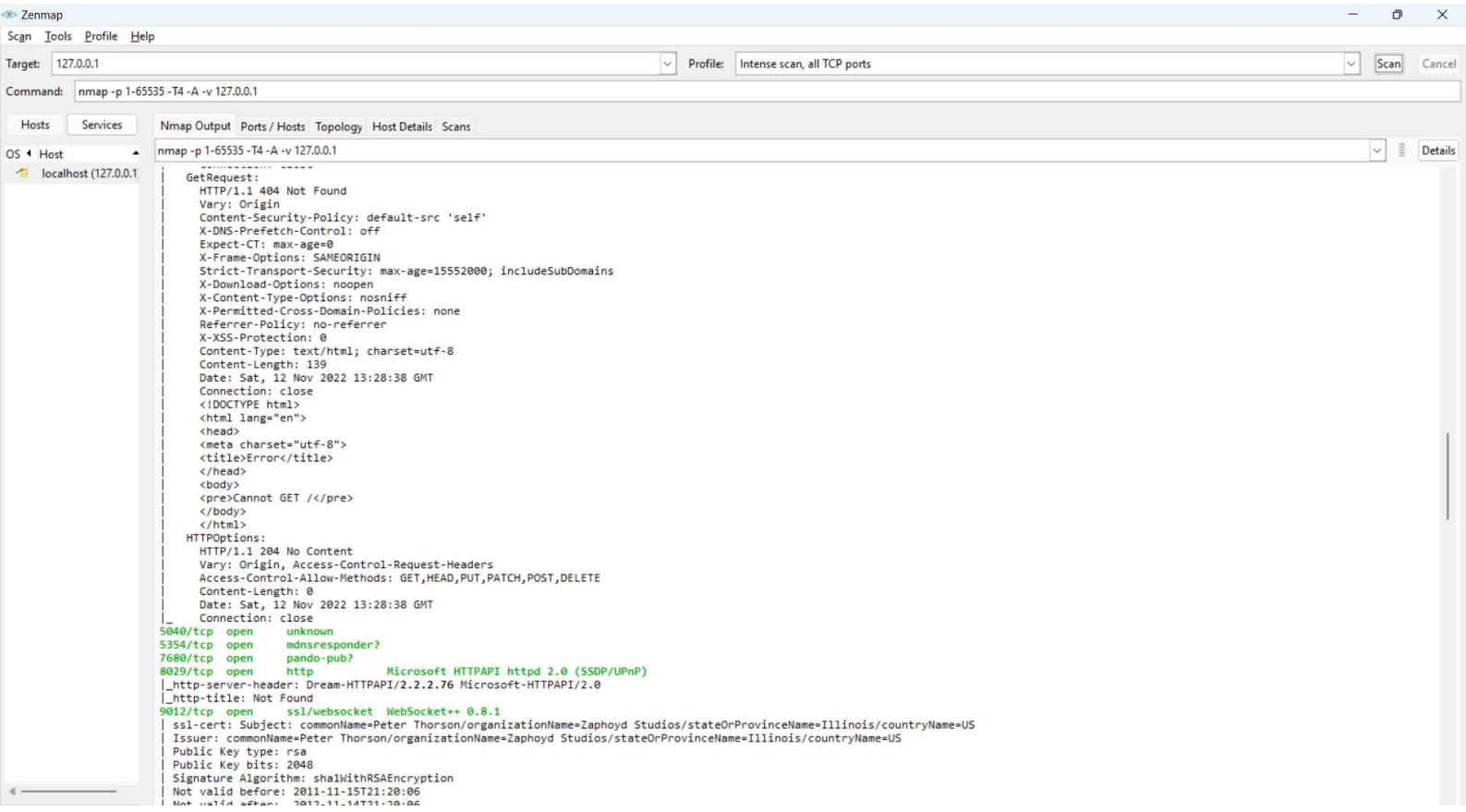
STEP 2:

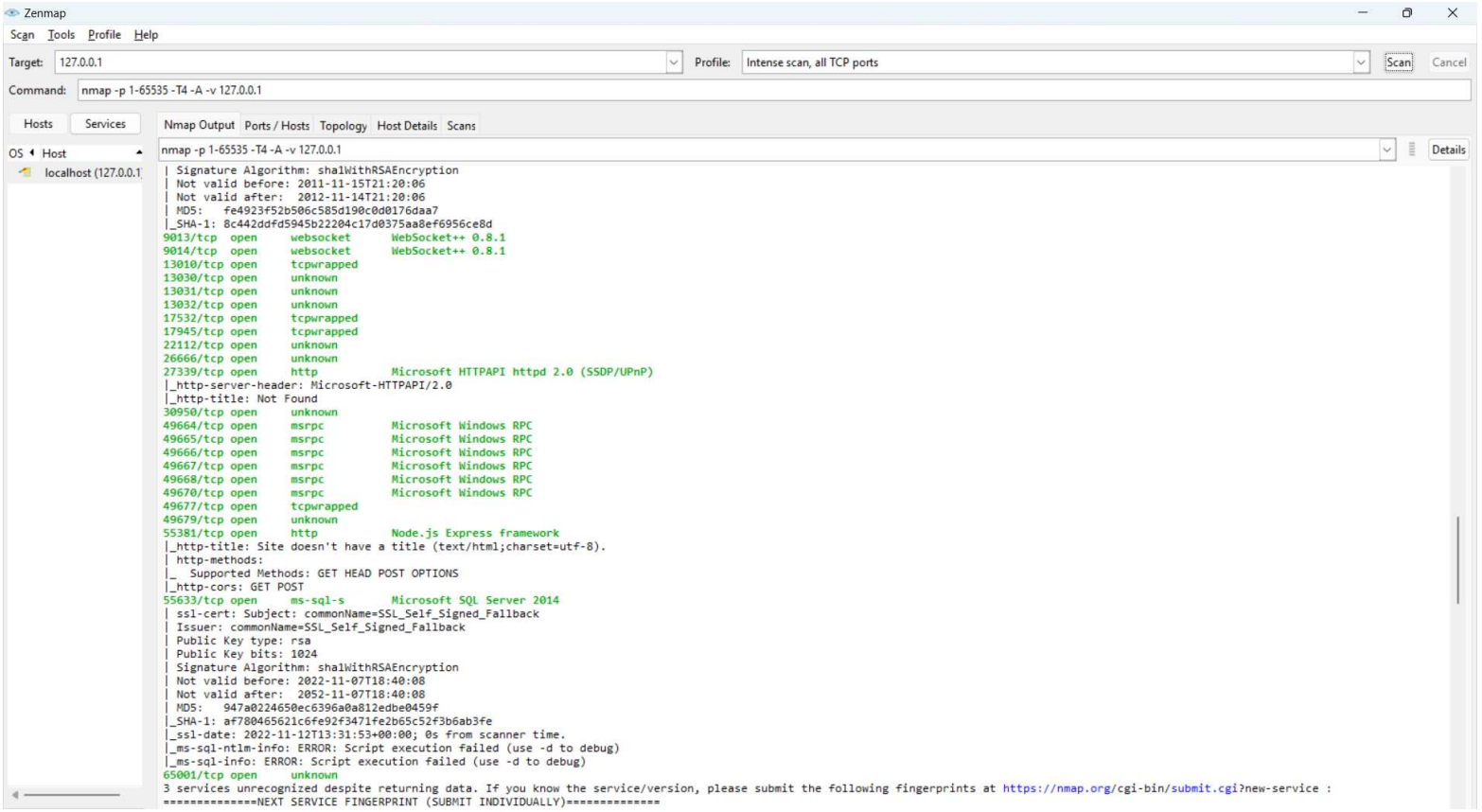
USING NMAP I WILL PRESENT THE SCREENSHOTS BELOW

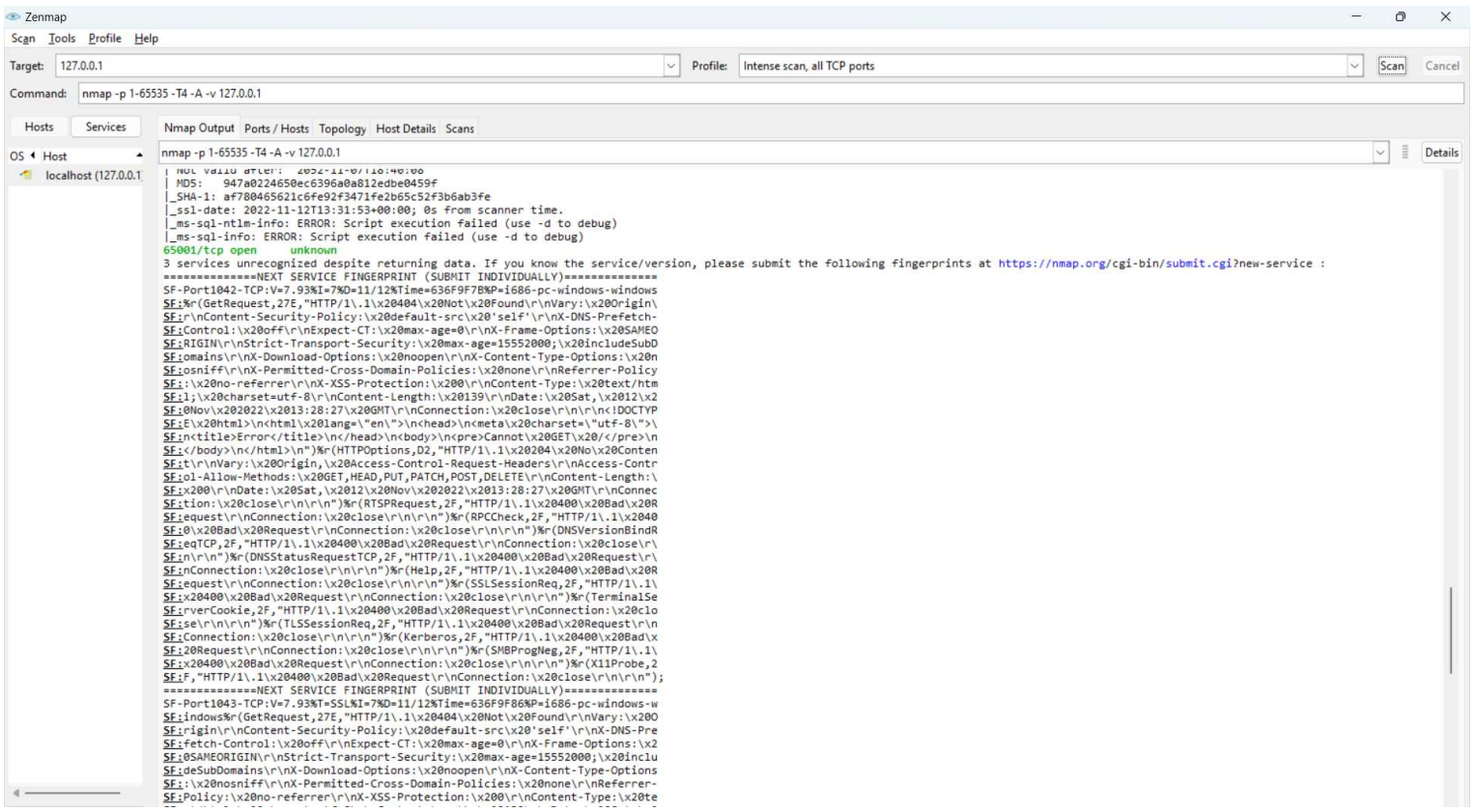

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
localhost (127.0.0.1)
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
Starting Nmap 7.93 (https://nmap.org) at 2022-11-12 18:58 India Standard Time
NSOCK ERROR [0.2470s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating NSE at 18:58
Completed NSE at 18:58, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:58
Completed Parallel DNS resolution of 1 host. at 18:58, 5.51s elapsed
Initiating SYN Stealth Scan at 18:58
Scanning localhost (127.0.0.1) [65535 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 49668/tcp on 127.0.0.1
Discovered open port 13010/tcp on 127.0.0.1
Discovered open port 22112/tcp on 127.0.0.1
Discovered open port 30950/tcp on 127.0.0.1
Discovered open port 9012/tcp on 127.0.0.1
Discovered open port 13032/tcp on 127.0.0.1
Discovered open port 49664/tcp on 127.0.0.1
Discovered open port 49666/tcp on 127.0.0.1
Discovered open port 49677/tcp on 127.0.0.1
Discovered open port 13031/tcp on 127.0.0.1
Discovered open port 5354/tcp on 127.0.0.1
Discovered open port 1042/tcp on 127.0.0.1
Discovered open port 8029/tcp on 127.0.0.1
Discovered open port 1043/tcp on 127.0.0.1
Discovered open port 65001/tcp on 127.0.0.1
Discovered open port 17945/tcp on 127.0.0.1
Discovered open port 55381/tcp on 127.0.0.1
Discovered open port 49667/tcp on 127.0.0.1
Discovered open port 13030/tcp on 127.0.0.1
Discovered open port 9014/tcp on 127.0.0.1
Discovered open port 27339/tcp on 127.0.0.1
Discovered open port 49679/tcp on 127.0.0.1
Discovered open port 55633/tcp on 127.0.0.1
Discovered open port 7680/tcp on 127.0.0.1
Discovered open port 17532/tcp on 127.0.0.1
Discovered open port 26666/tcp on 127.0.0.1
Discovered open port 5040/tcp on 127.0.0.1
Discovered open port 49670/tcp on 127.0.0.1
Discovered open port 9013/tcp on 127.0.0.1
Discovered open port 49665/tcp on 127.0.0.1
Completed SYN Stealth Scan at 18:58, 3.89s elapsed (65535 total ports)

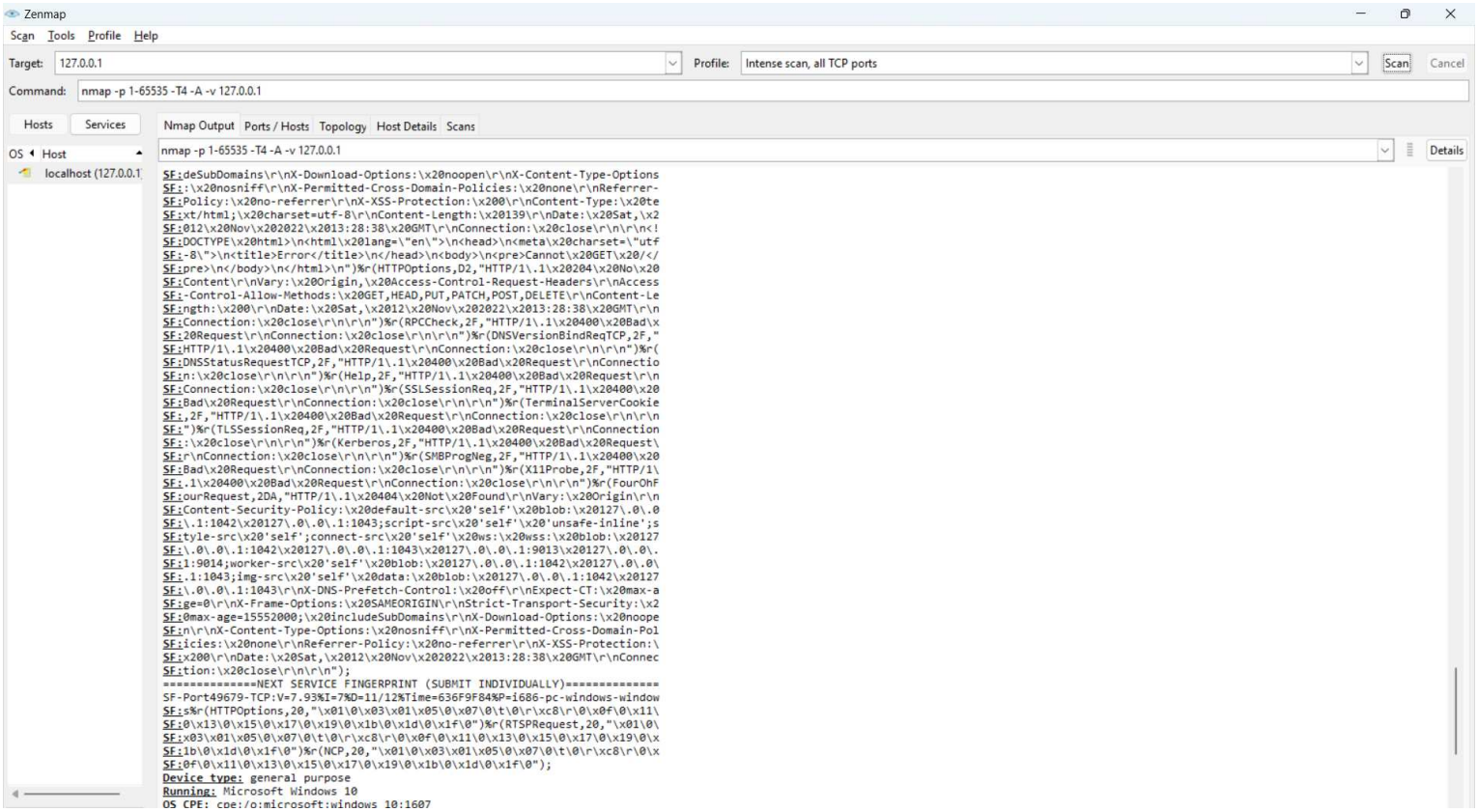

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
localhost (127.0.0.1)
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
Discovered open port 9013/tcp on 127.0.0.1
Discovered open port 49665/tcp on 127.0.0.1
Completed SYN Stealth Scan at 18:58, 3.89s elapsed (65535 total ports)
Initiating Service scan at 18:58
Scanning 32 services on localhost (127.0.0.1)
Service scan Timing: About 50.00% done; ETC: 18:59 (0:00:39 remaining)
Completed Service scan at 19:00, 156.07s elapsed (32 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 19:00
Completed NSE at 19:01, 59.42s elapsed
Initiating NSE at 19:01
Completed NSE at 19:01, 1.36s elapsed
Initiating NSE at 19:01
Completed NSE at 19:01, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00083s latency).
Not shown: 65502 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
137/tcp filtered netbios-ns
445/tcp open microsoft-ds?
1042/tcp open afrog?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, RPCCheck, RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
| HTTP/1.1 400 Bad Request
| Connection: close
| GetRequest:
| HTTP/1.1 404 Not Found
| Vary: Origin
| Content-Security-Policy: default-src 'self'
| X-DNS-Prefetch-Control: off
| Expect-CT: max-age=0
| X-Frame-Options: SAMEORIGIN
| Strict-Transport-Security: max-age=15552000; includeSubDomains
| X-Download-Options: noopen
| X-Content-Type-Options: nosniff
| X-Permitted-Cross-Domain-Policies: none
| Referrer-Policy: no-referrer
| X-XSS-Protection: 0
| Content-Type: text/html; charset=utf-8
| Content-Length: 139
| Date: Sat, 12 Nov 2022 13:28:27 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">

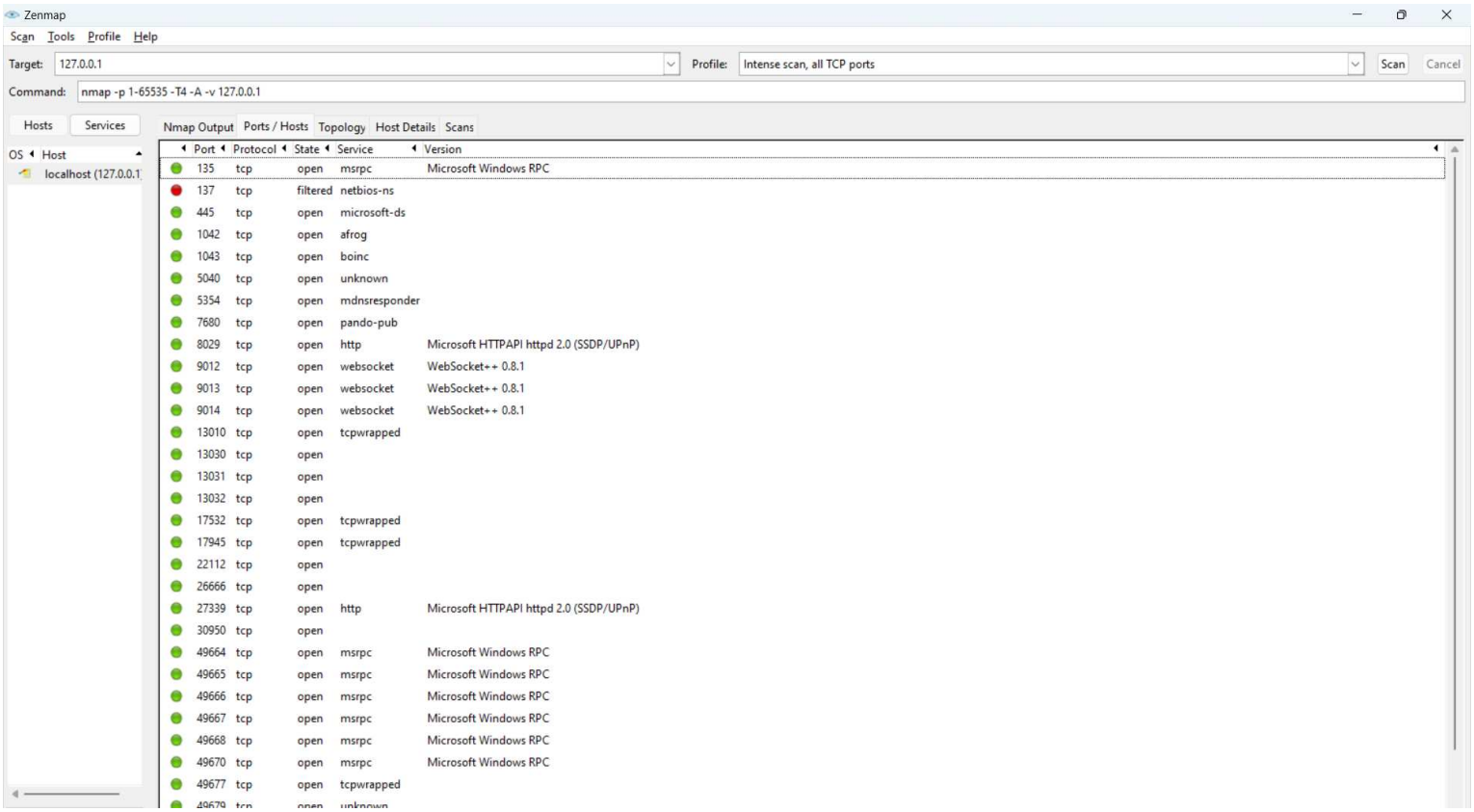

Zenmap
n Tools Profile Help
get: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan
Cancel
mmand: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Host
localhost (127.0.0.1
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot GET /</pre>
| </body>
| </html>
| HTTPOptions:
| HTTP/1.1 204 No Content
| Vary: Origin, Access-Control-Request-Headers
| Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
| Content-Length: 0
| Date: Sat, 12 Nov 2022 13:28:27 GMT
|_ Connection: close
1043/tcp open ssl/boinc?
| tls-alpn:
|_ http/1.1
| ssl-cert: Subject: commonName=ACC
| Issuer: commonName=ACC
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-10-03T03:21:49
| Not valid after: 2032-09-30T03:21:49
| MD5: 9cd30200859c3312d4ba233e9f4a4bb0
|_SHA-1: 8f00758b9677dab5ccae1463d2086056e924d188
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
| HTTP/1.1 400 Bad Request
| Connection: close
| FourOhFourRequest:
| HTTP/1.1 404 Not Found
| Vary: Origin
| Content-Security-Policy: default-src 'self' blob: 127.0.0.1:1042 127.0.0.1:1043;script-src 'self' 'unsafe-inline';style-src 'self';connect-src 'self' ws: wss: blob: 127.0.0.1:1042 127.0.0.1:1043 127.0.0.1:9013 127.0.0.1:9014;worker-src 'self' blob: 127.0.0.1:1042 127.0.0.1:1043;img-src 'self' data: blob: 127.0.0.1:1042 127.0.0.1:1043
| X-DNS-Prefetch-Control: off
| Expect-CT: max-age=0
| X-Frame-Options: SAMEORIGIN
| Strict-Transport-Security: max-age=15552000; includeSubDomains
| X-Download-Options: noopen
| X-Content-Type-Options: nosniff
| X-Permitted-Cross-Domain-Policies: none
| Referrer-Policy: no-referrer
| X-XSS-Protection: 0
| Date: Sat, 12 Nov 2022 13:28:38 GMT
| Connection: close
| GetRequest:
| HTTP/1.1 404 Not Found

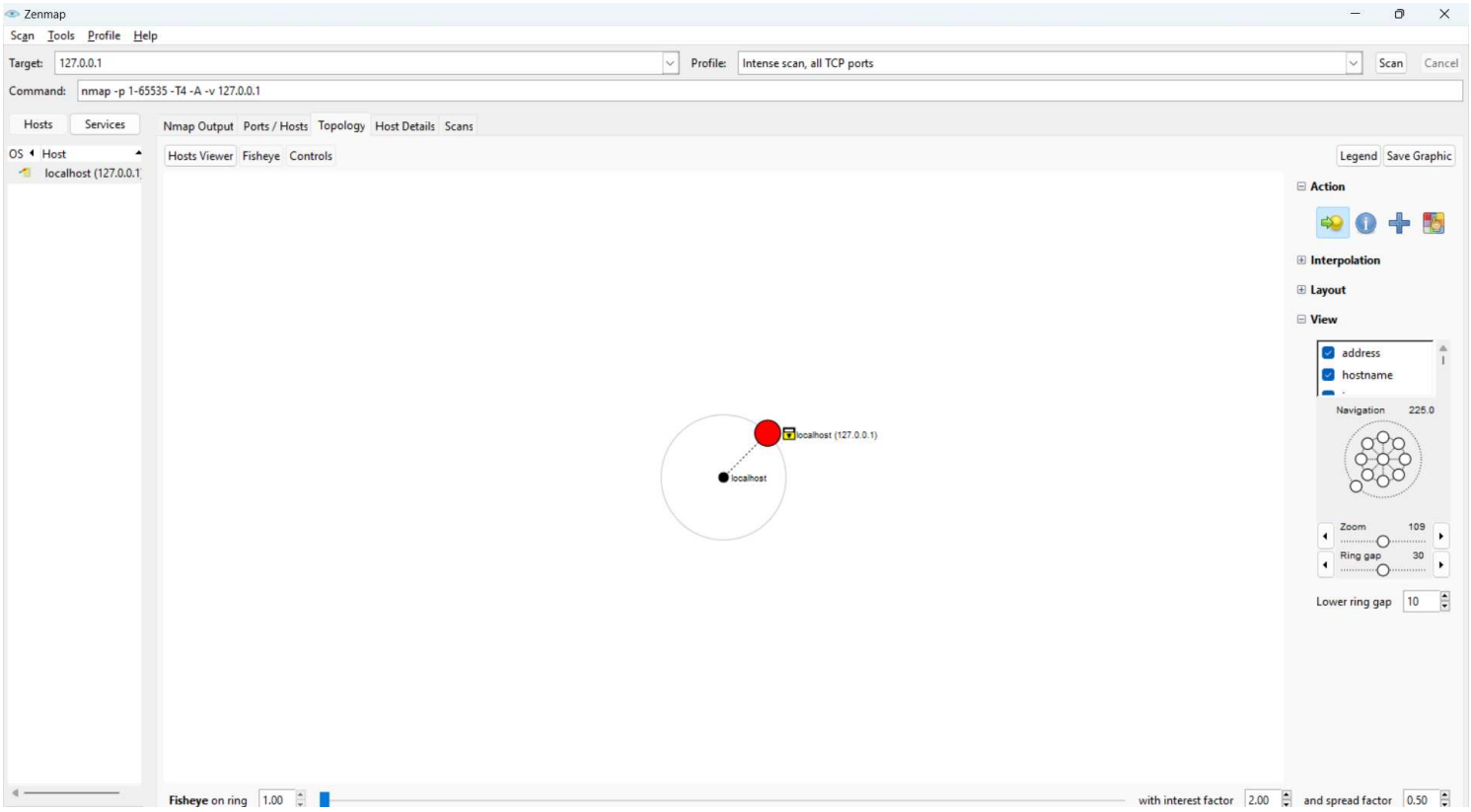

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
localhost (127.0.0.1
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
| GetRequest:
| HTTP/1.1 404 Not Found
| Vary: Origin
| Content-Security-Policy: default-src 'self'
| X-DNS-Prefetch-Control: off
| Expect-CT: max-age=0
| X-Frame-Options: SAMEORIGIN
| Strict-Transport-Security: max-age=15552000; includeSubDomains
| X-Download-Options: noopen
| X-Content-Type-Options: nosniff
| X-Permitted-Cross-Domain-Policies: none
| Referrer-Policy: no-referrer
| X-XSS-Protection: 0
| Content-Type: text/html; charset=utf-8
| Content-Length: 139
| Date: Sat, 12 Nov 2022 13:28:38 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot GET /</pre>
| </body>
| </html>
| HTTPOptions:
| HTTP/1.1 204 No Content
| Vary: Origin, Access-Control-Request-Headers
| Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
| Content-Length: 0
| Date: Sat, 12 Nov 2022 13:28:38 GMT
|_ Connection: close
5040/tcp open unknown
5354/tcp open mdnsresponder?
7680/tcp open pando-pub?
8029/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Dream-HTTPAPI/2.2.2.76 Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9012/tcp open ssl/websocket WebSocket++ 0.8.1
| ssl-cert: Subject: commonName=Peter Thorson/organizationName=Zaphoyd Studios/stateOrProvinceName=Illinois/countryName=US
| Issuer: commonName=Peter Thorson/organizationName=Zaphoyd Studios/stateOrProvinceName=Illinois/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-15T21:20:06

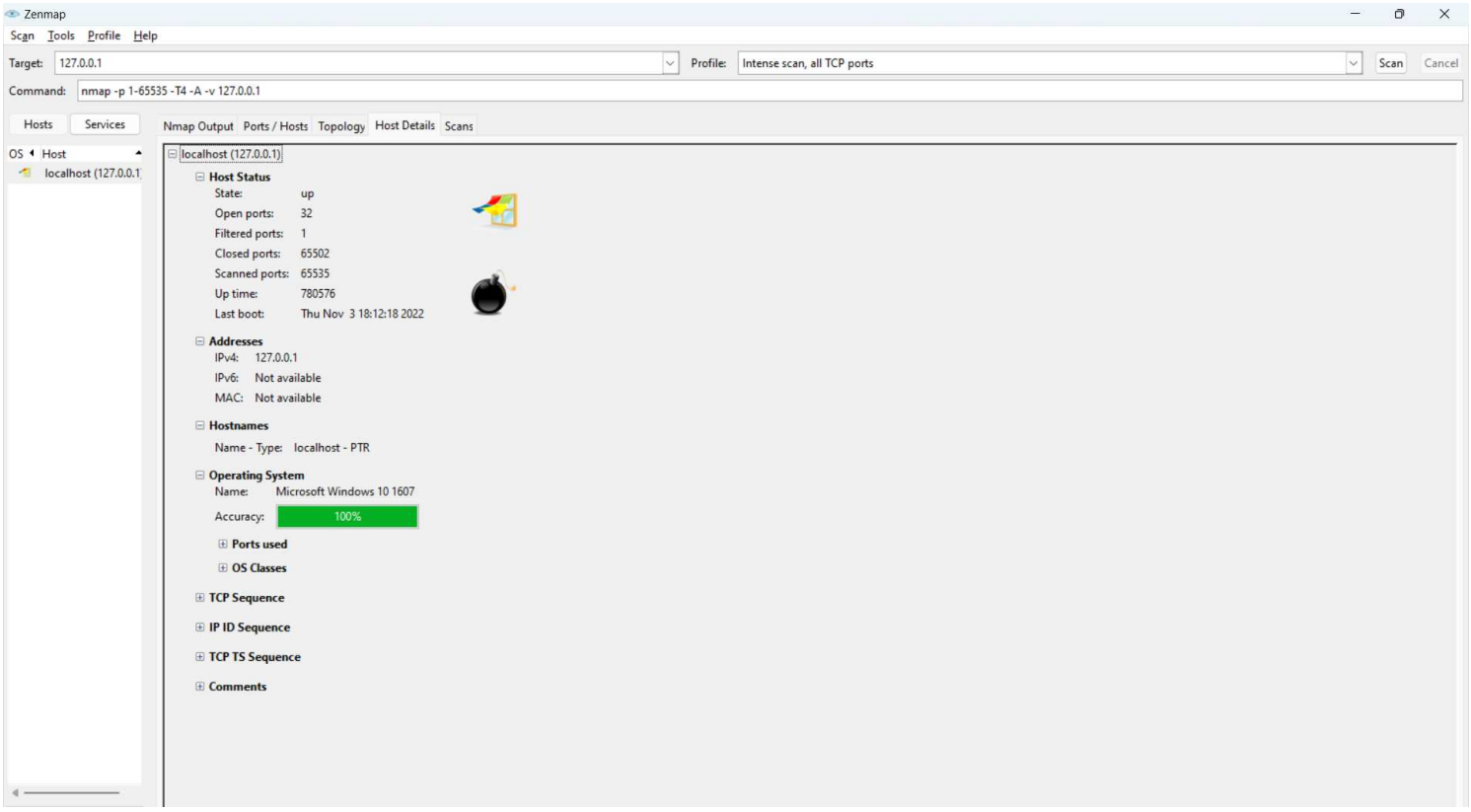

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
localhost (127.0.0.1
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-15T21:20:06
| Not valid after: 2012-11-14T21:20:06
| MD5: fe4923f52b506c585d190c0d0176daa7
|_SHA-1: 8c442ddfd5945b22204c17d0375aa8ef6956ce8d
9013/tcp open websocket WebSocket++ 0.8.1
9014/tcp open websocket WebSocket++ 0.8.1
13010/tcp open tcpwrapped
13030/tcp open unknown
13031/tcp open unknown
13032/tcp open unknown
17532/tcp open tcpwrapped
17945/tcp open tcpwrapped
22112/tcp open unknown
26666/tcp open unknown
27339/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
30950/tcp open unknown
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49670/tcp open msrpc Microsoft Windows RPC
49677/tcp open tcpwrapped
49679/tcp open unknown
55381/tcp open http Node.js Express framework
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-cors: GET POST
55633/tcp open ms-sql-s Microsoft SQL Server 2014
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-11-07T18:40:08
| Not valid after: 2052-11-07T18:40:08
| MD5: 947a0224650ec6396a0a812edbe0459f
|_SHA-1: af780465621c6fe92f3471fe2b65c52f3b6ab3fe
|_ssl-date: 2022-11-12T13:31:53+00:00; 0s from scanner time.
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
65001/tcp open unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============


Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
localhost (127.0.0.1
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
| MD5: 947a0224650ec6396a0a812edbe0459f
|_SHA-1: af780465621c6fe92f3471fe2b65c52f3b6ab3fe
|_ssl-date: 2022-11-12T13:31:53+00:00; 0s from scanner time.
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
65001/tcp open unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1042-TCP:V=7.93%I=7%D=11/12%Time=636F9F7B%P=i686-pc-windows-windows
SF:%r(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Origin\
SF:r\nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefetch-
SF:Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEO
SF:RIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20includeSubD
SF:omains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20n
SF:osniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Policy
SF::\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text/htm
SF:l;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Sat,\x2012\x2
SF:0Nov\x202022\x2013:28:27\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYP
SF:E\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">\
SF:n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n
SF:</body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Conten
SF:t\r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-Contr
SF:ol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Length:\
SF:x200\r\nDate:\x20Sat,\x2012\x20Nov\x202022\x2013:28:27\x20GMT\r\nConnec
SF:tion:\x20close\r\n\r\n")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20R
SF:equest\r\nConnection:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindR
SF:eqTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\
SF:n\r\n")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\
SF:nConnection:\x20close\r\n\r\n")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20R
SF:equest\r\nConnection:\x20close\r\n\r\n")%r(SSLSessionReq,2F,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(TerminalSe
SF:rverCookie,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clo
SF:se\r\n\r\n")%r(TLSSessionReq,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Connection:\x20close\r\n\r\n")%r(Kerberos,2F,"HTTP/1\.1\x20400\x20Bad\x
SF:20Request\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,2F,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(X11Probe,2
SF:F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1043-TCP:V=7.93%T=SSL%I=7%D=11/12%Time=636F9F86%P=i686-pc-windows-w
SF:indows%r(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20O
SF:rigin\r\nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Pre
SF:fetch-Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x2
SF:0SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20inclu
SF:deSubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options
SF::\x20nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-
SF:Policy:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20te

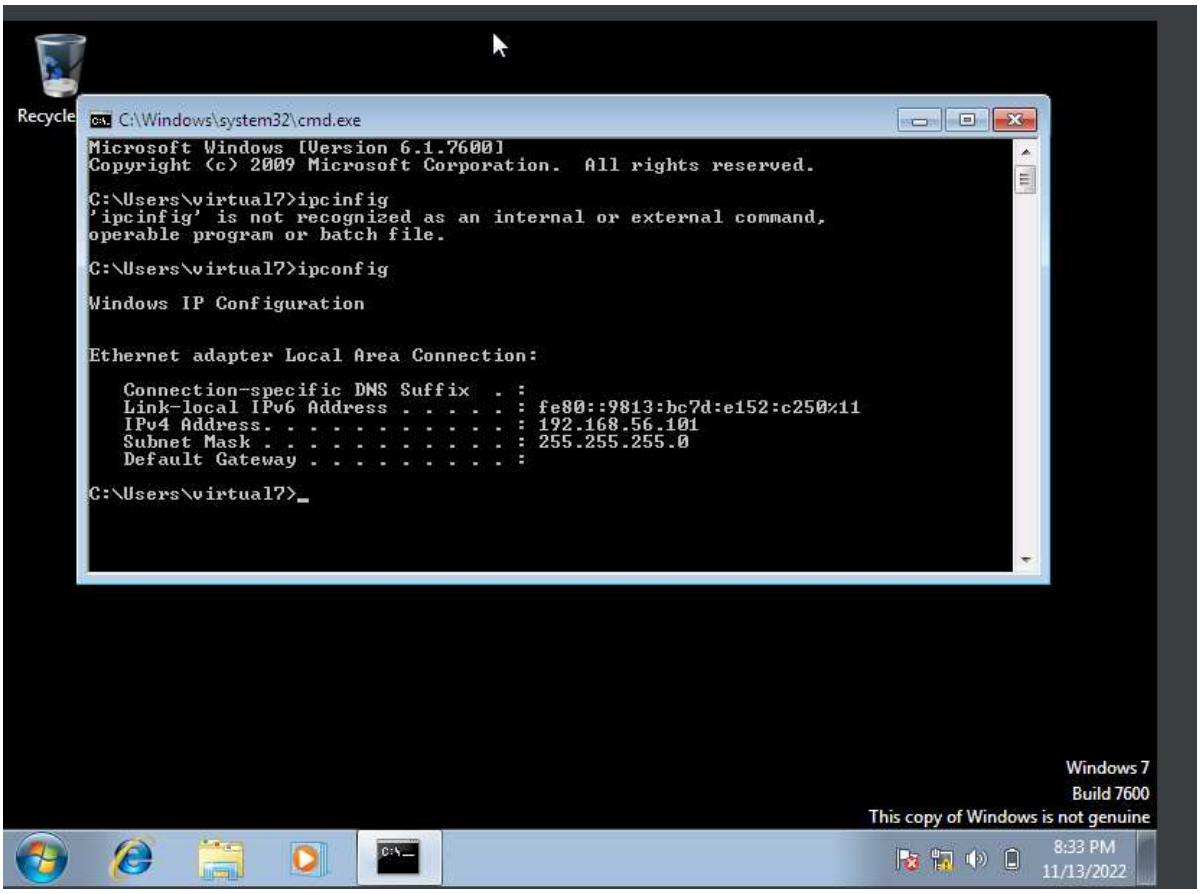

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
OS Host
localhost (127.0.0.1
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 1-65535 -T4 -A -v 127.0.0.1
Details
SF:deSubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options
SF::\x20nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-
SF:Policy:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20te
SF:xt/html;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Sat,\x2
SF:012\x20Nov\x202022\x2013:28:38\x20GMT\r\nConnection:\x20close\r\n\r\n<!
SF:DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf
SF:-8\">\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</
SF:pre>\n</body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20
SF:Content\r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess
SF:-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Le
SF:ngth:\x200\r\nDate:\x20Sat,\x2012\x20Nov\x202022\x2013:28:38\x20GMT\r\n
SF:Connection:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20Bad\x
SF:20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(
SF:DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnectio
SF:n:\x20close\r\n\r\n")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Connection:\x20close\r\n\r\n")%r(SSLSessionReq,2F,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCookie
SF:,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n
SF:")%r(TLSSessionReq,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection
SF::\x20close\r\n\r\n")%r(Kerberos,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\
SF:r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,2F,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(X11Probe,2F,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(FourOhF
SF:ourRequest,2DA,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Origin\r\n
SF:Content-Security-Policy:\x20default-src\x20'self'\x20blob:\x20127\.0\.0
SF:\.1:1042\x20127\.0\.0\.1:1043;script-src\x20'self'\x20'unsafe-inline';s
SF:tyle-src\x20'self';connect-src\x20'self'\x20ws:\x20wss:\x20blob:\x20127
SF:\.0\.0\.1:1042\x20127\.0\.0\.1:1043\x20127\.0\.0\.1:9013\x20127\.0\.0\.
SF:1:9014;worker-src\x20'self'\x20blob:\x20127\.0\.0\.1:1042\x20127\.0\.0\
SF:.1:1043;img-src\x20'self'\x20data:\x20blob:\x20127\.0\.0\.1:1042\x20127
SF:\.0\.0\.1:1043\r\nX-DNS-Prefetch-Control:\x20off\r\nExpect-CT:\x20max-a
SF:ge=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x2
SF:0max-age=15552000;\x20includeSubDomains\r\nX-Download-Options:\x20noope
SF:n\r\nX-Content-Type-Options:\x20nosniff\r\nX-Permitted-Cross-Domain-Pol
SF:icies:\x20none\r\nReferrer-Policy:\x20no-referrer\r\nX-XSS-Protection:\
SF:x200\r\nDate:\x20Sat,\x2012\x20Nov\x202022\x2013:28:38\x20GMT\r\nConnec
SF:tion:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port49679-TCP:V=7.93%I=7%D=11/12%Time=636F9F84%P=i686-pc-windows-window
SF:s%r(HTTPOptions,20,"\x01\0\x03\x01\x05\0\x07\0\t\0\r\xc8\r\0\x0f\0\x11\
SF:0\x13\0\x15\0\x17\0\x19\0\x1b\0\x1d\0\x1f\0")%r(RTSPRequest,20,"\x01\0\
SF:x03\x01\x05\0\x07\0\t\0\r\xc8\r\0\x0f\0\x11\0\x13\0\x15\0\x17\0\x19\0\x
SF:1b\0\x1d\0\x1f\0")%r(NCP,20,"\x01\0\x03\x01\x05\0\x07\0\t\0\r\xc8\r\0\x
SF:0f\0\x11\0\x13\0\x15\0\x17\0\x19\0\x1b\0\x1d\0\x1f\0");
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607


Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
OS Host
localhost (127.0.0.1
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
135 tcp open msrpc Microsoft Windows RPC
137 tcp filtered netbios-ns
445 tcp open microsoft-ds
1042 tcp open afrog
1043 tcp open boinc
5040 tcp open unknown
5354 tcp open mdnsresponder
7680 tcp open pando-pub
8029 tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9012 tcp open websocket WebSocket++ 0.8.1
9013 tcp open websocket WebSocket++ 0.8.1
9014 tcp open websocket WebSocket++ 0.8.1
13010 tcp open tcpwrapped
13030 tcp open
13031 tcp open
13032 tcp open
17532 tcp open tcpwrapped
17945 tcp open tcpwrapped
22112 tcp open
26666 tcp open
27339 tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
30950 tcp open
49664 tcp open msrpc Microsoft Windows RPC
49665 tcp open msrpc Microsoft Windows RPC
49666 tcp open msrpc Microsoft Windows RPC
49667 tcp open msrpc Microsoft Windows RPC
49668 tcp open msrpc Microsoft Windows RPC
49670 tcp open msrpc Microsoft Windows RPC
49677 tcp open tcpwrapped
49679 tcp open unknown

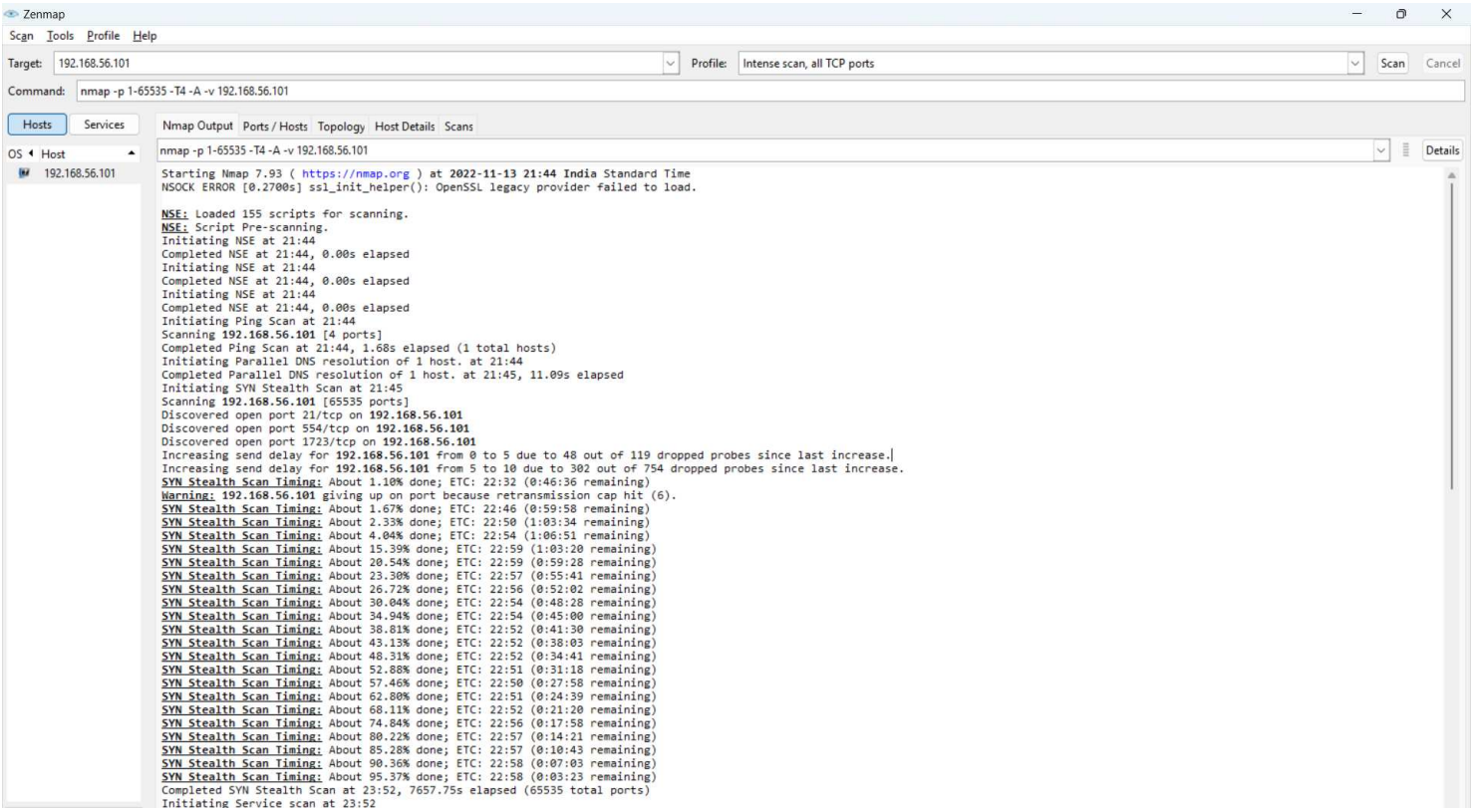

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
OS Host
localhost (127.0.0.1
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
Action
Interpolation
Layout
View
address
hostname
Navigation 225.0
Zoom 109
Ring gap 30
Lower ring gap 10
localhost (127.0.0.1)
localhost
Fisheye on ring 1.00
with interest factor 2.00
and spread factor 0.50

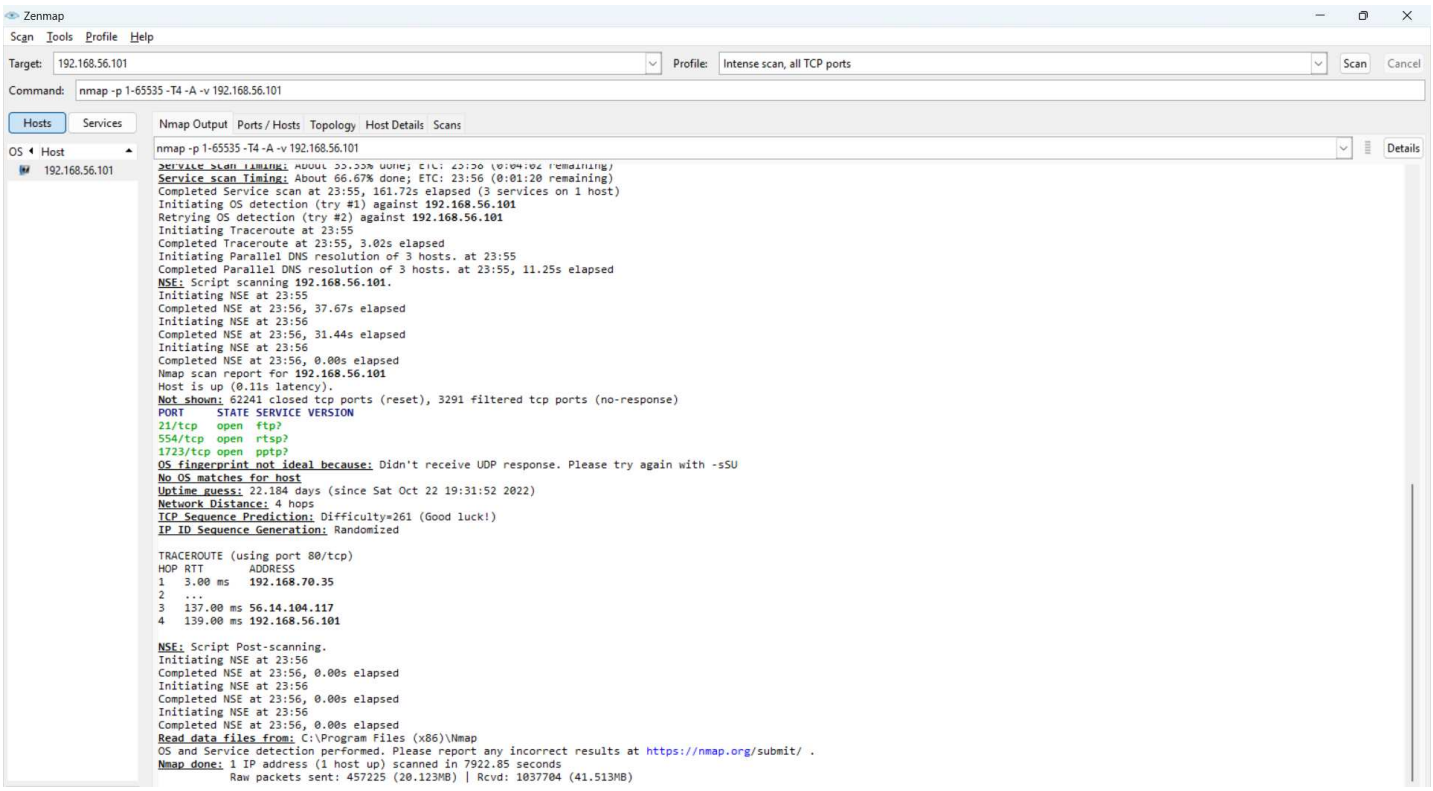

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 127.0.0.1
Hosts Services
OS Host
localhost (127.0.0.1
Nmap Output Ports / Hosts Topology Host Details Scans
localhost (127.0.0.1)
Host Status
State: up
Open ports: 32
Filtered ports: 1
Closed ports: 65502
Scanned ports: 65535
Up time: 780576
Last boot: Thu Nov 3 18:12:18 2022
Addresses
IPv4: 127.0.0.1
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: localhost - PTR
Operating System
Name: Microsoft Windows 10 1607
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

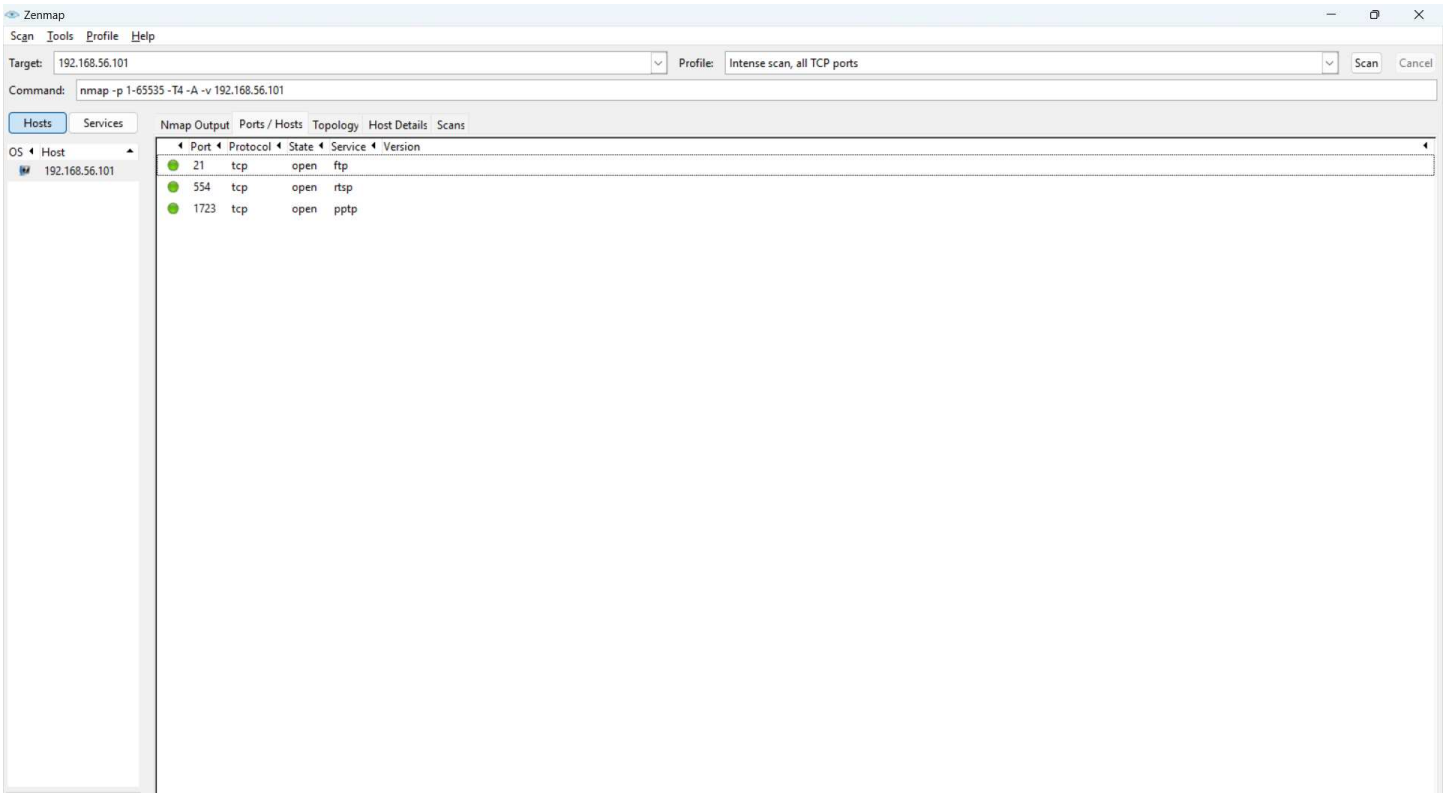
1.VICTIM MACHINE : WINDOWS 7

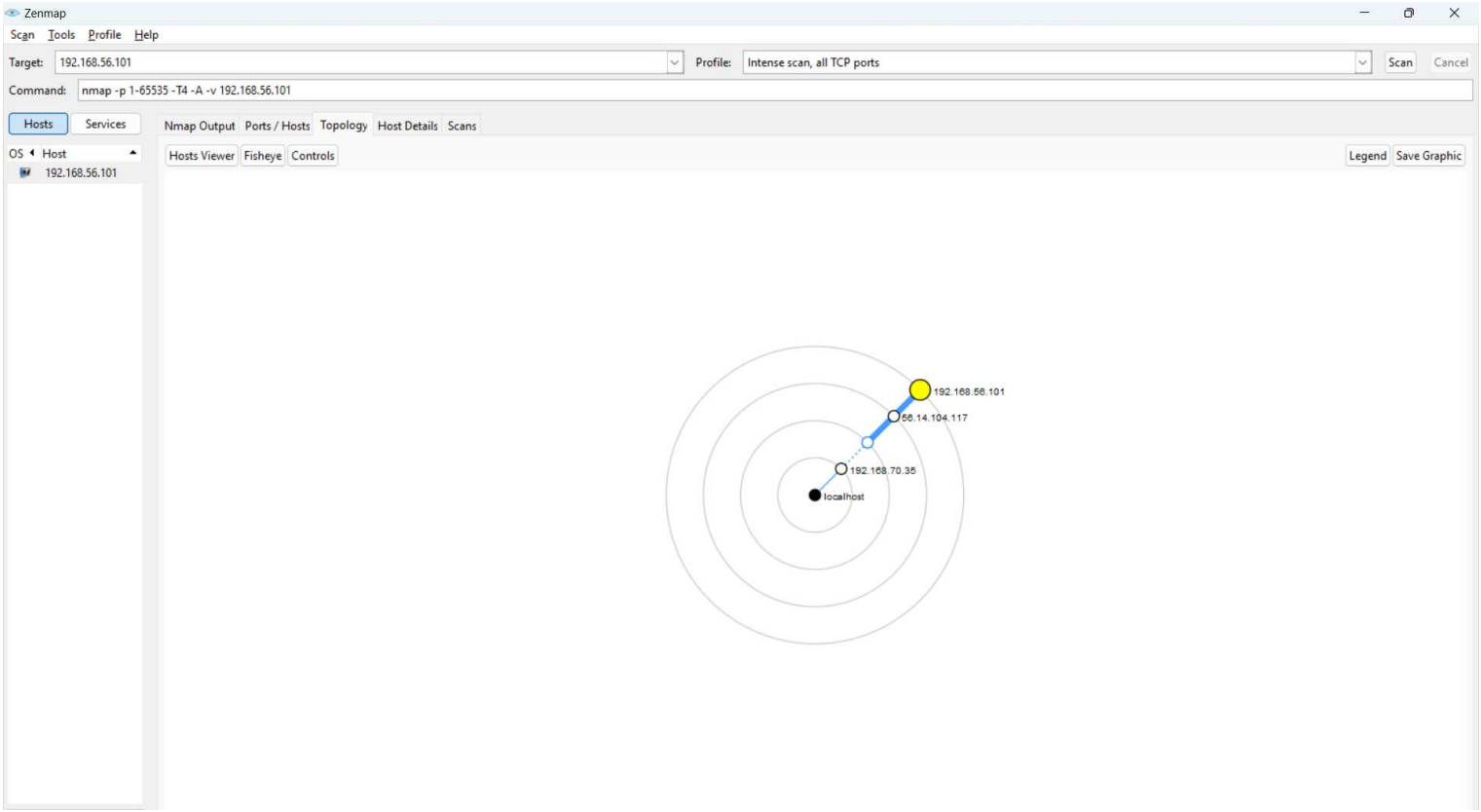


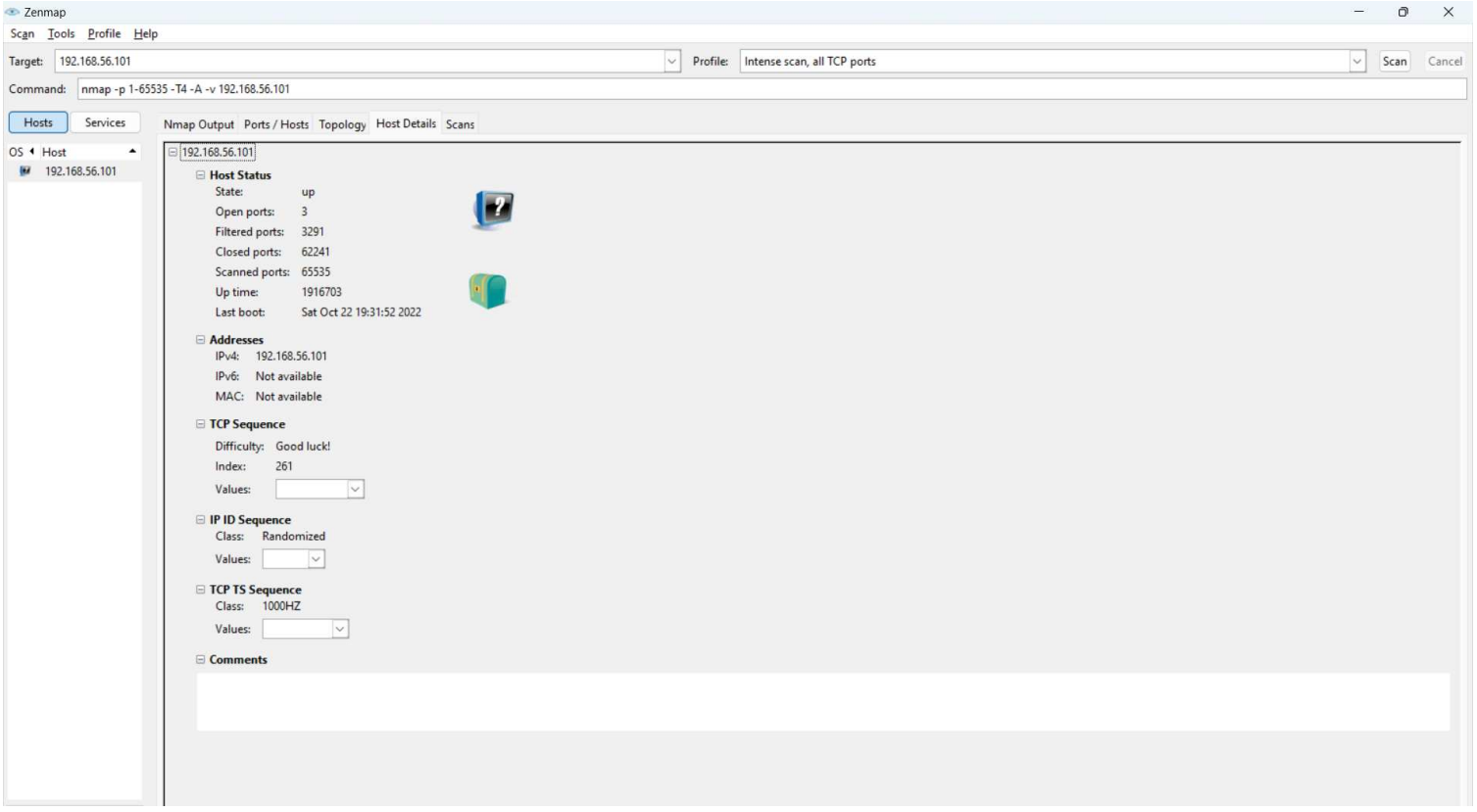
BELOW THERE ARE SCREENSHOTS TAKEN IN NMAP



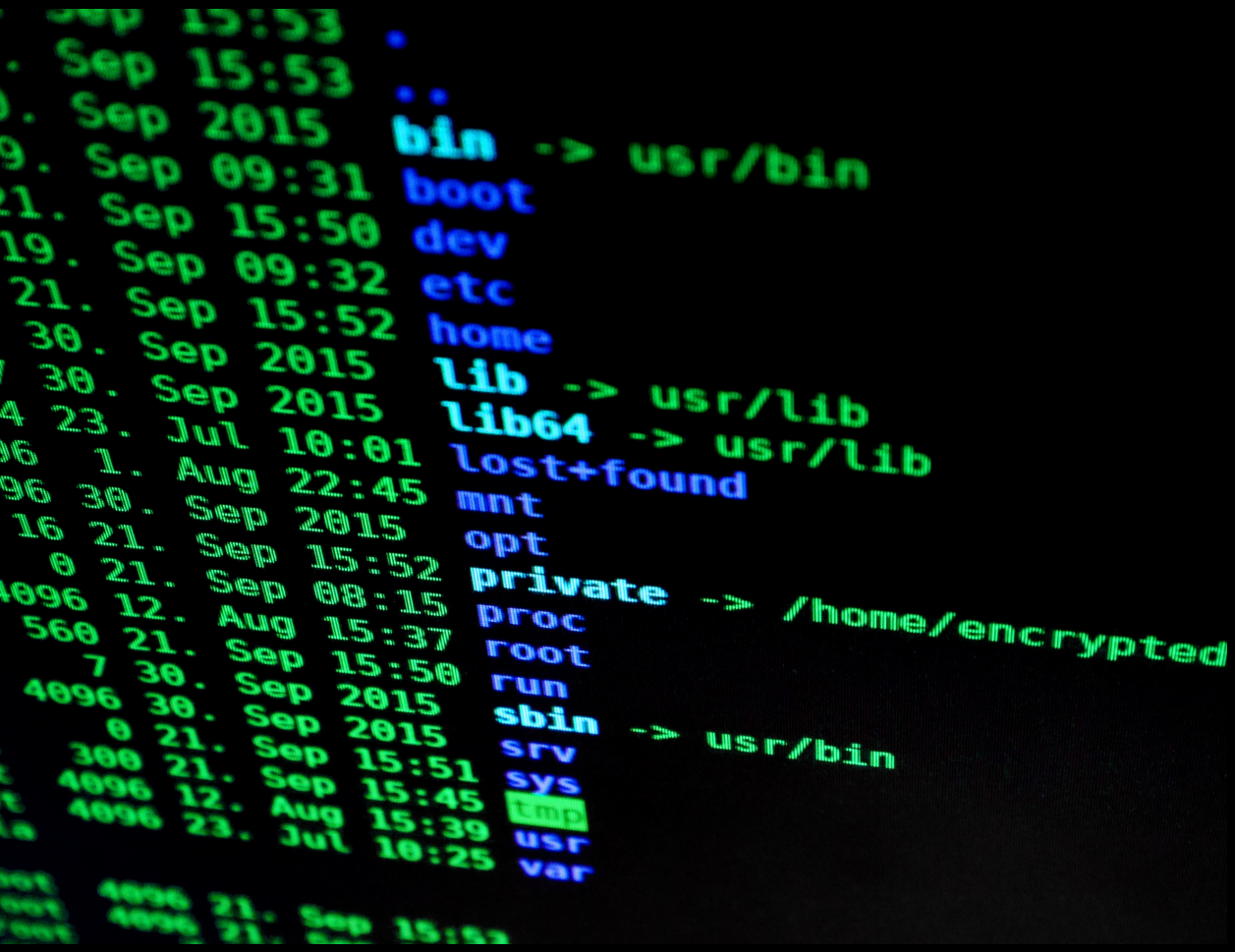

Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p 1-65535 -T4 -A -v 192.168.56.101
Details
Service scan Timing: About 66.67% done; ETC: 23:56 (0:01:20 remaining)
Completed Service scan at 23:55, 161.72s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.101
Retrying OS detection (try #2) against 192.168.56.101
Initiating Traceroute at 23:55
Completed Traceroute at 23:55, 3.02s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 23:55
Completed Parallel DNS resolution of 3 hosts. at 23:55, 11.25s elapsed
NSE: Script scanning 192.168.56.101.
Initiating NSE at 23:55
Completed NSE at 23:56, 37.67s elapsed
Initiating NSE at 23:56
Completed NSE at 23:56, 31.44s elapsed
Initiating NSE at 23:56
Completed NSE at 23:56, 0.00s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.11s latency).
Not shown: 62241 closed tcp ports (reset), 3291 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp?
554/tcp open rtsp?
1723/tcp open pptp?
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Uptime guess: 22.184 days (since Sat Oct 22 19:31:52 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Randomized
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.00 ms 192.168.70.35
2 ...
3 137.00 ms 56.14.104.117
4 139.00 ms 192.168.56.101
NSE: Script Post-scanning.
Initiating NSE at 23:56
Completed NSE at 23:56, 0.00s elapsed
Initiating NSE at 23:56
Completed NSE at 23:56, 0.00s elapsed
Initiating NSE at 23:56
Completed NSE at 23:56, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7922.85 seconds
Raw packets sent: 457225 (20.123MB) | Rcvd: 1037704 (41.513MB)


Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
21 tcp open ftp
554 tcp open rtsp
1723 tcp open pptp


Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
192.168.56.101
56.14.104.117
192.168.70.35
localhost


Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan, all TCP ports
Scan Cancel
Command: nmap -p 1-65535 -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
192.168.56.101
Host Status
State: up
Open ports: 3
Filtered ports: 3291
Closed ports: 62241
Scanned ports: 65535
Up time: 1916703
Last boot: Sat Oct 22 19:31:52 2022
Addresses
IPv4: 192.168.56.101
IPv6: Not available
MAC: Not available
TCP Sequence
Difficulty: Good luck!
Index: 261
Values:
IP ID Sequence
Class: Randomized
Values:
TCP TS Sequence
Class: 1000HZ
Values:
Comments

2.METASPLOIT TOOL



★ ★ ★ ★

METASPLOIT TOOL

THE METASPLOIT FRAMEWORK IS A TOOL FOR DEVELOPING AND EXECUTING EXPLOIT CODE AGAINST A REMOTE TARGET MACHINE.

IT CAN BE USED TO EXPLOIT VULNERABILITIES IN SYSTEMS AND APPLICATIONS.

THE METASPLOIT FRAMEWORK INCLUDES A WIDE RANGE OF TOOLS FOR CREATING, TESTING, AND EXECUTING EXPLOITS.

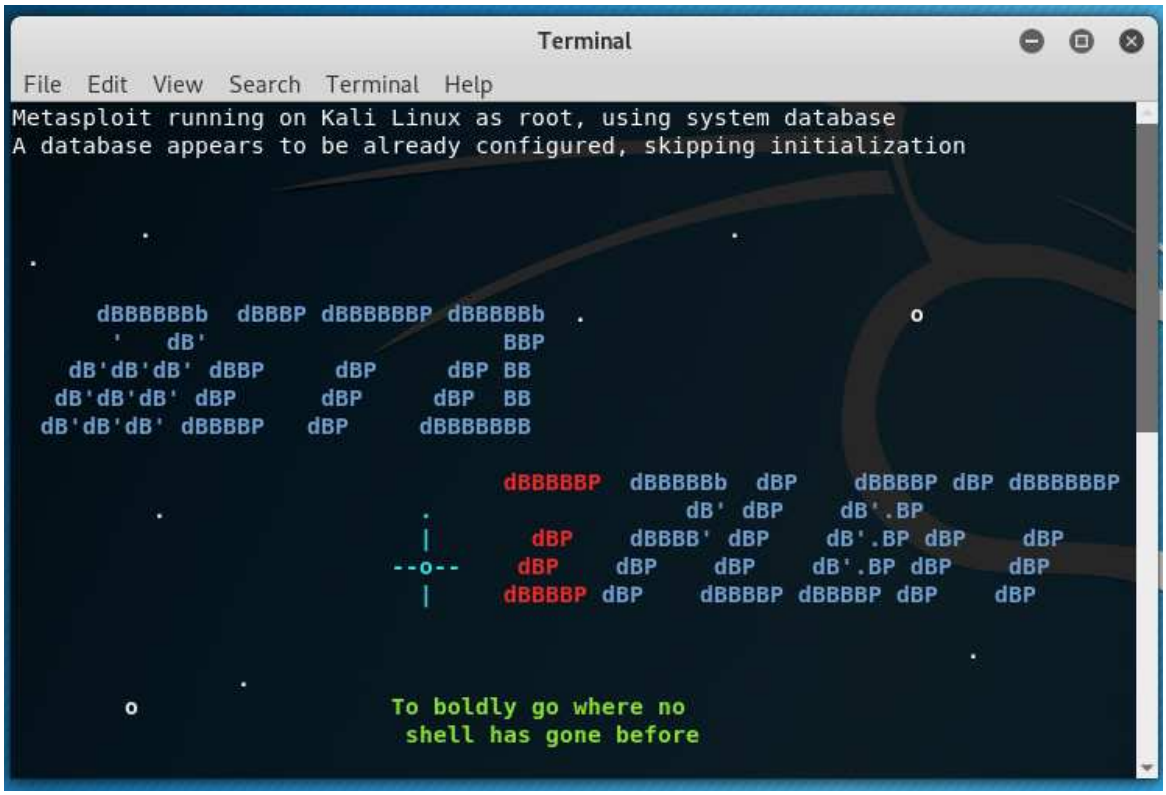
THESE TOOLS CAN BE USED TO EXPLOIT VULNERABILITIES IN SYSTEMS AND APPLICATIONS.THE METASPLOIT FRAMEWORK IS A TOOL FOR DEVELOPING AND EXECUTING EXPLOIT CODE AGAINST A REMOTE TARGET MACHINE.

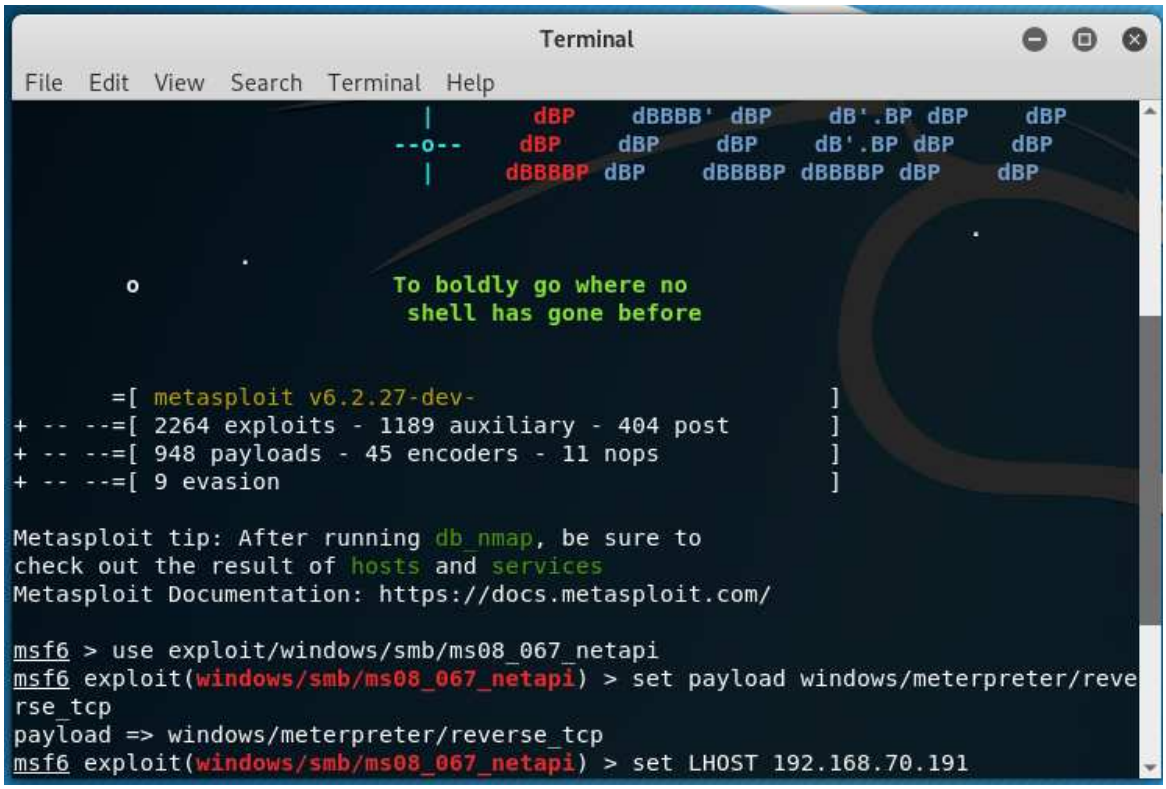
IT CAN BE USED TO EXPLOIT VULNERABILITIES IN SYSTEMS AND APPLICATIONS.

THE METASPLOIT FRAMEWORK INCLUDES A WIDE RANGE OF TOOLS FOR CREATING, TESTING, AND EXECUTING EXPLOITS.

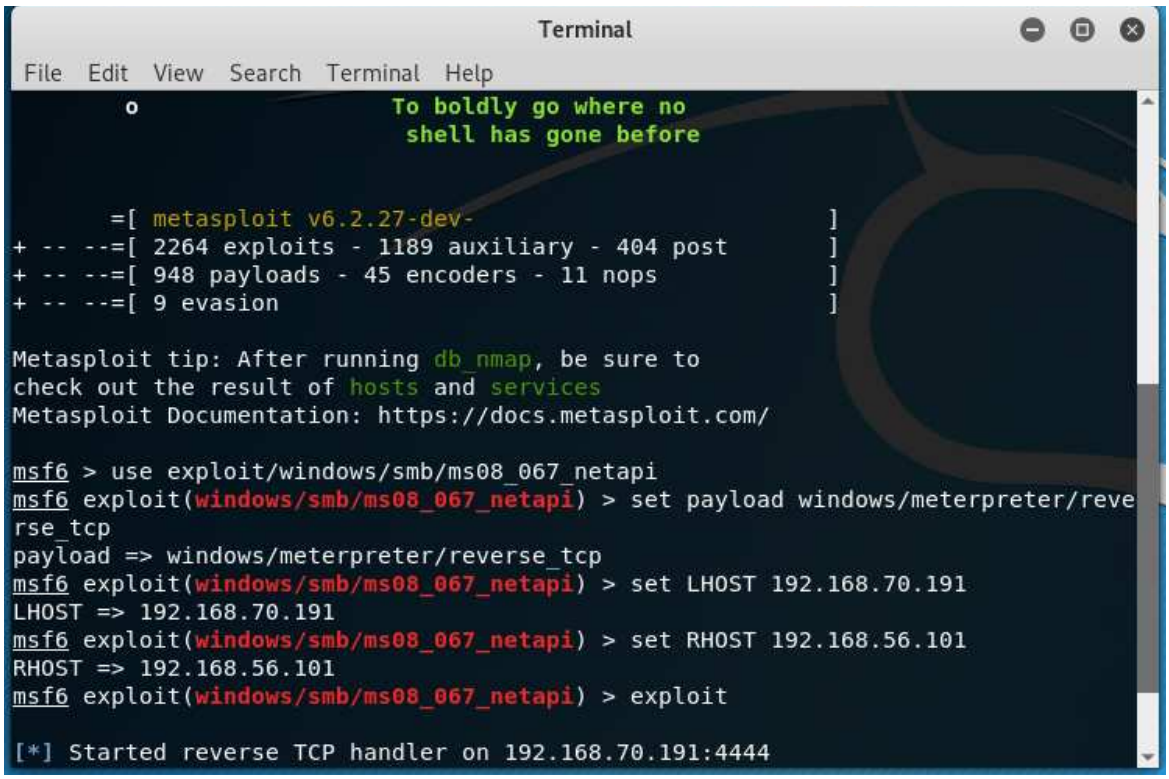
THESE TOOLS CAN BE USED TO EXPLOIT VULNERABILITIES IN SYSTEMS AND APPLICATIONS.

STEP 1: INSTALL METASPLOIT USING TERMINAL

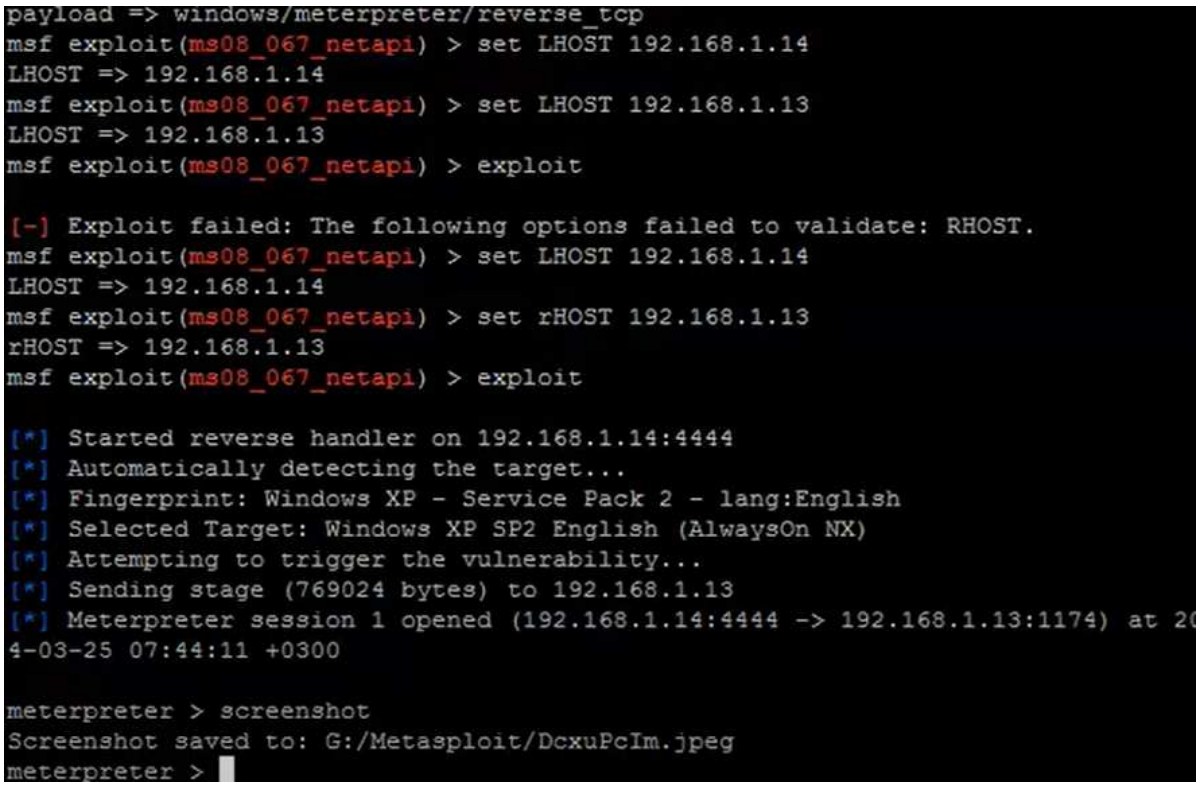




NOW WE EXECUTE THE COMMAND TO GET THE SCREENSHOT OF WIN 7

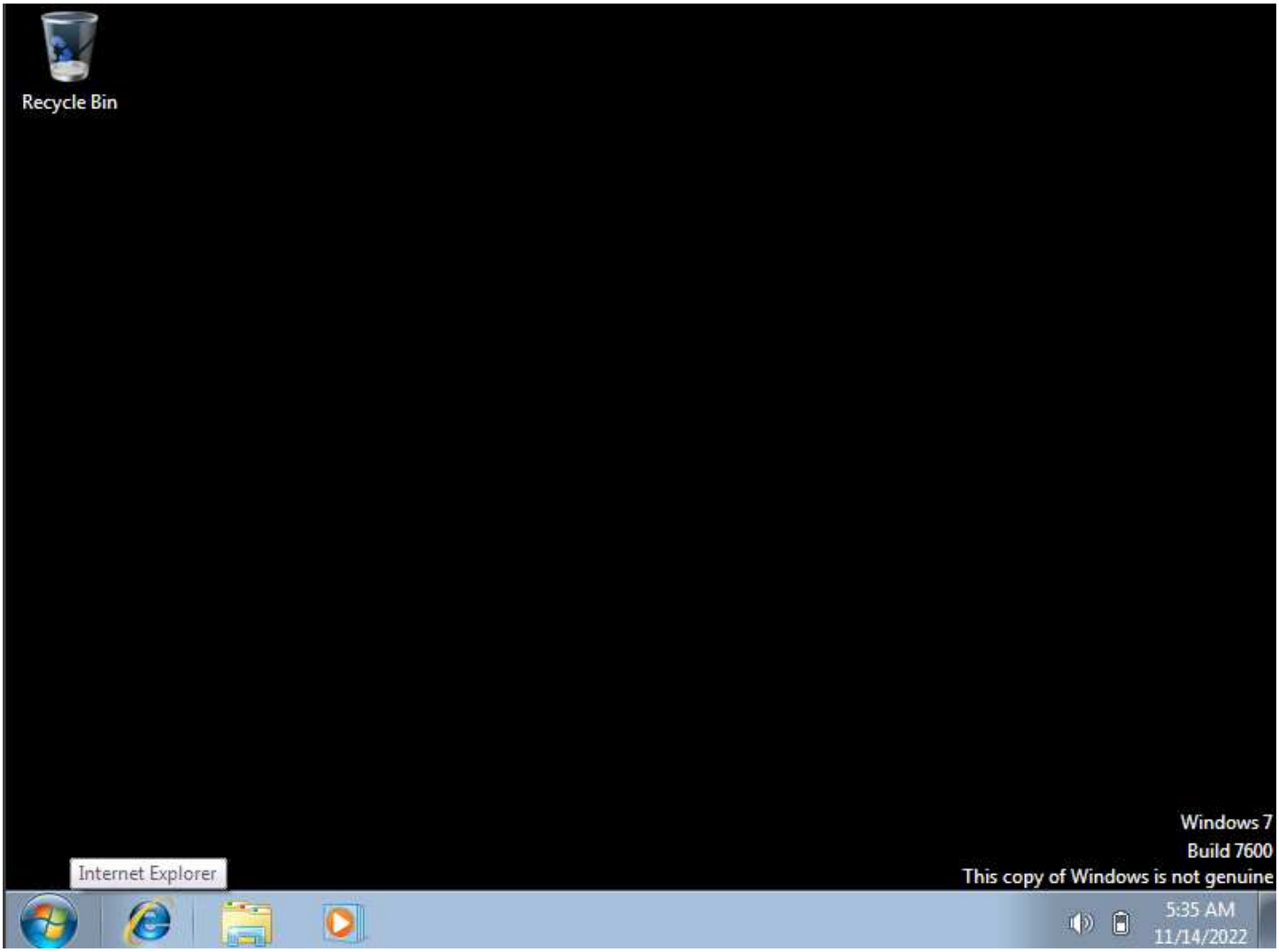


LHOST - IP OF YOUR MACHINE
RHOST - IP OF THE TARGET MACHINE



SCREENSHOT

THE TOOL IN THE KALI LINUX HAS TAKEN THE SCREEN SHOT IN TARGET DEVICE WINDOWS 7 --



SUGGEST TH SECURITYPATCH AND METHODS TO AVOID METASPLOIT TOOL

THE SECURITY PATCH TO AVOID METASPLOIT TOOL IS TO UPDATE YOUR SOFTWARE TO THE LATEST VERSION.

THERE IS NO SINGLE SILVER BULLET THAT WILL PROTECT AGAINST ALL ATTACKS USING METASPLOIT, BUT SOME BASIC DEFENSES INCLUDE:-

KEEP YOUR SOFTWARE UP TO DATE

USE A FIREWALL

USE INTRUSION DETECTION/PREVENTION SYSTEMS

DISABLE UNNECESSARY SERVICES

LIMIT ACCESS TO CRITICAL SYSTEMS

TRAIN EMPLOYEES IN SECURITY AWARENESS

HACKER MACHINE:

KALI LINUX

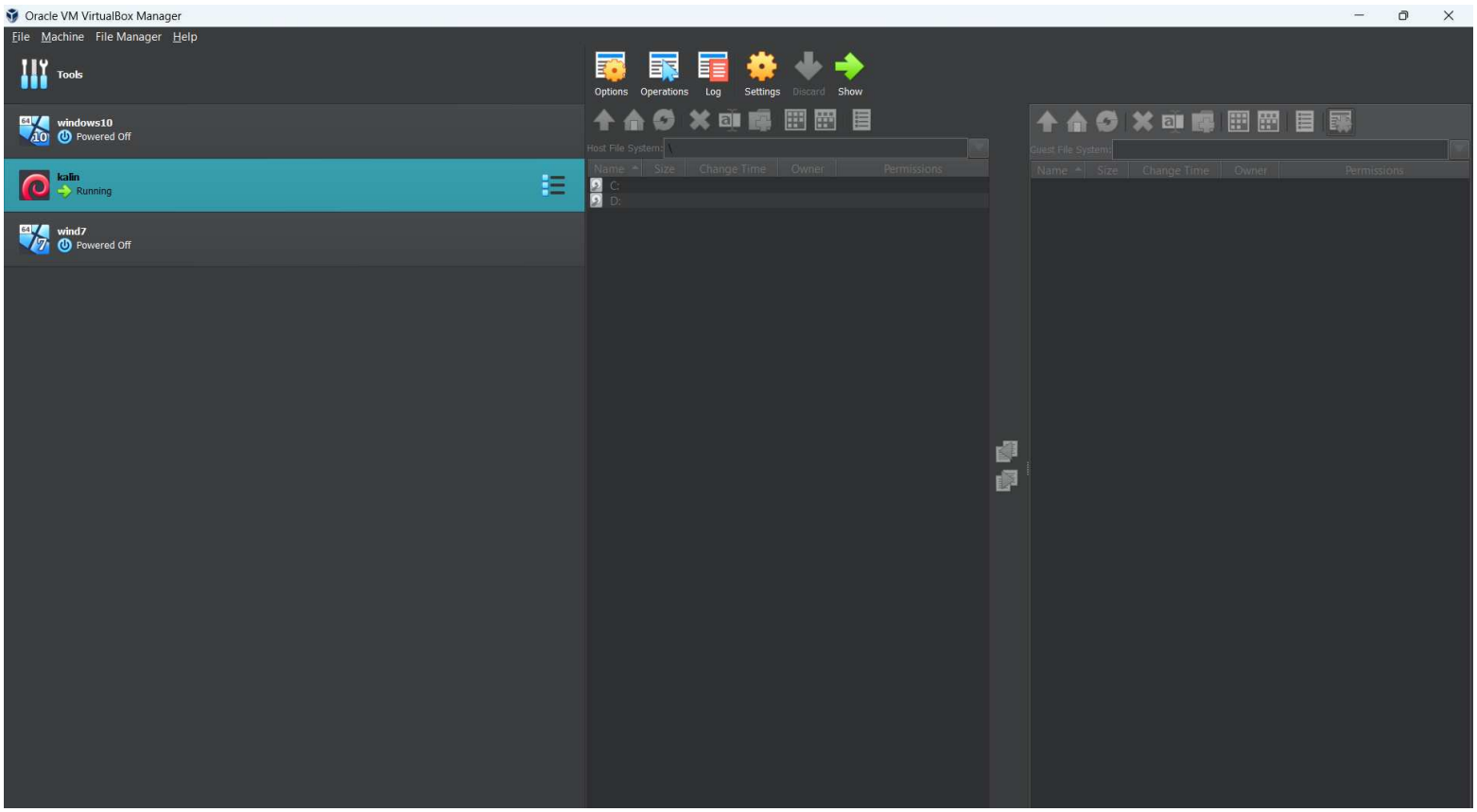
VICTIM MACHINE:

WINDOWS 7

3.USING SET TOOL TO CREATE FAKE GMAIL PAGE

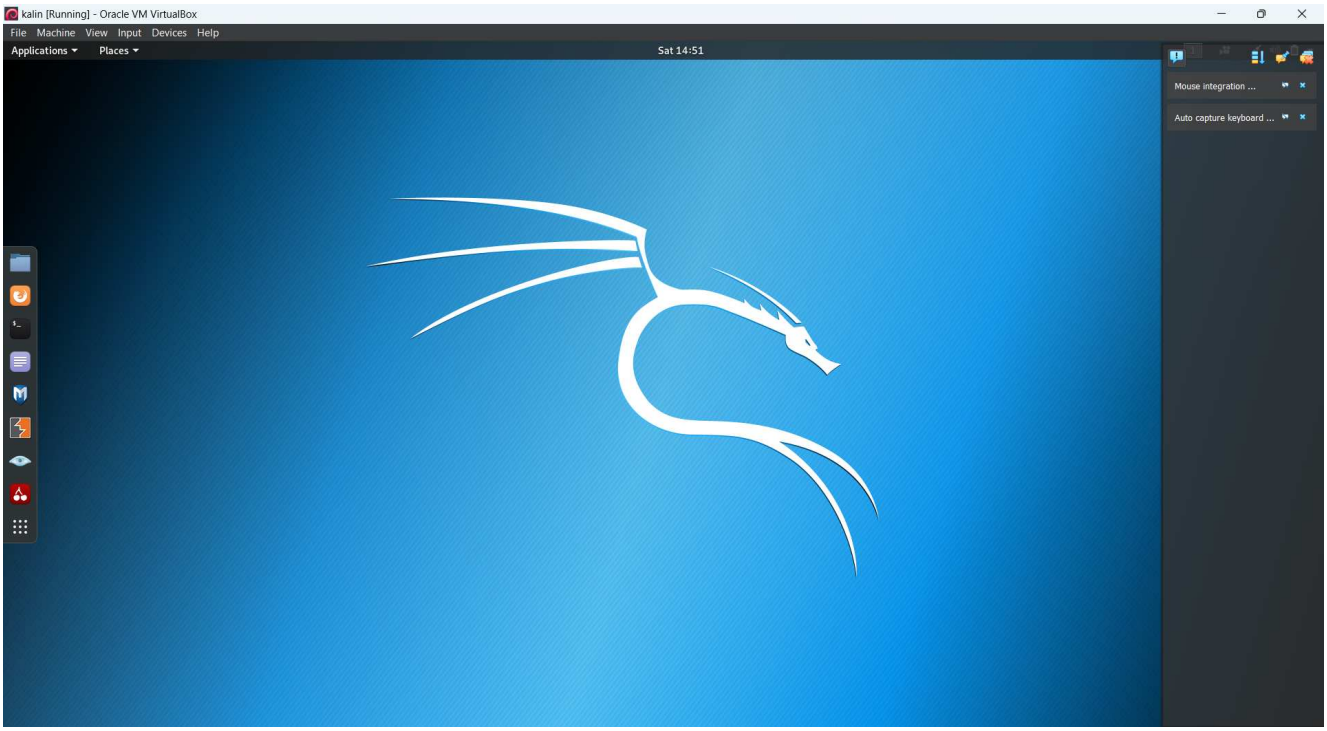
STEP 1:

OPEN VIRTUAL BOX AND OPEN KALI LINUX



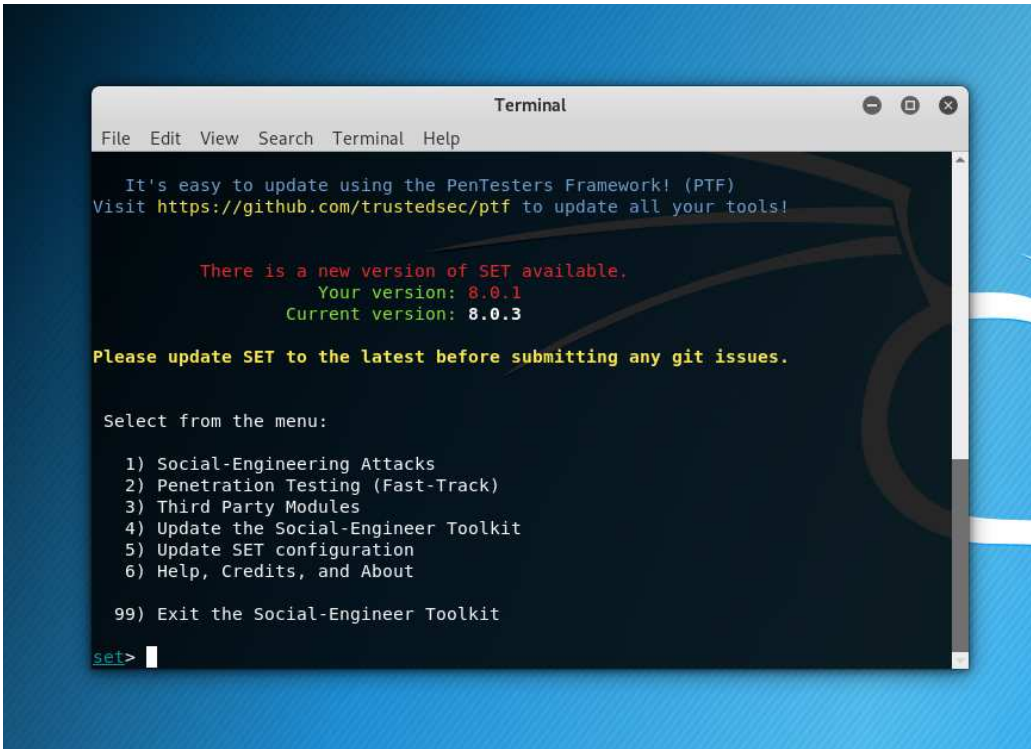
STEP 2:

OPEN SET TOOL IN KALI LINUX



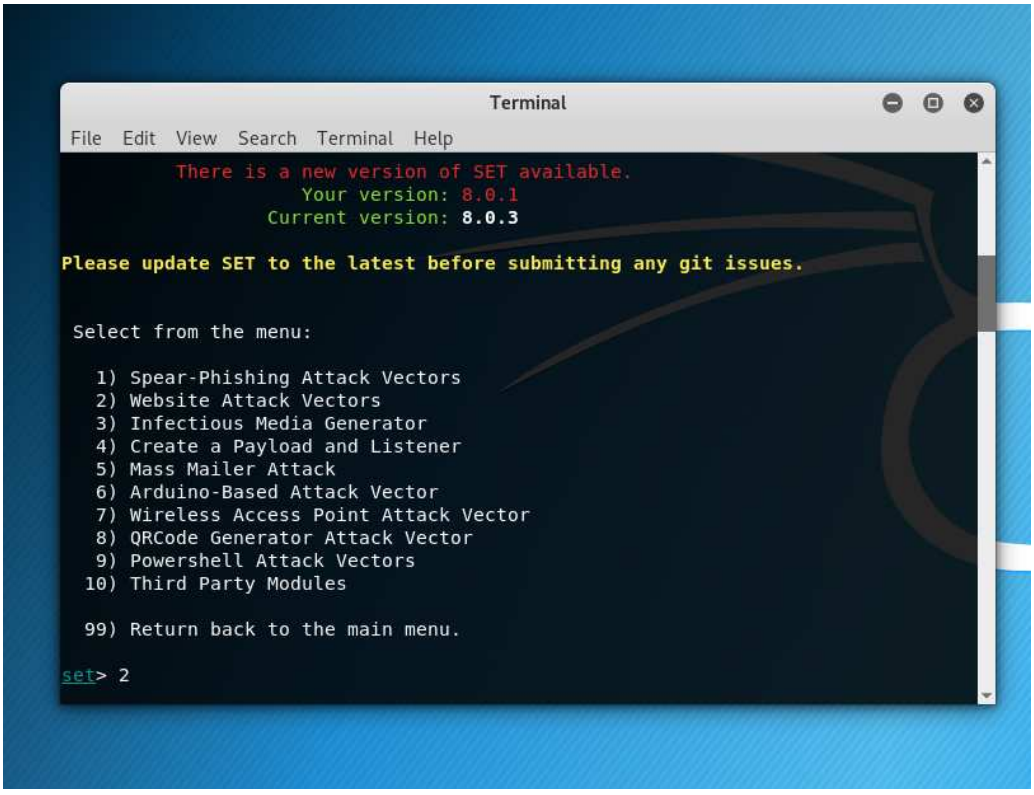
STEP 3:

AFTER OPENING CLICK NO.1 FOR SOCIAL ENGINEERING TOOL KIT



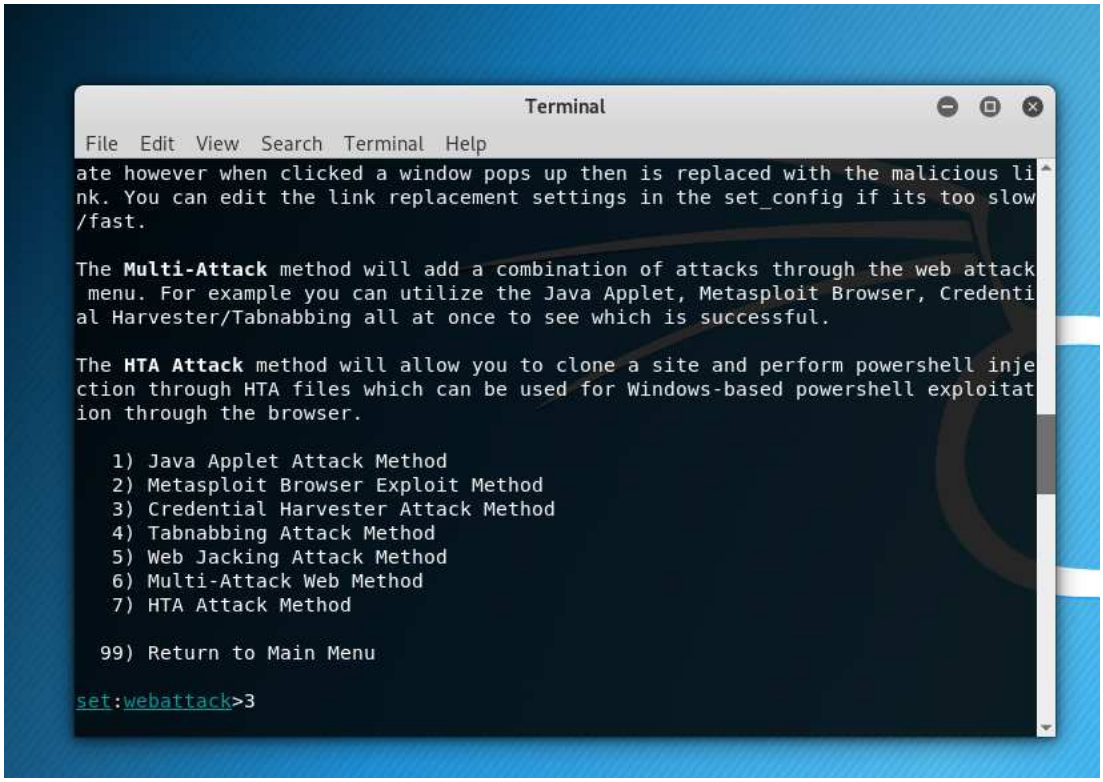
STEP 4:

CLICK NO.2 FOR ATTACKING WEBSITES



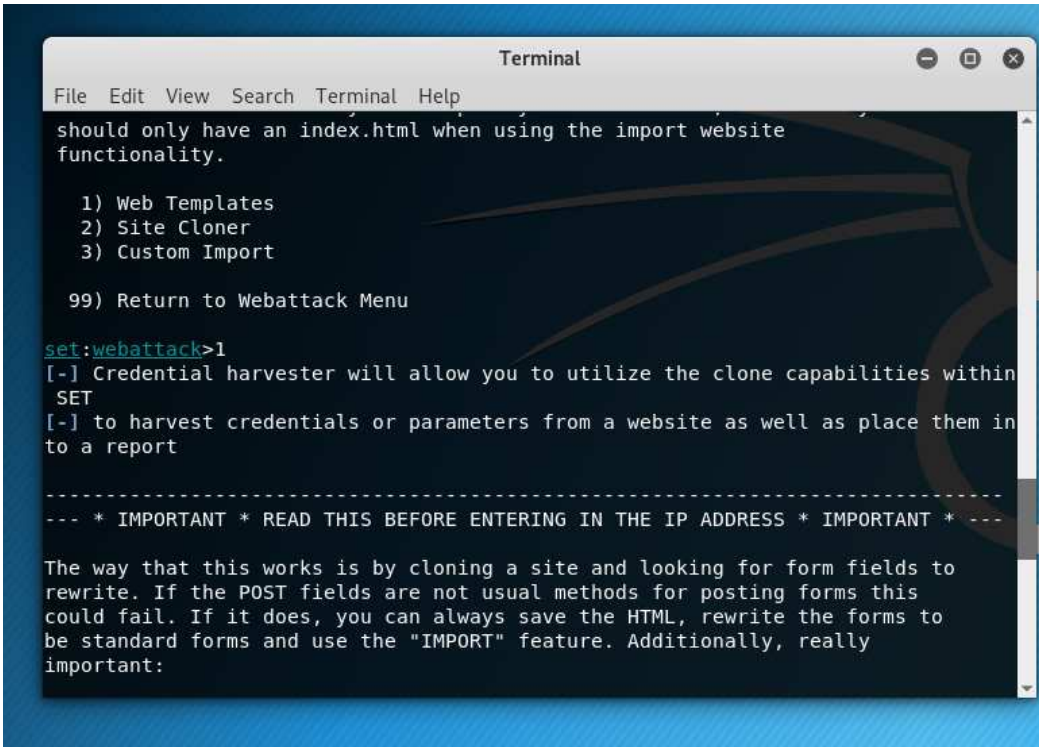
STEP 5:

CLICK NO.3 FOR CREDENTIAL HARVESTER ATTACK METHOD



STEP 6:

CLICK NO.1 FOR WEBSITES TEMPLATES

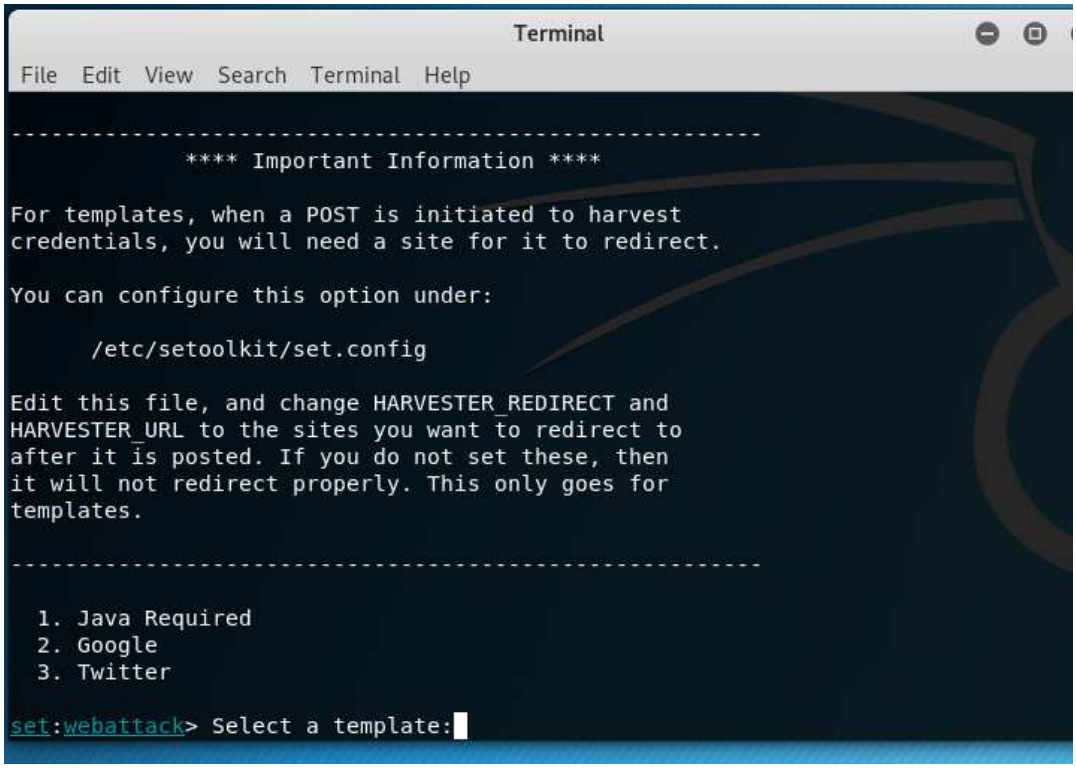


STEP 7:

SET TOOL WILL ASK FOR THE IP ADDRESS FOR THE LINK

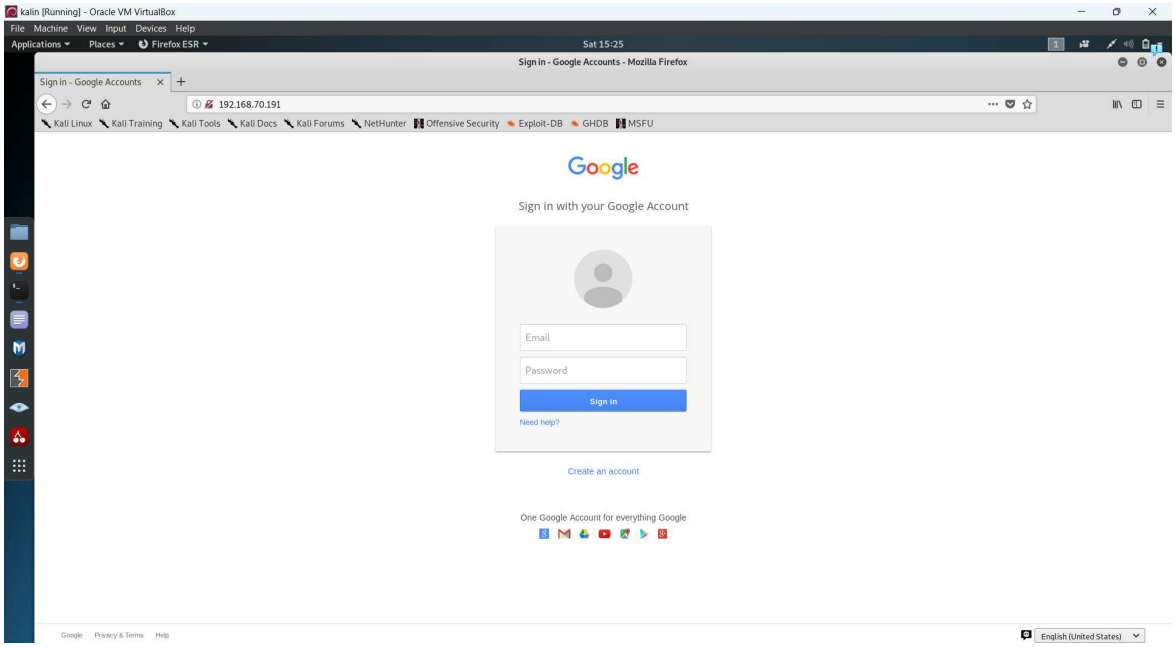
STEP 8:

SELECT THE TEMPLATE NEEDED



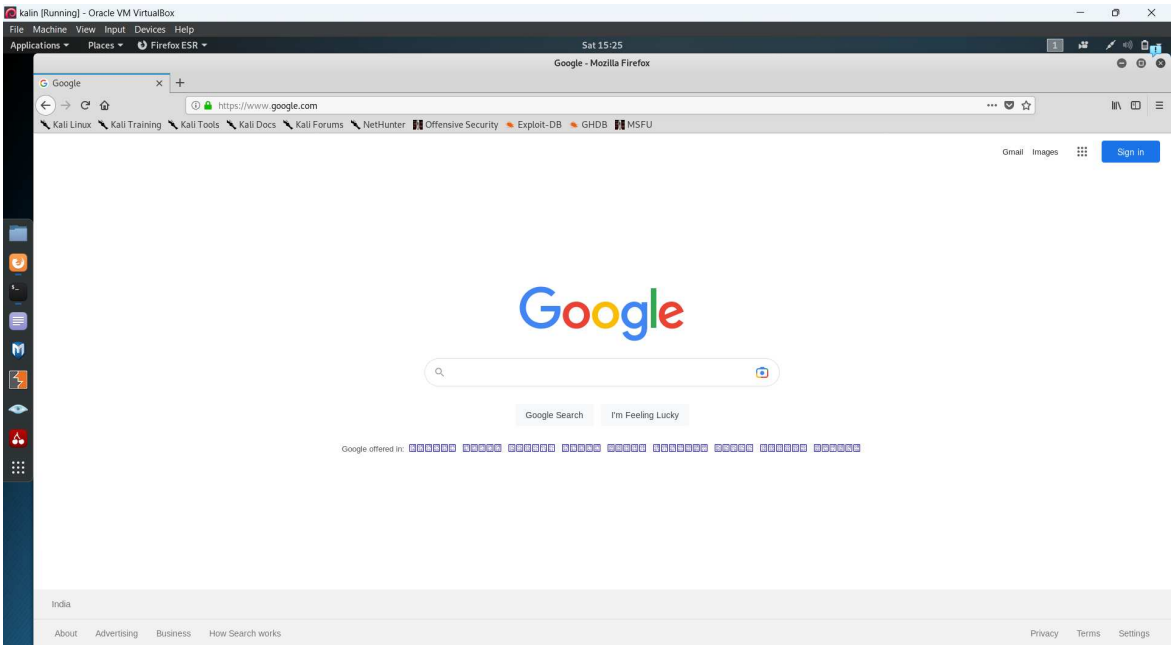
STEP 9:

OPEN CHROME AND TYPE THE IP ADDRESS TO OPEN THE LINK - ENTER THE USERNAME AND PASSWORD AND SIGN IN



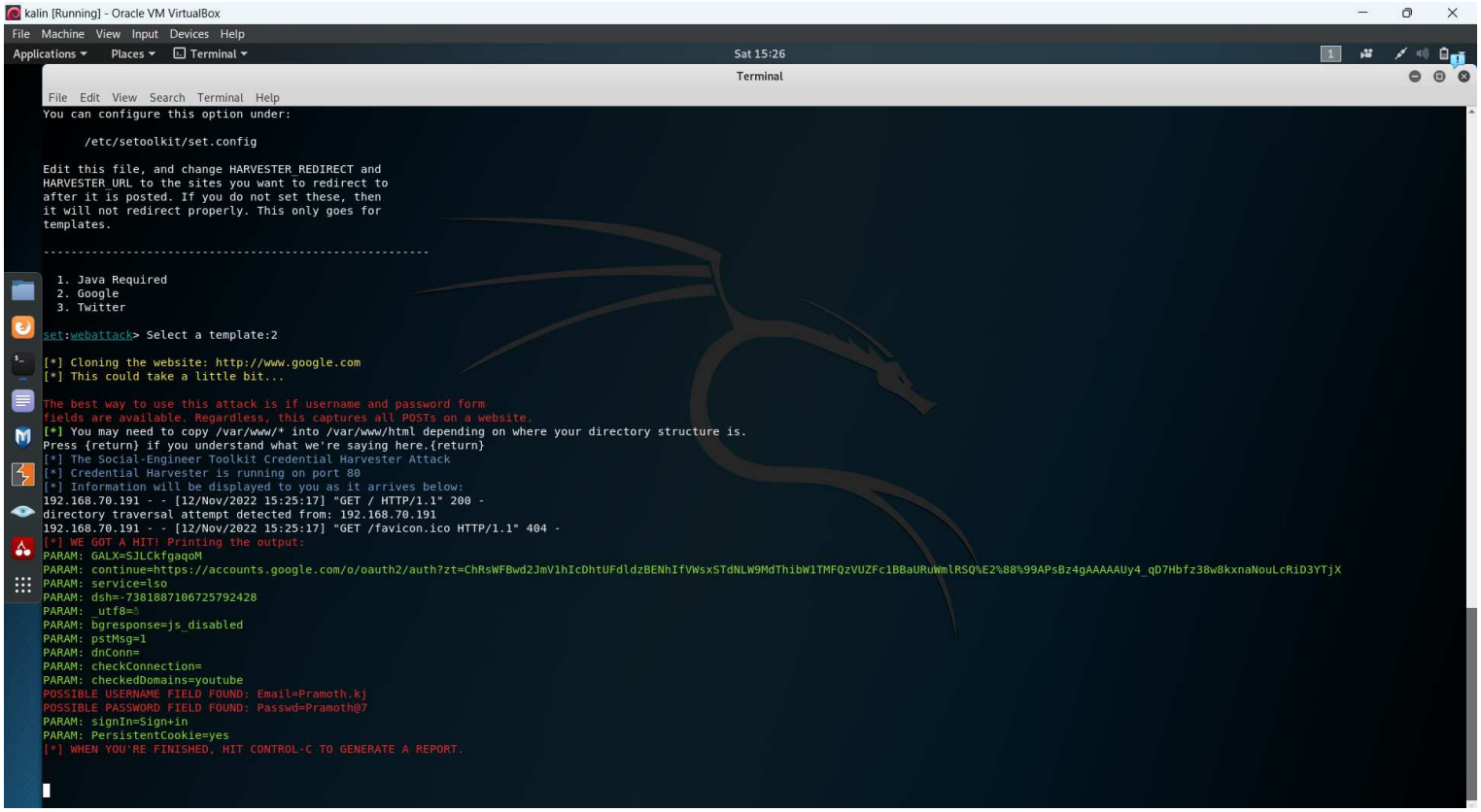
STEP 10:

WHEN YOU SIGN IN THE PAGE REDIRECT TO GOOGLE.COM



STEP 11:

OPEN TERMINAL AND FIND THE USERNAME AND PASSWORD



PREVENTIONS :

1) Never click any link unless it is from the trustrable source.

2) Use antivirus to block suspisious links.

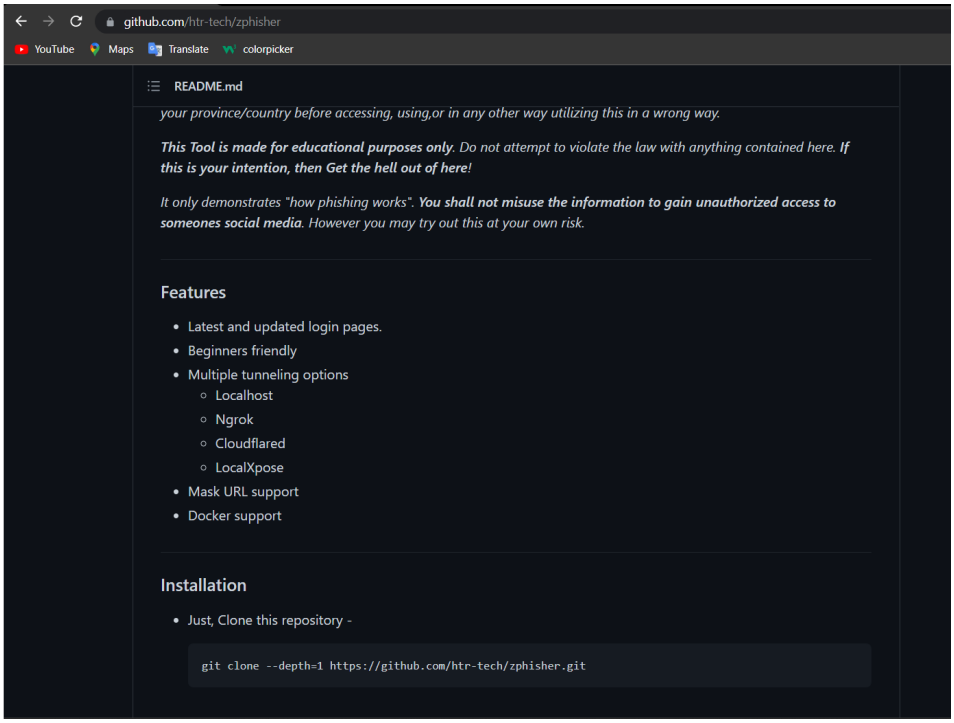
3) Check for SSL certificates so that we can check the link is secure.

4.USING PHISHING TOOL FROM GITHUB FOR A PHISHING PAGE AT LAB SETUP

(I USED ZPHISHER TOOL INSTEAD OF SOCIALPHISH TOOL BECAUSE THE LINK IS NOT WORKING . SIR ALSO TOLD YOU CAN USE ZPHISHER TOOL)

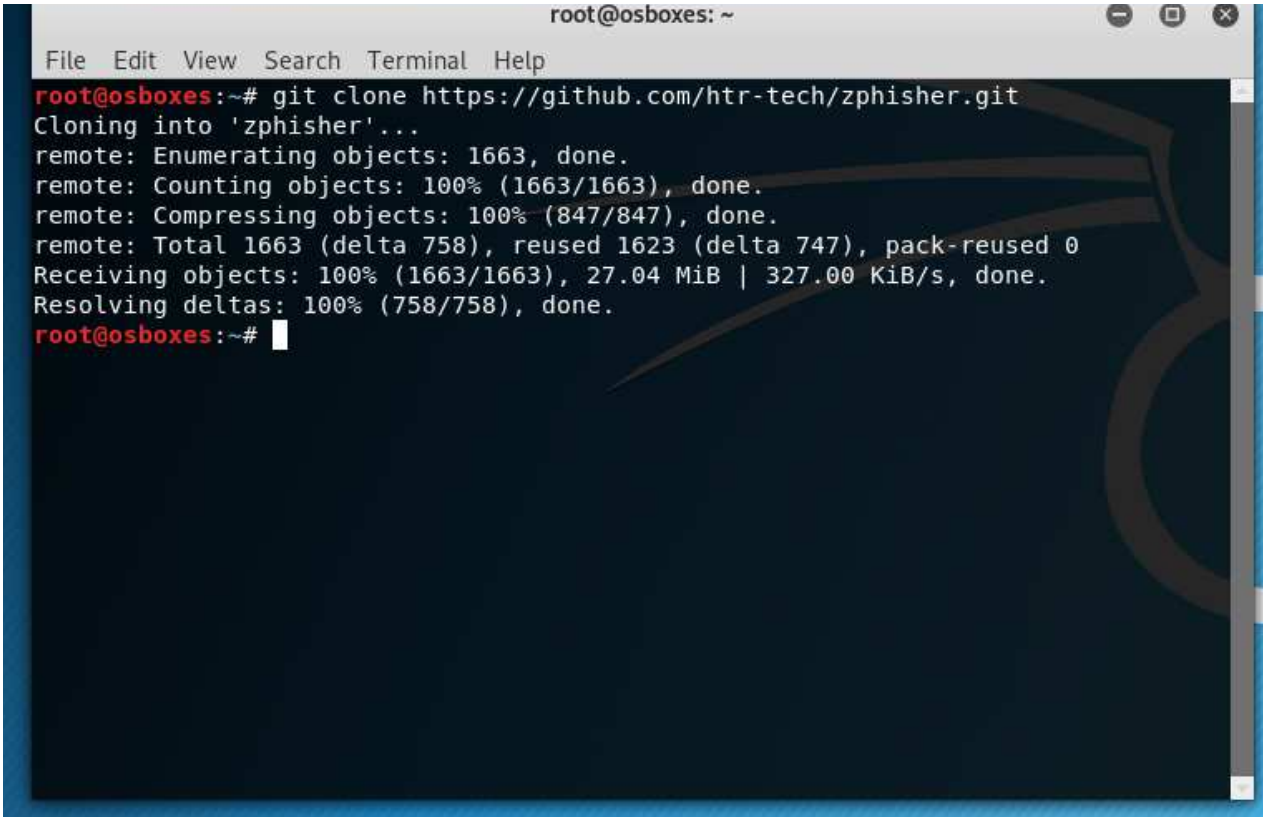
STEP 1:

OPEN GITHUB AND GET THE ZPHISHER LINK



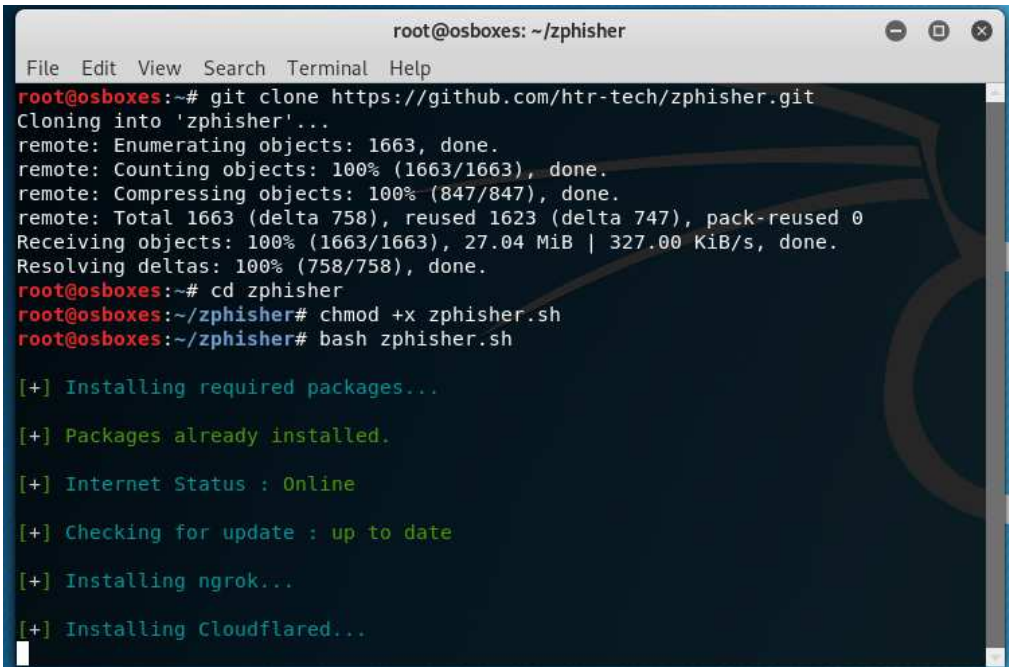
STEP 2:

OPEN KALI LINUX AND PUT THE LINK IN THE TERMINAL



STEP 3:

INSTALLING IN PROGRESS ..

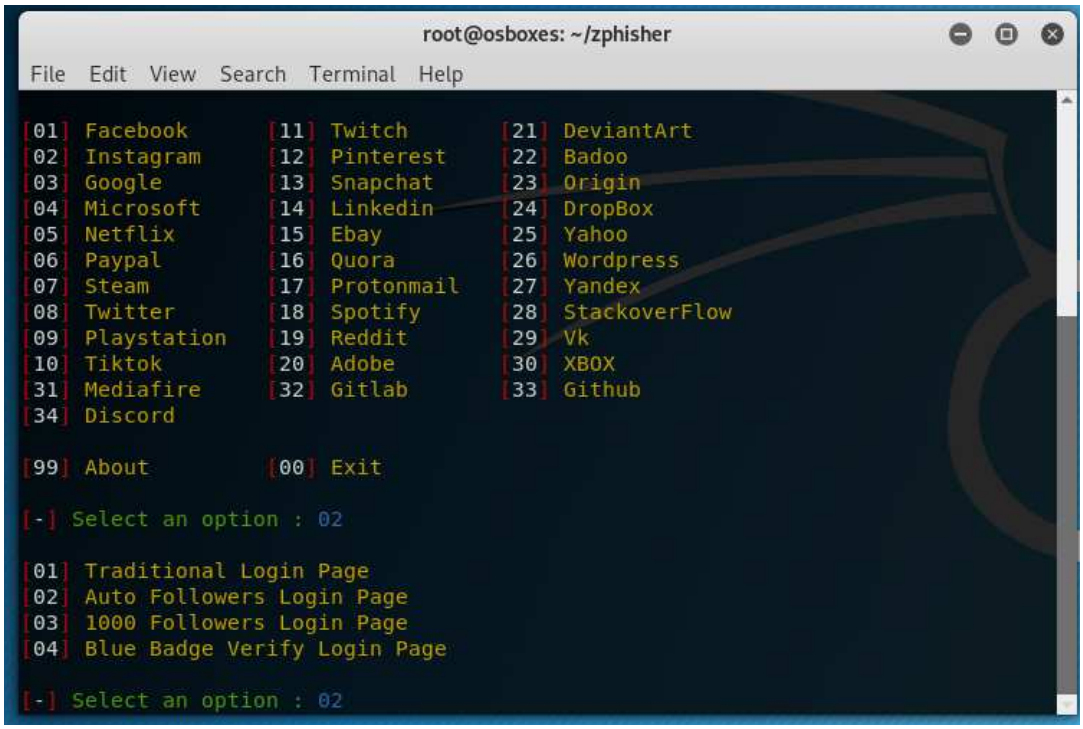


STEP 4:

ZPHISHER TOOL WILL BE OPENED

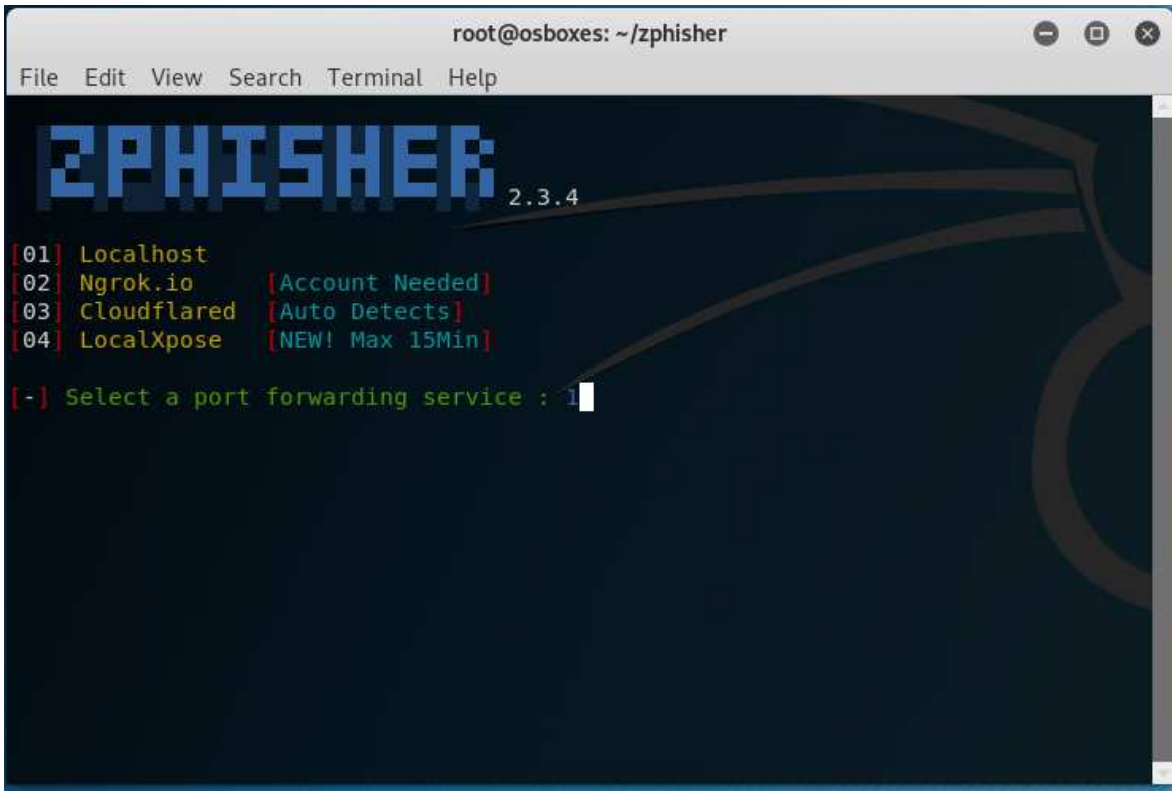
STEP 5:

SELECT THE SOCIAL MEDIA AND AND THE LOGIN PAGE YOU WANT IN THE ABOVE (I'VE SELECTED INSTAGRAM)



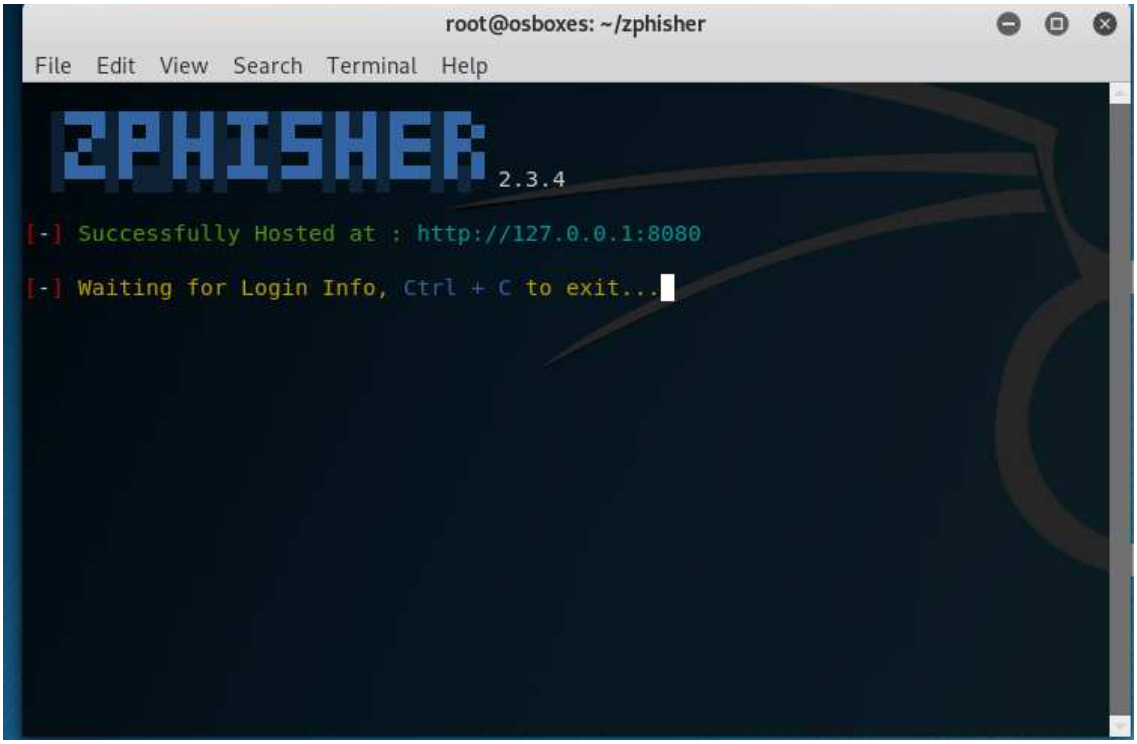
STEP 6:

THE PAGE WILL SHOW "4" OPTIONS TO CREATE LINK



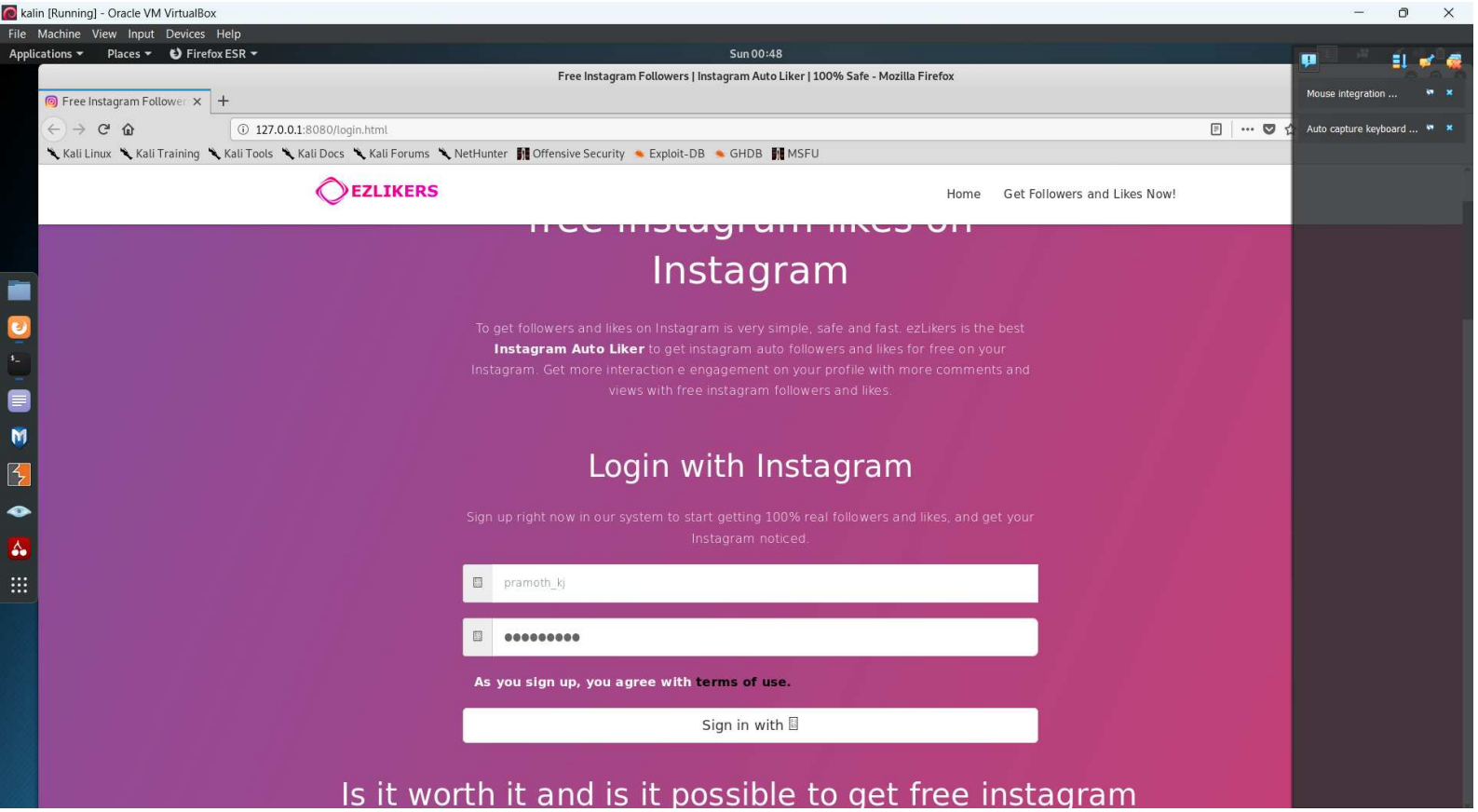
STEP 7:

THE LINK IS CREATED



STEP 8:

IN YOU CAN TYPE ID AND PASSWORD



STEP 9:

THE ID AND PASSWORD IS SHOWN

PREVENTIONS :

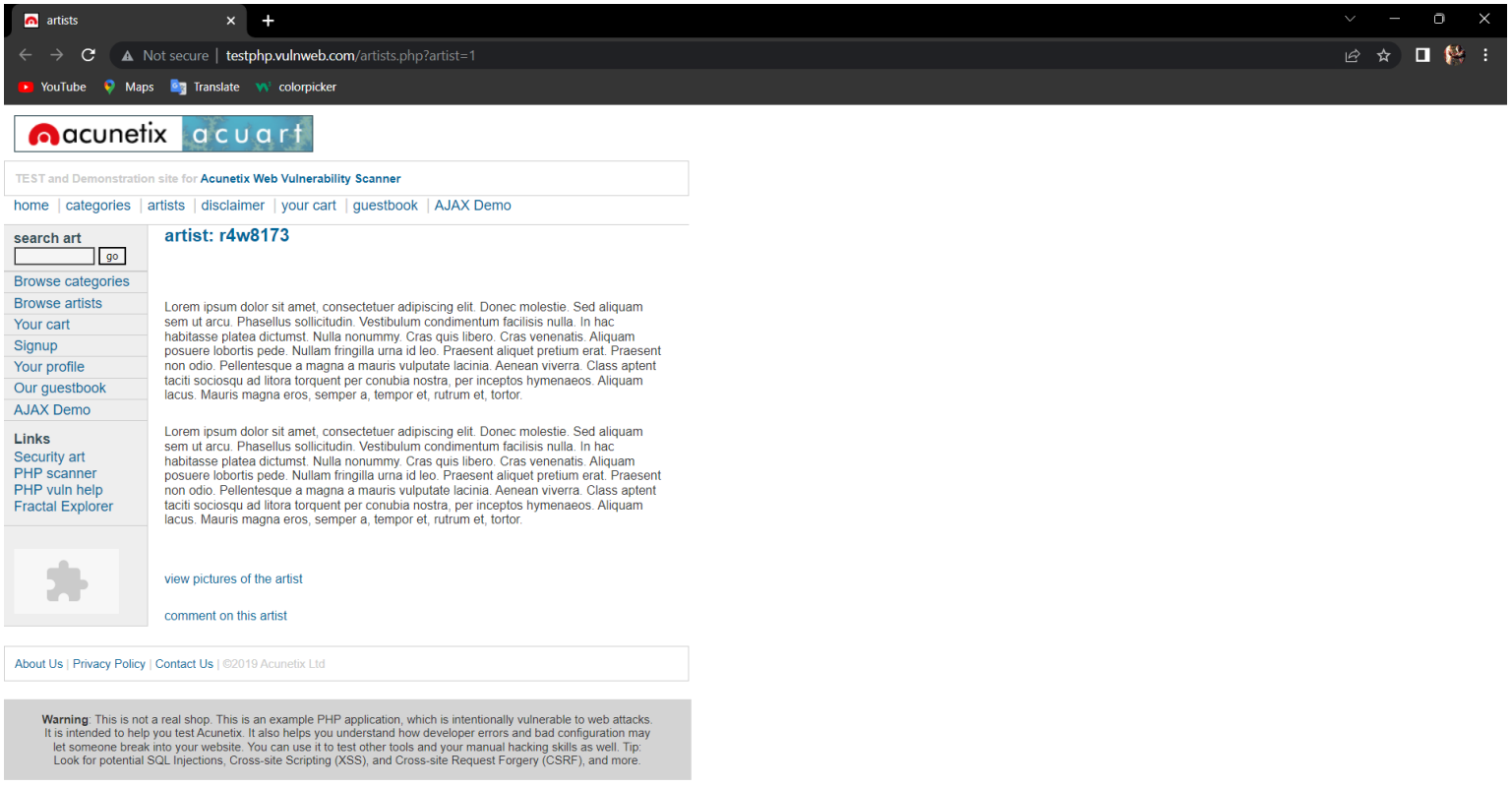
1) AS TOLDNEVER CLICK ANY LINK UNLESS IT IS FROM THE TRUSTRABLE SOURCE.

2) USE ANTIVIRUS TO BLOCK SUSPISIOUS LINKS

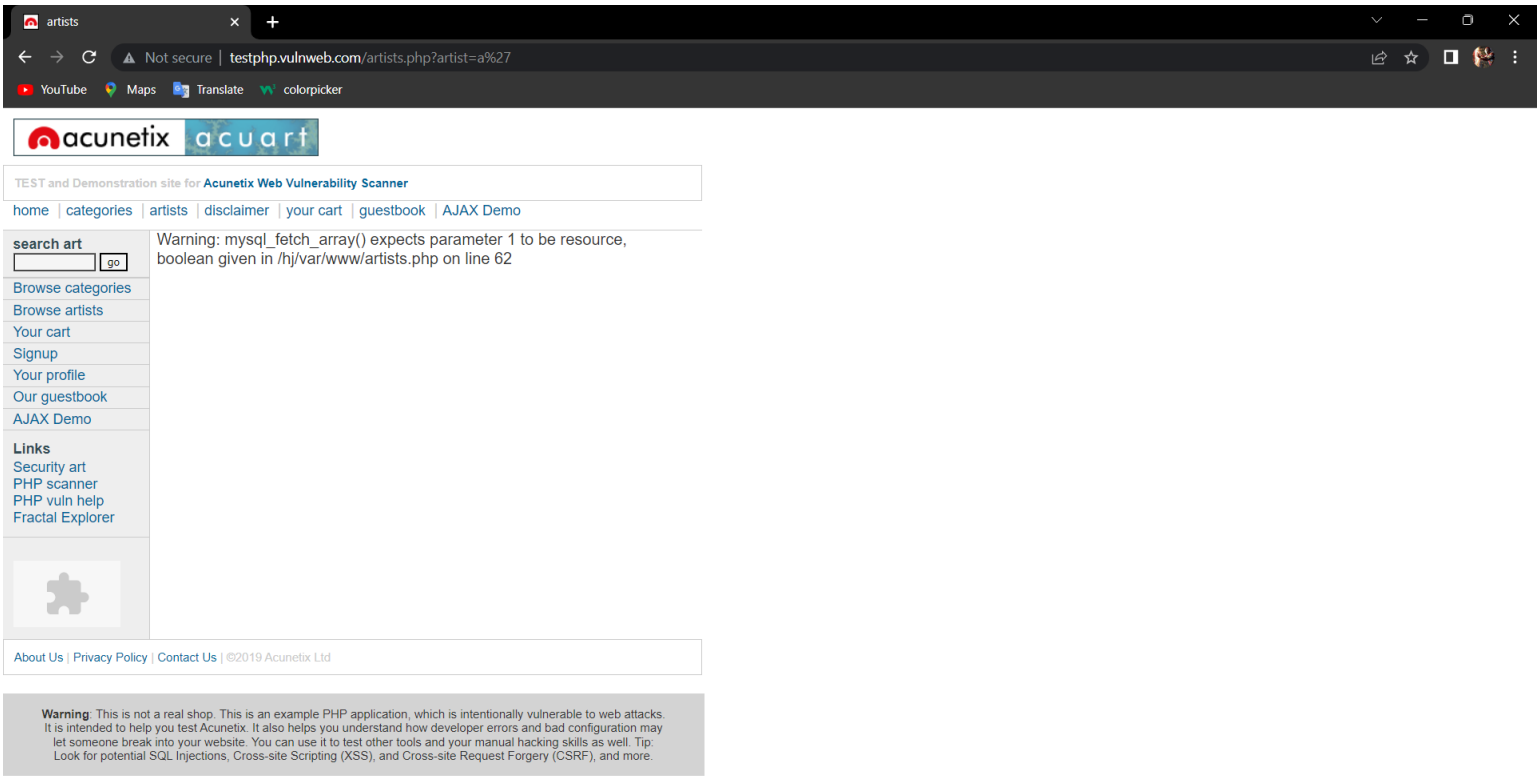
5.PERFORM SQL INJECTION

WEBSITE : HTTP://TESTPHP.VULNWEB.COM

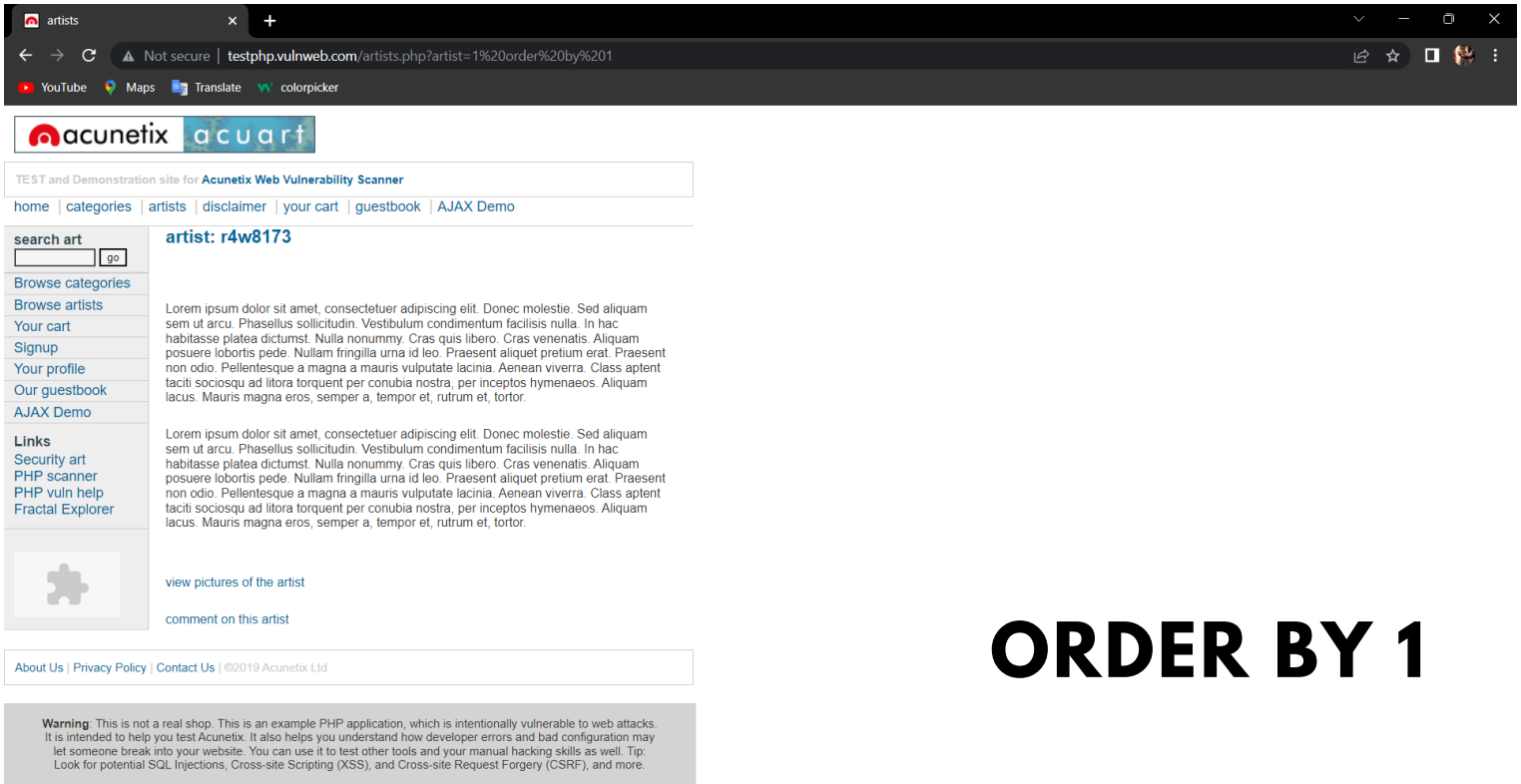
1. YOU NEED TO WHETHER WEBSITE IS CONNECTED TO DB OR NOT (NUMERICAL NUMBERS LIKE ID= ? IN URL'S)



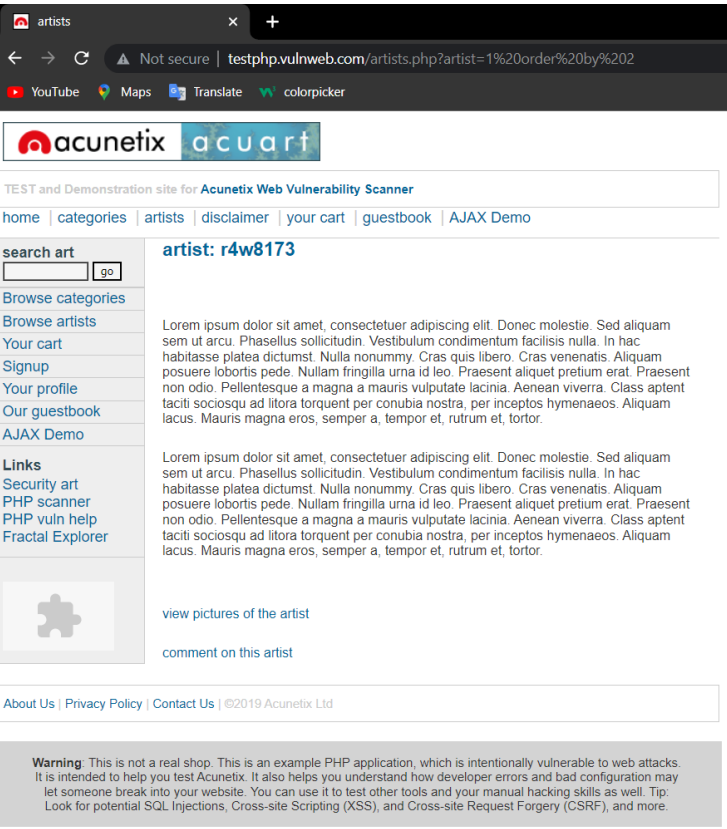
2. WILL CHECK THE VULNERABILITY IS EXISTED OR NOT (INSERT A ' AFTER NUMERICAL NUMBER)



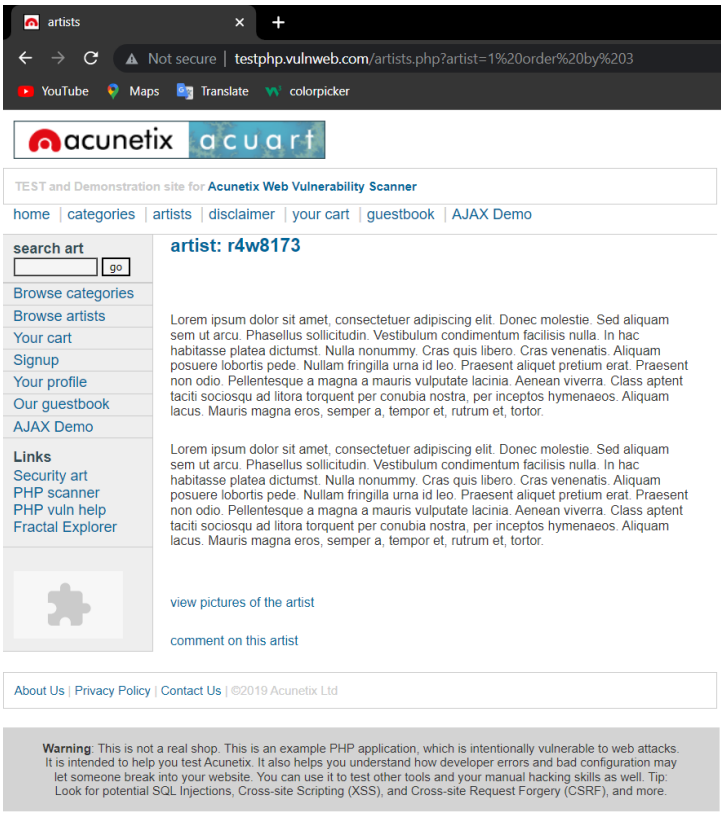
3. WE ARE GNG TO CHECK HOW MANY PUBLIC COLUMNS ARE AVAILABLE (ORDER BY 1,2,3 ETC)



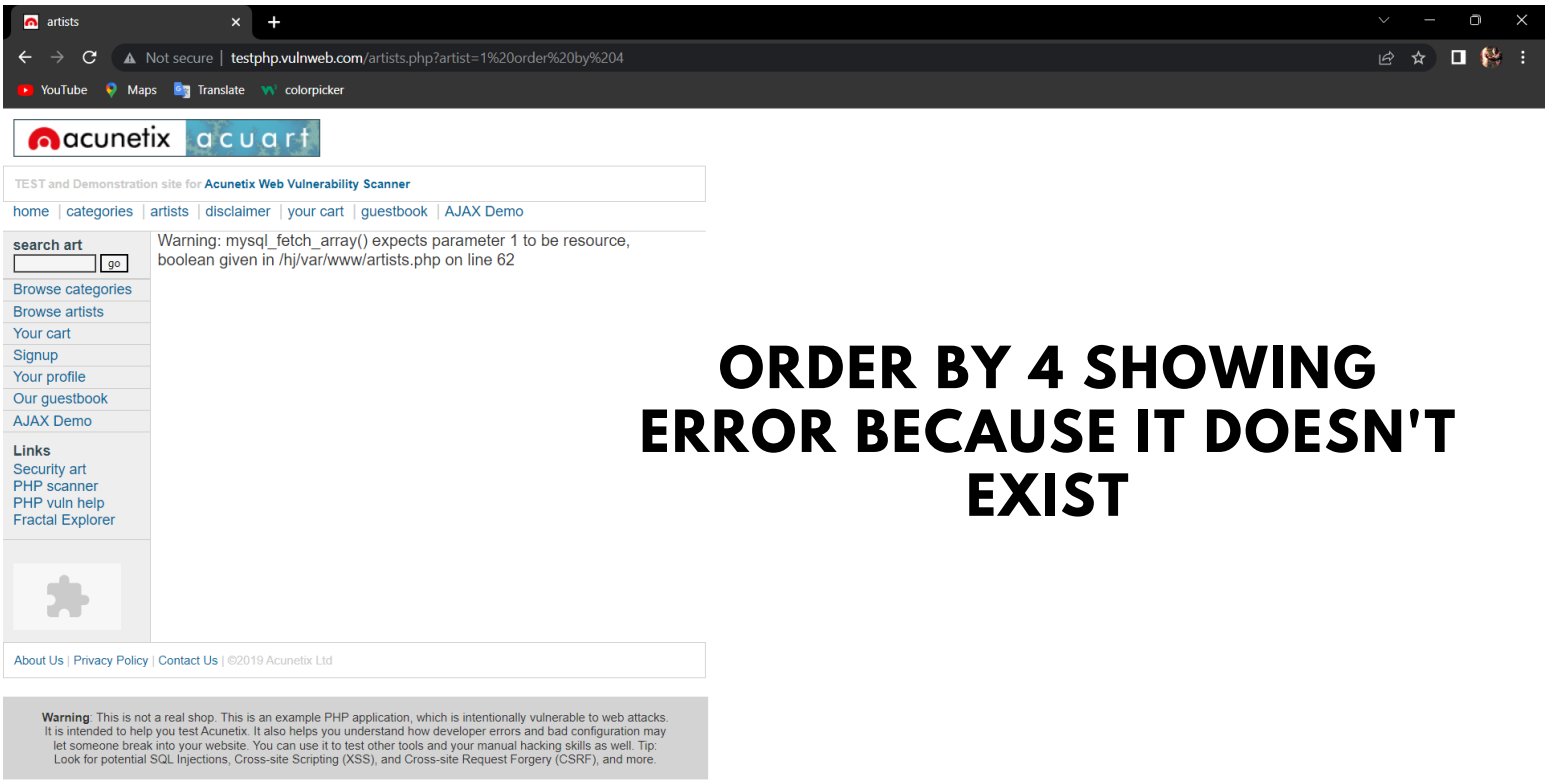
ORDER BY 1



ORDER BY 2

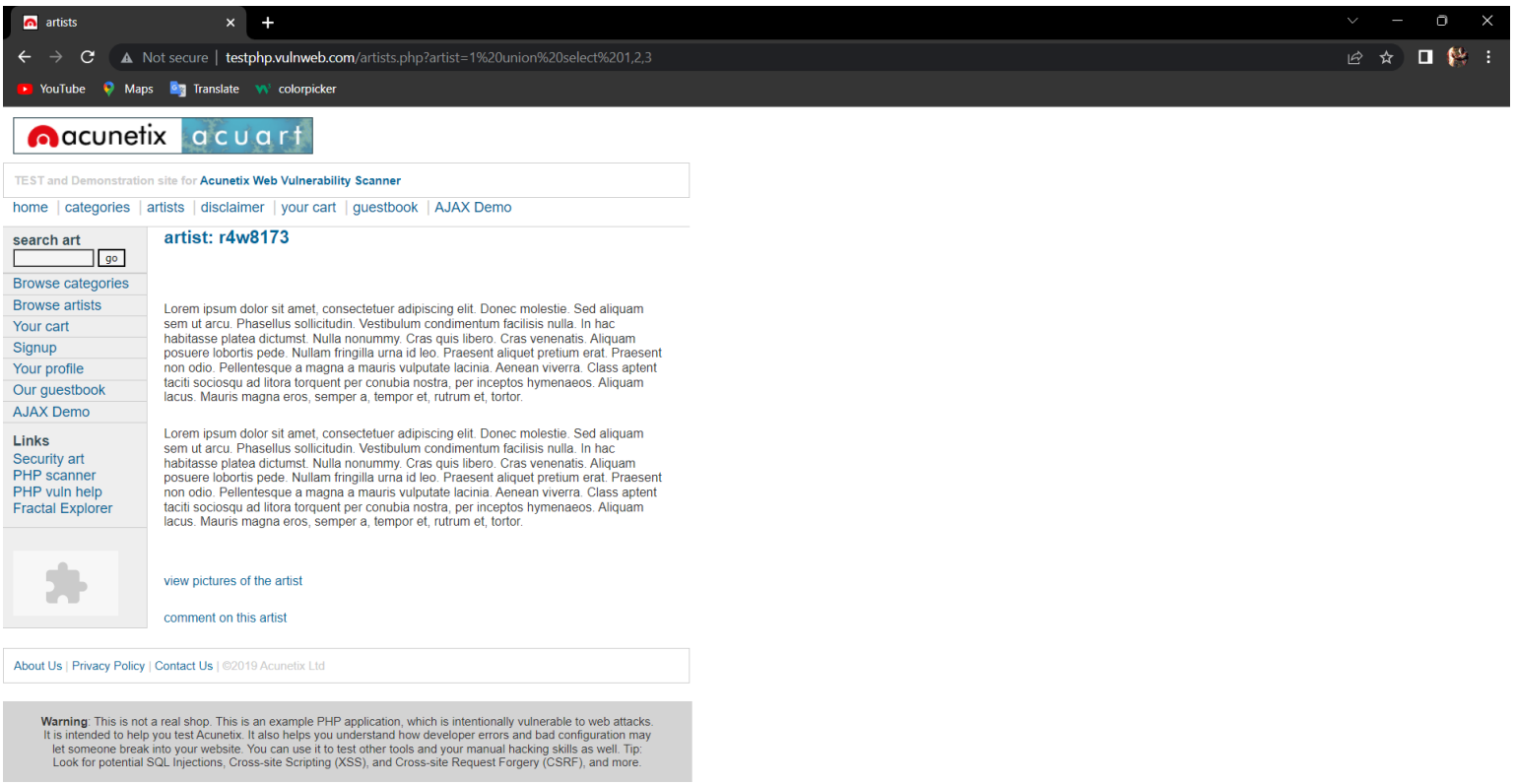


ORDER BY 3



ORDER BY 4 SHOWING ERROR BECAUSE IT DOESN'T EXIST

4. UNION SELECT 1 TO 3 FIND WHICH IS VULNERABLE



5.SO WE CAN FIND THE VULNERABILITIES

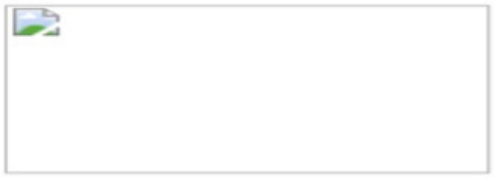
Trees

bla bla bla

painted by: Blad3

comment on this picture

7



2

painted by: 9

comment on this picture

6. FIND THE STRING TO HEX CONVERSION FOR USERS AND FIND COLUMNS PRESENT IN USERS

acunetix acuart

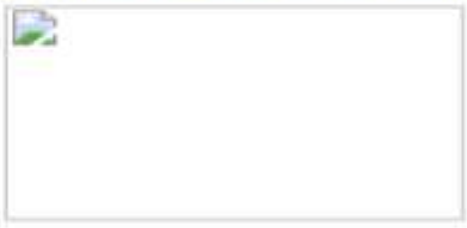
Trees

bla bla bla

painted by: Blad3

comment on this picture

address,cart,cc,email,name,pass,phone,uname

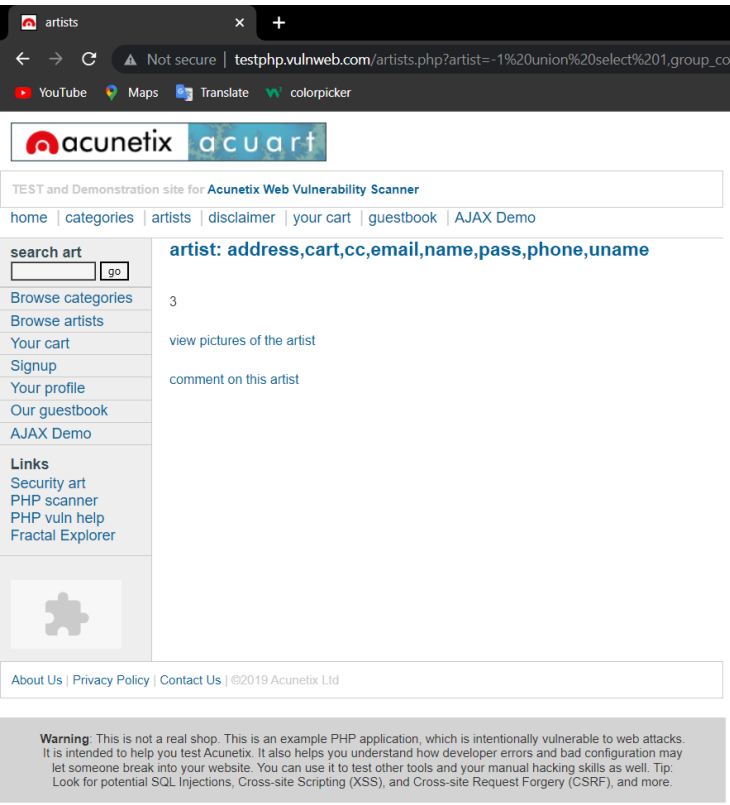


acuart

painted by: 9

comment on this picture

7. REPLACE USING UNAME

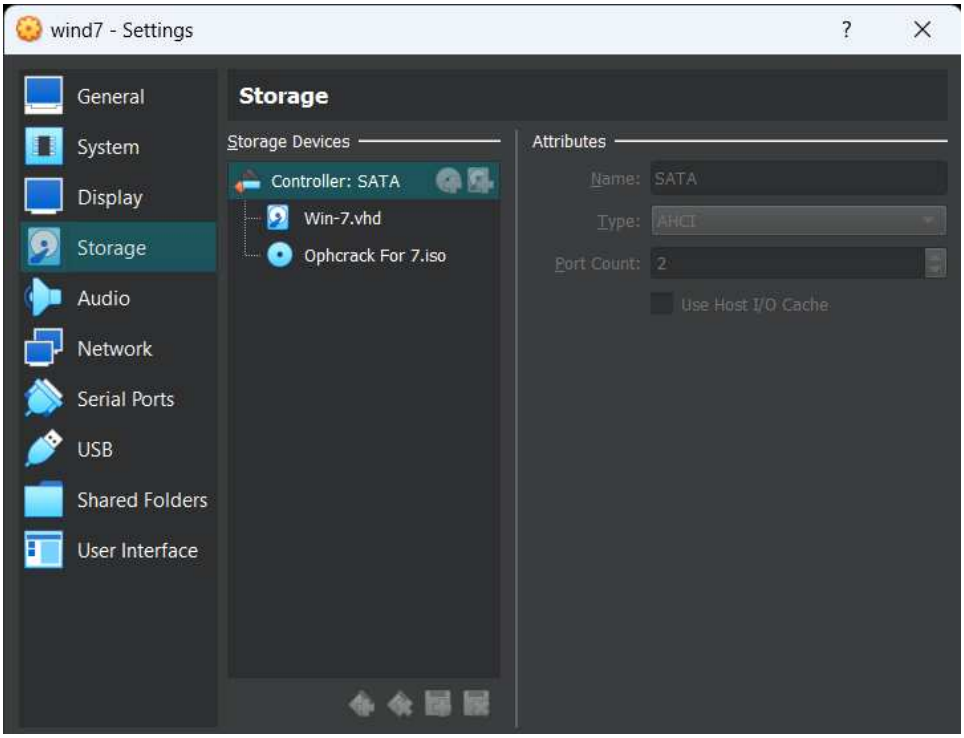


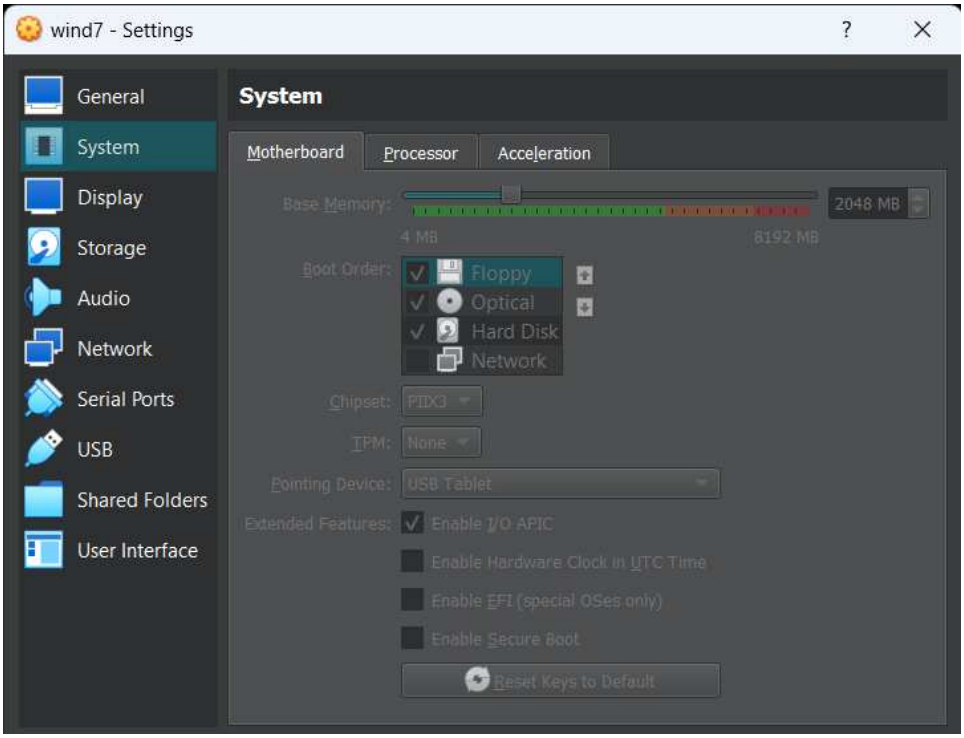
PREVENTIONS

- DATABASE SHOULD BE SECURED. IT SHOULD NOT ACCEPTS COMMAND FROM END USER.
- PAGE HAS TO BE REDIRECTED TO 404 ERROR PAGE IF CHANGES IN LINK OCCURS
- FIREWALL SHOULD BE CONFIGURED PROPERLY AS IT SHOULD NOT BYPASS ANY HEX DECIMALS
- DATA BASE SHOULD NOT ACCEPT ANY SPECIAL CHARACTERS OTHER THAN @

6.WINDOWS PASSWORD CRACKING USING OPHCRACK TOOL

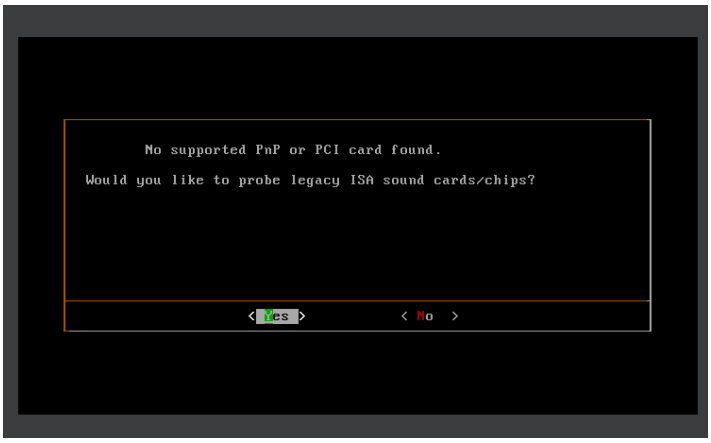
STEP 1: : INSTALL OPHCRACK TOOL AND CONNECT IT TO WINDOWS 7 IN STORAGE AND BOOT ORDER AS OPTICAL DISK

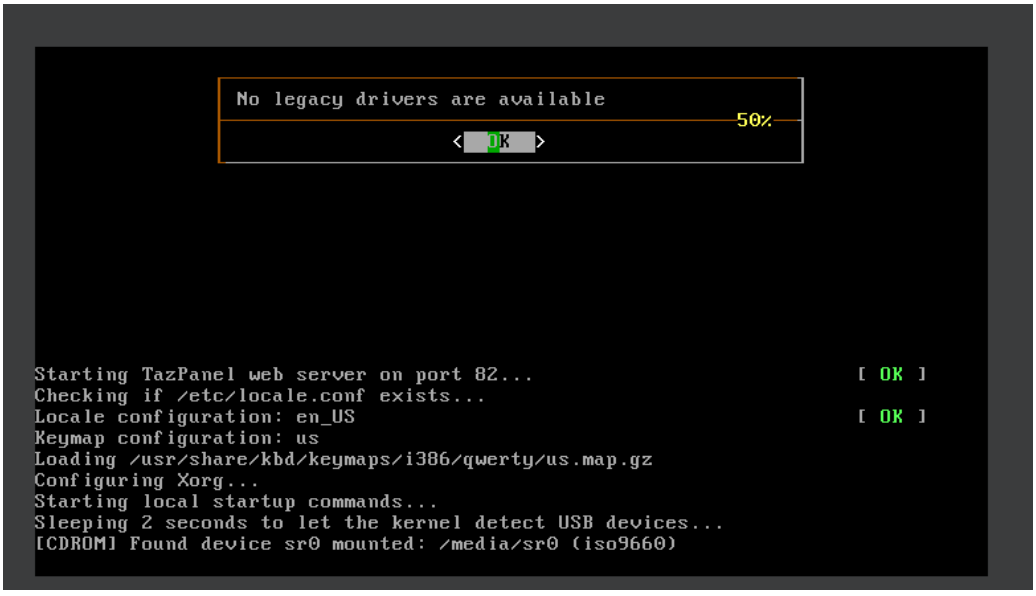




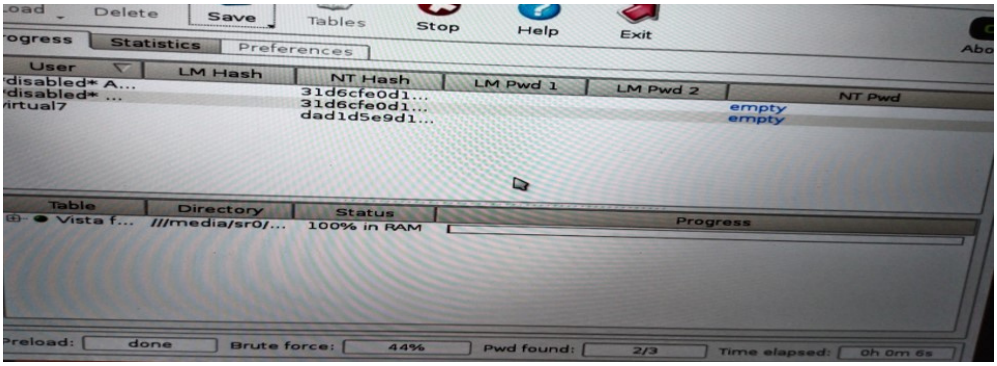
STEP 2: OPEN WINDOWS AND THE OPHCRACK WILL BE OPENED

STEP 3: IT WILL ASK THE PERMISSIONS AND GIVE YES TO ALL

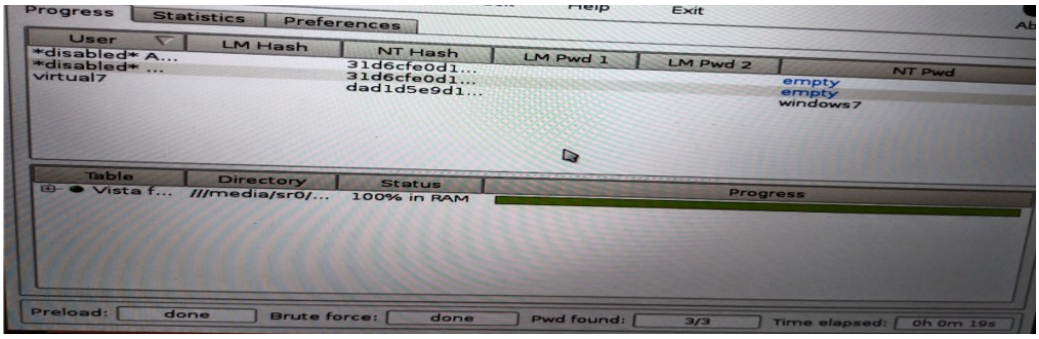




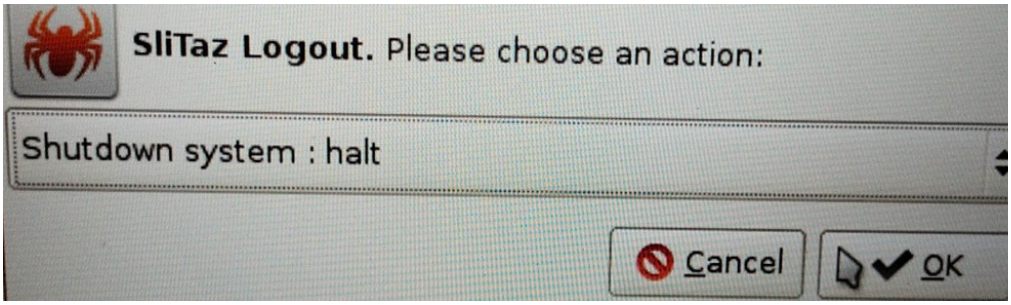
STEP 4: THE OPHCRACK TOOL WILL BE INTIALIZED AND TRY TO CRACK THE PASSWORD



STEP 5 : THE PASSWORD IS CRACKED



STEP 6 : SHUT DOWN THE SYSTEM



STEP 7 : NOW UNSELECT THE OPTICAL DISC OPTION

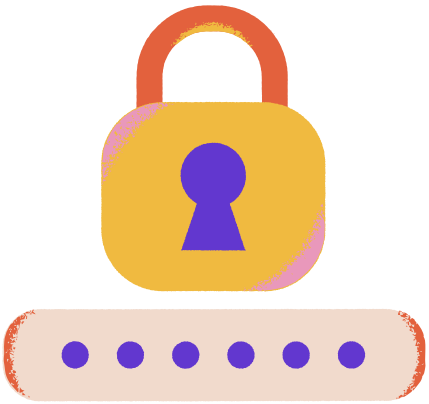
PREVENTIONS :

1) ALWAYS CLOSE THE SYSTEM LOGGED OFF.

2) SET A PASSWORD IN THE BIOS THAT MUST BE ENTERED BEFORE BOOTING THE OPERATING SYSTEM. ALSO SET THE SUPERVISOR PASSWORD IN THE BOIS SO BOIS SETUP CAN'T BE ENTERED WITHOUT IT.

3)FROM BOIS, CHANGE THE BOOT ORDER TO HARD DISK FIRST.

4)SET STRONG PASSWORD ON ALL ACCOUNTS INCLUDING THE ADMINISTRATOR ACCOUNT.



7.ARTICLE ON CYBER SECURITY

Cybersecurity is the practice of protecting computer networks and systems from digital attacks. These attacks can come in the form of viruses, malware, phishing scams, and more. In recent years, cybersecurity has become a hot-button issue due to the increasing number of high-profile attacks. Some of the most notable attacks include the WannaCry ransomware attack, the NotPetya malware attack, and the Equifax data Breach.

The WannaCry ransomware attack was a global cyberattack that took place in May of 2017. The attack used a piece of malware called WannaCry to encrypt files on victims' computers. The attackers then demanded a ransom in order to decrypt the files. The WannaCry attack affected over 200,000 computers in 150 countries.

The NotPetya malware attack was a cyberattack that took place in June of 2017. The attack used a piece of malware called NotPetya to encrypt files on victims' computers. The attackers then demanded a ransom in order to decrypt the files. The NotPetya attack affected over 10,000 computers in 64 countries.

The Equifax data breach was a data breach that took place in July of 2017. The breach exposed the personal information of over 145 million people. The Equifax data breach is considered to be one of the largest data breaches in history.

I learned about the different types of attacks that can be used to target a computer system. These include denial of service attacks, malware attacks, and phishing attacks. I also learned about the different methods that can be used to protect against these attacks. These include firewalls, antivirus software, and spam filters.

TOPIC LEARNED IN THIS COURSE

Now let's see how the Nmap tool can be used with the Nmap Scripting Engine (NSE) to get more information about the open ports.

Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) is a powerful tool for information gathering. It can be used to scan for specific ports and services. It can also be used to gather more information about the open ports.

Let's see how NSE can be used to scan for HTTP servers using the command nmap -sS -T4 -A -v -p 80 127.0.0.1 .

We can see that there are two HTTP servers running in the system.

The output of the Nmap tool shows that there is an HTTP server running on port 80. NSE can also be used to gather more information about the HTTP server.

The command nmap -sS -T4 -A -v -p 80 --script=http-headers 127.0.0.1 can be used to gather more information about the HTTP server.

The output of the command shows the HTTP headers of the server. This information can be used to find the version of the server and the operating system it is running on.

The Nmap tool can also be used to scan for specific ports and services.

The command nmap -sS -T4 -A -v -p- 127.0.0.1 can be used to scan for all ports in the system.

The output of the command shows all the ports in the system.

The Nmap tool can also be used to gather information about the operating system of the system.

The command nmap -sS -T4 -A -v -O 127.0.0.1 can be used to gather information about the operating system.

The output of the command shows that the system is running on Windows.

The Nmap tool can also be used to scan for specific ports and services.

The command nmap -sS -T4 -A -v -p 22,80,443 127.0.0.1 can be used to scan for specific ports.

The output of the command shows that the ports are open.

The Nmap tool can also be used to gather information about the services running on the system.

The command nmap -sS -T4 -A -v -sV 127.0.0.1 can be used to gather information about the services running on the system.

The output of the command shows that the system is running SSH and HTTP services.

The Nmap tool can also be used to scan for specific ports and services.

The command nmap -sS -T4 -A -v -p 22 --script=ssh-hostkey 127.0.0.1 can be used to scan for specific ports and gather information about the SSH service.

The output of the command shows the host key of the SSH service. This information can be used to authenticate to the SSH service.