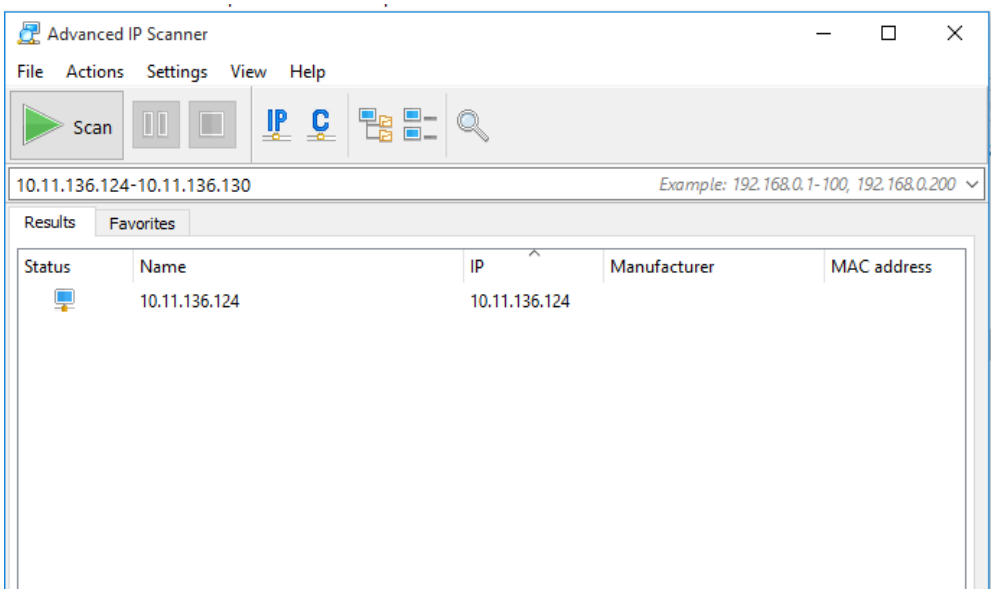
Scanning Network
Module 3 (Lab Assignment)

Name : Sachin Saj T K
Roll NO : CB.EN.P2CEN18012
Date of Submission: 1/06/19

Lab Objective:

- Check live system and open ports
- Perform banner grabbing and OS fingerprinting
- Identify Network Vulnerabilities
- Draw Network Diagrams of Vulnerable hosts.

Scanning system and network resources using advanced IP scanner



Tool/Utility	Information Collected/Objective Achieved
Advance IP Scanner	Scan Information: **IP address**: 10.11.136.124 **System Name**:10.11.136.124 **MAC address**: nil **NetBIOS information**: nil **Manufacturer**: nil **System status**: Not Alive

Banner Grabbing to Determine a remote target system using ID serve

Tools/Utility	Information Collected/Objective Achieved
ID Serve	**IP Address**:162.241.216.11
	Server Connection: HTTP port 80
	Response headers returned from server: **HTTP** / 1.1 200 OK **Server:** Apache **X-Powered-By**: PHP/4.4.8 **Transfer-Encoding**: gzip **Content-Type**: text/html

Monitoring TCP/IP connections using the CurrPorts tool

1. All the items report

TCP/UDP Ports List

Created by using CurrPorts

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Sent Bytes	I
chrome.exe	640	TCP	51366		10.0.2.15	443	https	172.217.160.131	maa03s29-in-f3.1e100.net	Close Wait		
chrome.exe	640	TCP	51378		10.0.2.15	443	https	185.199.111.154		Established		
chrome.exe	640	TCP	51379		10.0.2.15	443	https	185.199.111.154		Established		
chrome.exe	640	TCP	51399		10.0.2.15	443	https	216.58.197.42	maa03s20-in-f10.1e100.net	Established		
chrome.exe	640	TCP	51400		10.0.2.15	443	https	172.217.26.163	maa03s22-in-f3.1e100.net	Established		
chrome.exe	640	TCP	51402		10.0.2.15	443	https	172.217.163.104	maa05s03-in-f8.1e100.net	Established		
chrome.exe	640	TCP	51404		10.0.2.15	443	https	172.217.166.110	maa05s09-in-f14.1e100.net	Established		
chrome.exe	640	TCP	51411		10.0.2.15	443	https	172.217.163.206	maa05s06-in-f14.1e100.net	Established		
chrome.exe	640	TCP	51412		10.0.2.15	443	https	216.58.197.33	maa03s20-in-f33.1e100.net	Established		
chrome.exe	640	TCP	51415		10.0.2.15	443	https	151.101.154.180		Established		

2. Selected items report

TCP/UDP Ports List

Created by using CurrPorts

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets	Receiv Packe
chrome.exe	640	TCP	51462		10.0.2.15	80	http	104.91.48.141	a104-91-48-141.deploy.static.akamaitechnologies.com	Established				
chrome.exe	640	TCP	51464		10.0.2.15	80	http	216.58.200.142	maa05s10-in-f14.1e100.net	Established				
chrome.exe	640	TCP	51487		10.0.2.15	80	http	172.217.167.129	maa03s26-in-f1.1e100.net	Established				
chrome.exe	640	TCP	51498		10.0.2.15	80	http	192.229.237.25		Established				

3. Properties of the port

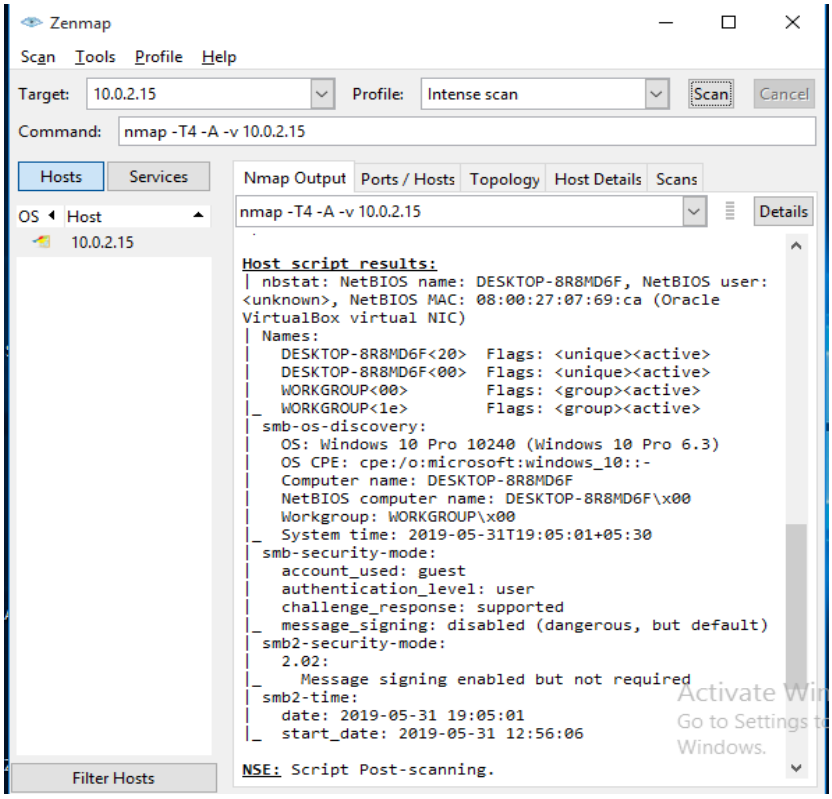
Properties

Process Name:	chrome.exe
Process ID:	640
Protocol:	TCP
Local Port:	51464
Local Port Name:	
Local Address:	10.0.2.15
Remote Port:	80
Remote Port Name:	http
Remote Address:	216.58.200.142
Remote Host Name:	maa05s10-in-f14.1e100.net
State:	Established
Sent Bytes:	
Received Bytes:	
Sent Packets:	
Received Packets:	
Process Path:	C:\Program Files (x86)\Google\Chrome\Application\cl
Product Name:	Google Chrome
File Description:	Google Chrome
File Version:	74.0.3729.169
Company:	Google Inc.
Process Created On:	31-05-2019 13:12:15
User Name:	DESKTOP-8R8MD6F\Sachin
Process Services:	
Process Attributes:	A

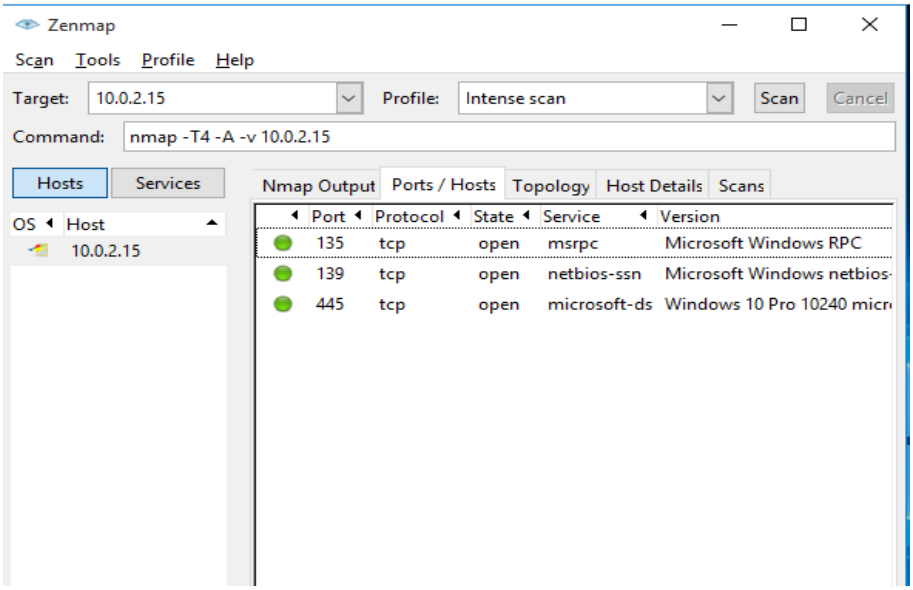
Tool/Utility	Information Collected/Objective Achieved
CurrPorts	Scanned Report: **Process Name**: chrome.exe **Process ID**: 640 **Protocol:** TCP **local Port**: 51434 **local Address**: 10.0.2.15 **Remote Port**: 443 **Remote Port address**: https **Remote address**: 172.217.163.98 **Remote host name**: maa05s03-in-f2.1

Exploring and Auditing a Network using Nmap

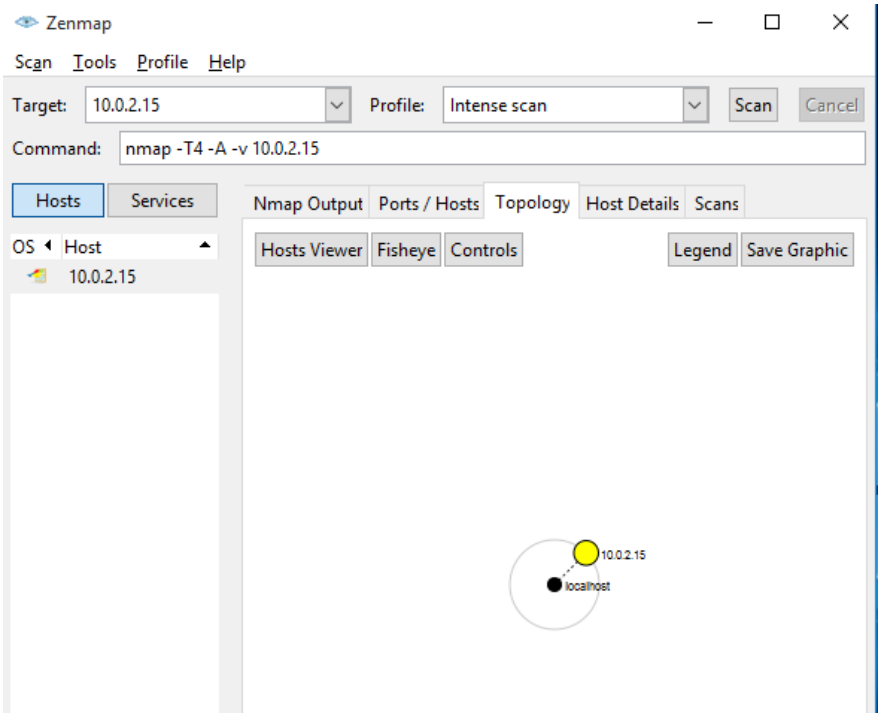
1. Scan 10.0.2.15 (IP address of my virtual machine)



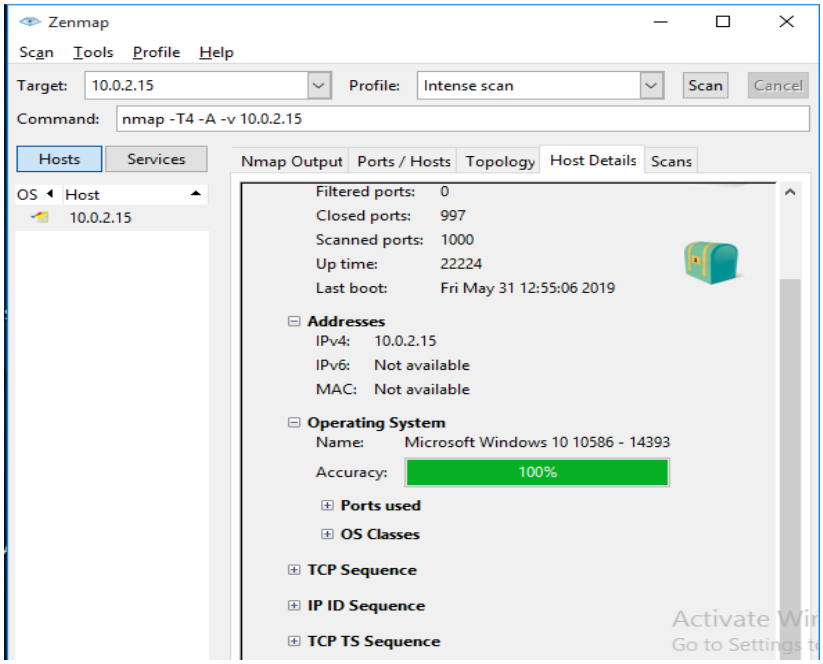
2. About Ports details



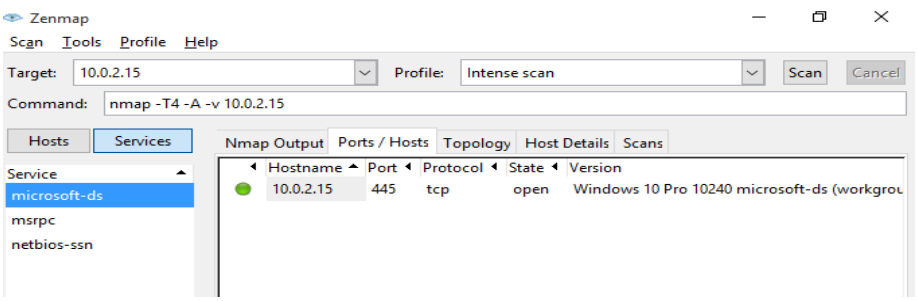
3. Topology details

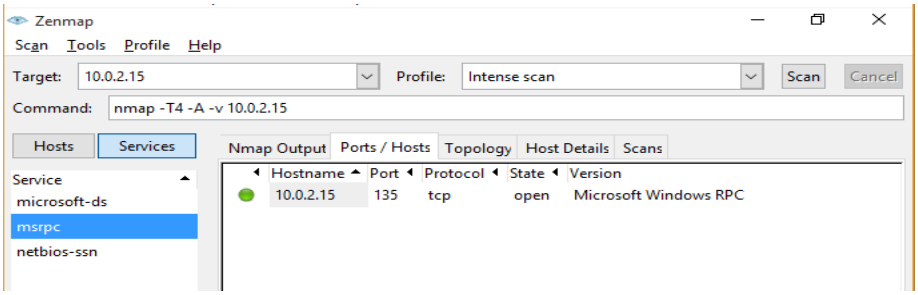


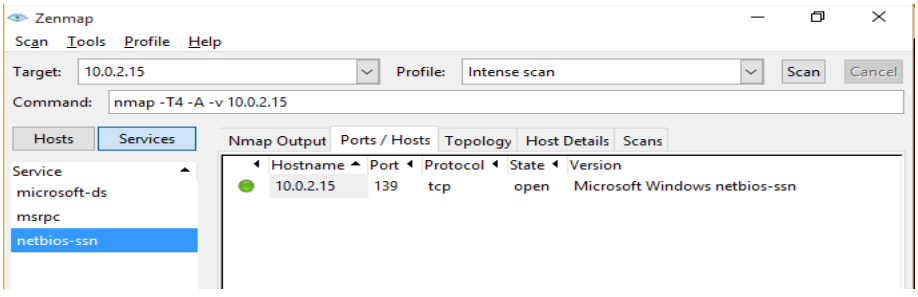
4. Host Details



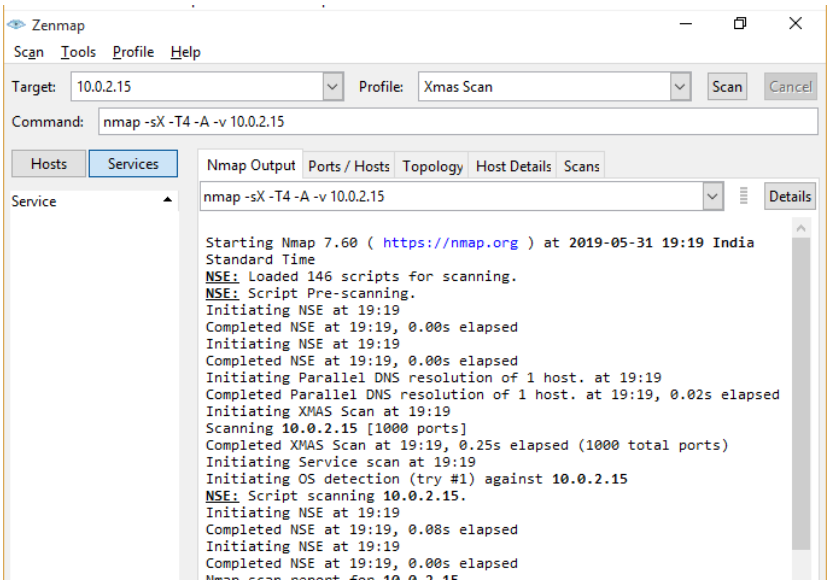
5. Details from Services tab



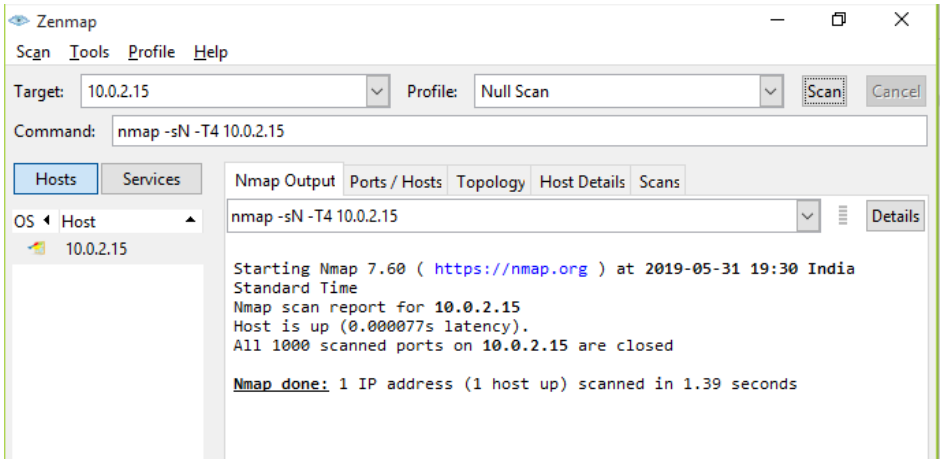


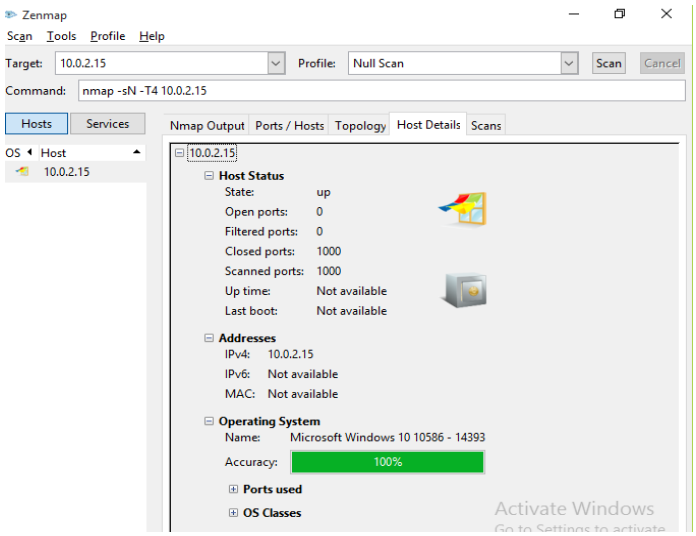


5. Xmas Scan

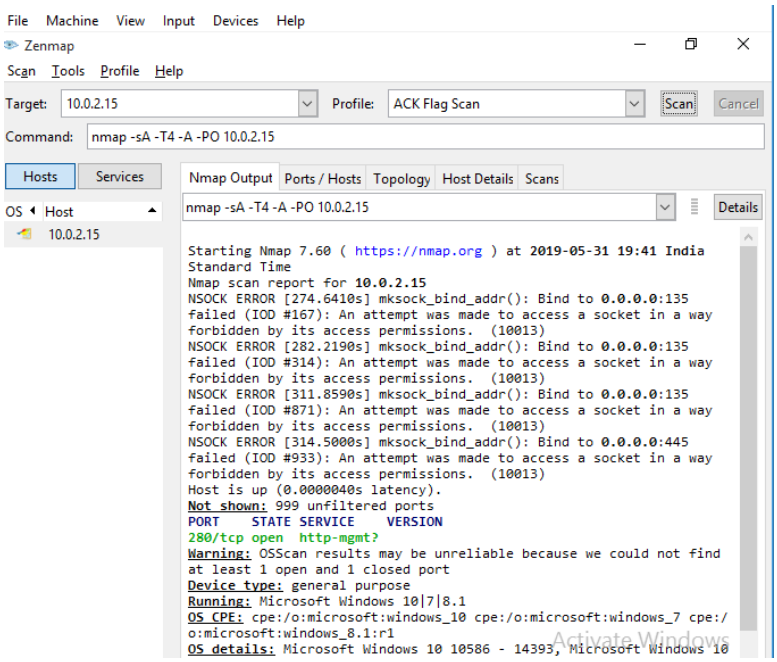


6. Null Scan





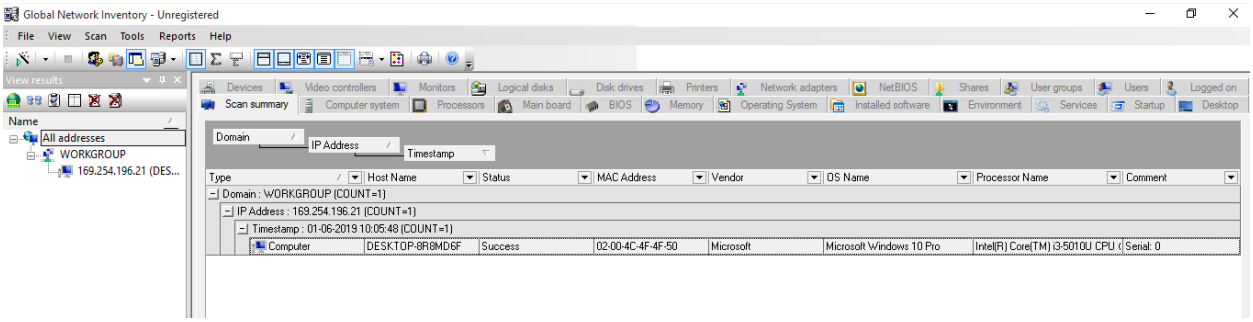
7. Ack Flag Scan



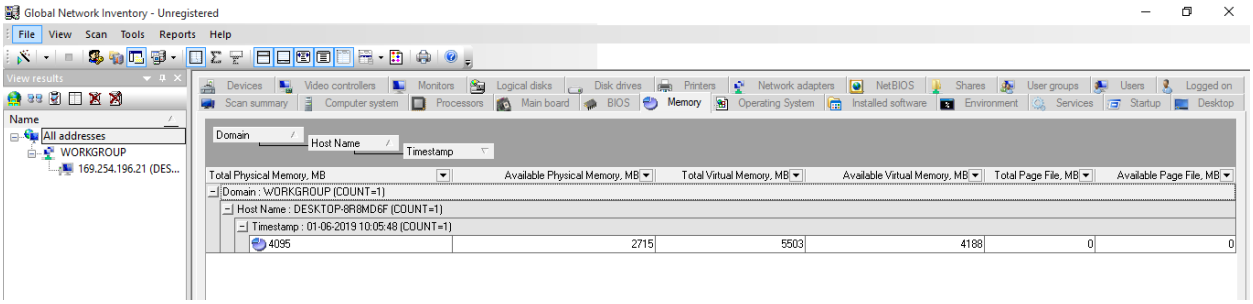
Tool/Utility	**Information Collected/Objective Achieved**
Nmap	**Types of Scan used**: Intense Scan Xmas Scan Null Scan ACK Flag scan
	ARP Ping Scan – 1 host Parallel DNS resolution of 1 host SYN stealth scan Discovered open port on 10.0.2.15 139/tcp,139/tcp,445/tcp **MAC address**: nil **Operating System Details**: Windows 10 Pro **Uptime Guess**: 22224 **Network Distance**: 0 hops **TCP Sequence Prediction:** 114875B2 **IP ID Sequence Generation**: 54D4

Auditing Scanning by using Global Network Inventory

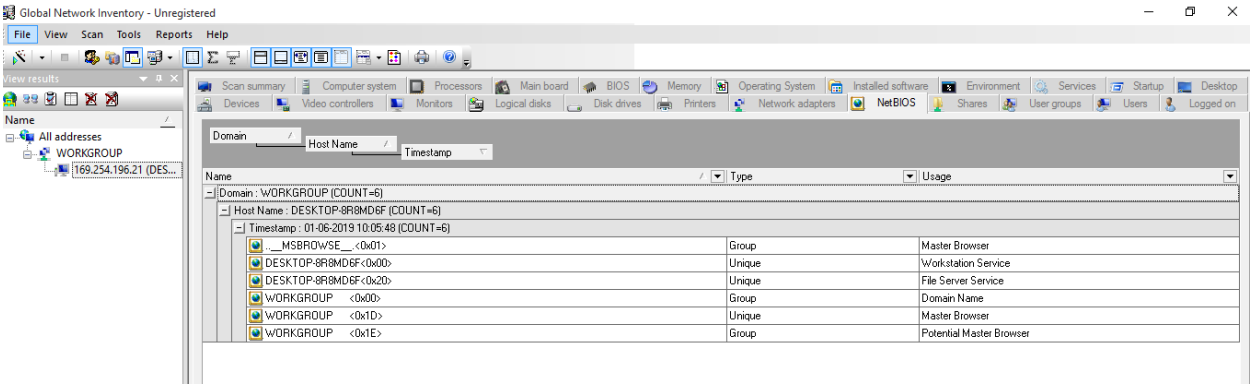
1. Scanning IP address range



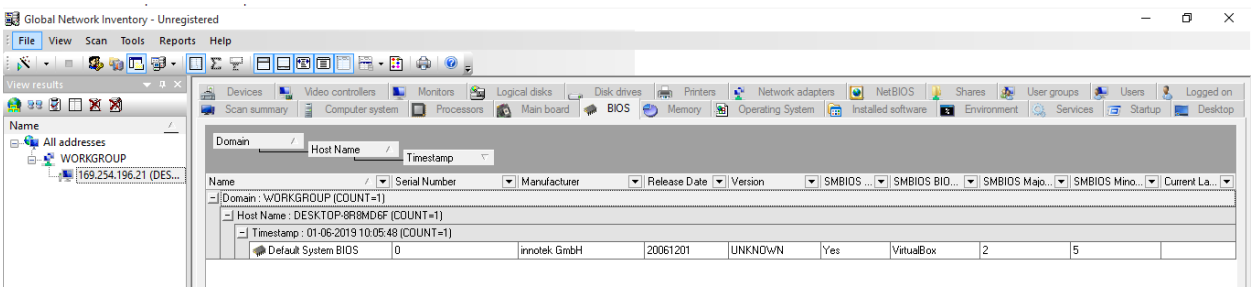
2. Memory of the scanned device



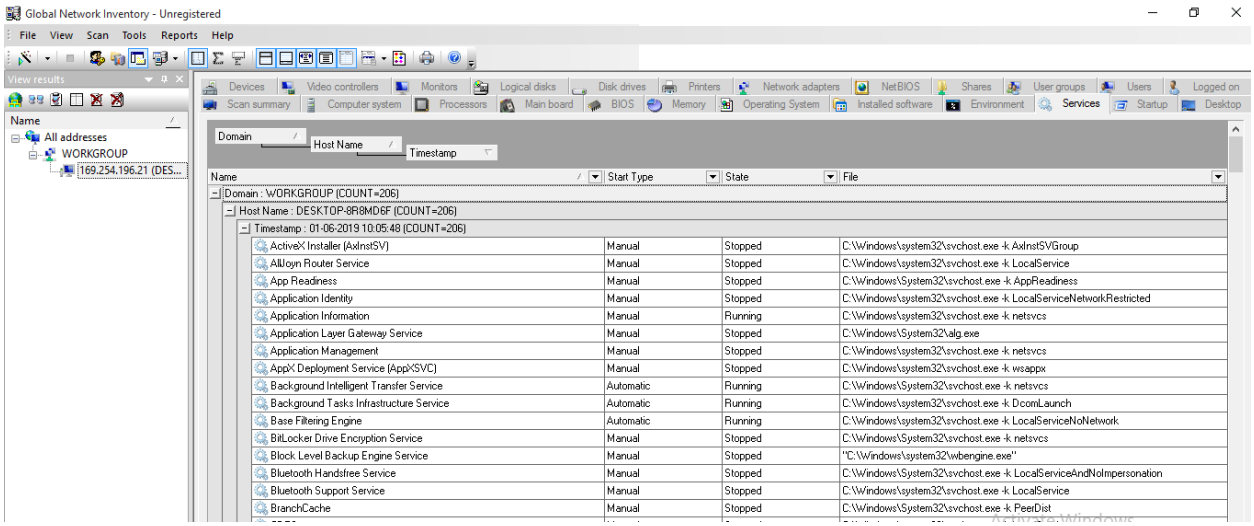
3. NetBIOS



4. BIOS

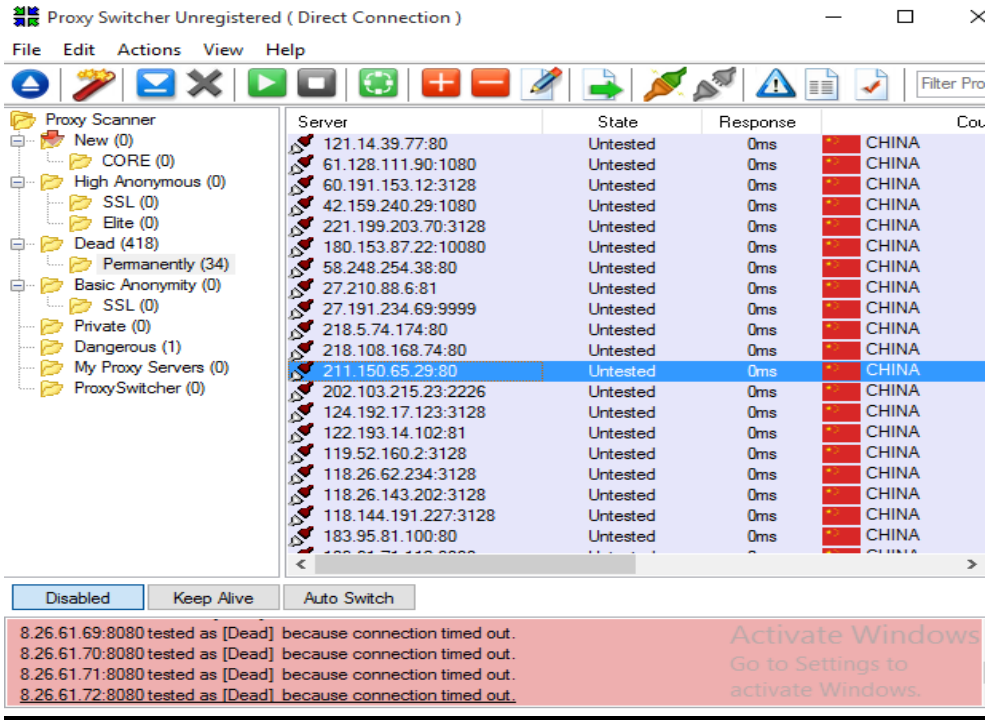


5. Services



Tool/Utility	**Information Collected/Objective Achieved**
Global Network Inventory	**IP Scan Range:** 169.254.196.1 – 169.254.196.255
	Scanned IP Address: 169.254.196.21
	Result: **Scan Summary:** Given Above **BIOS:** Given Above **Memory:** Given Above **NetBIOS:** Given Above **Services:** Given Above

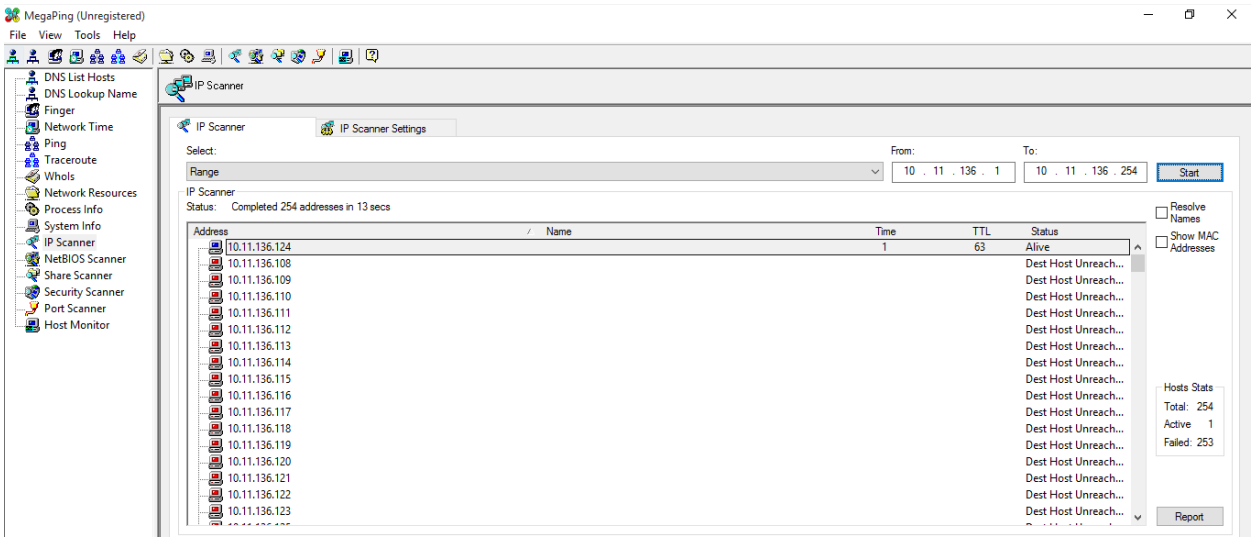
Anonymous Browsing using Proxy Switcher



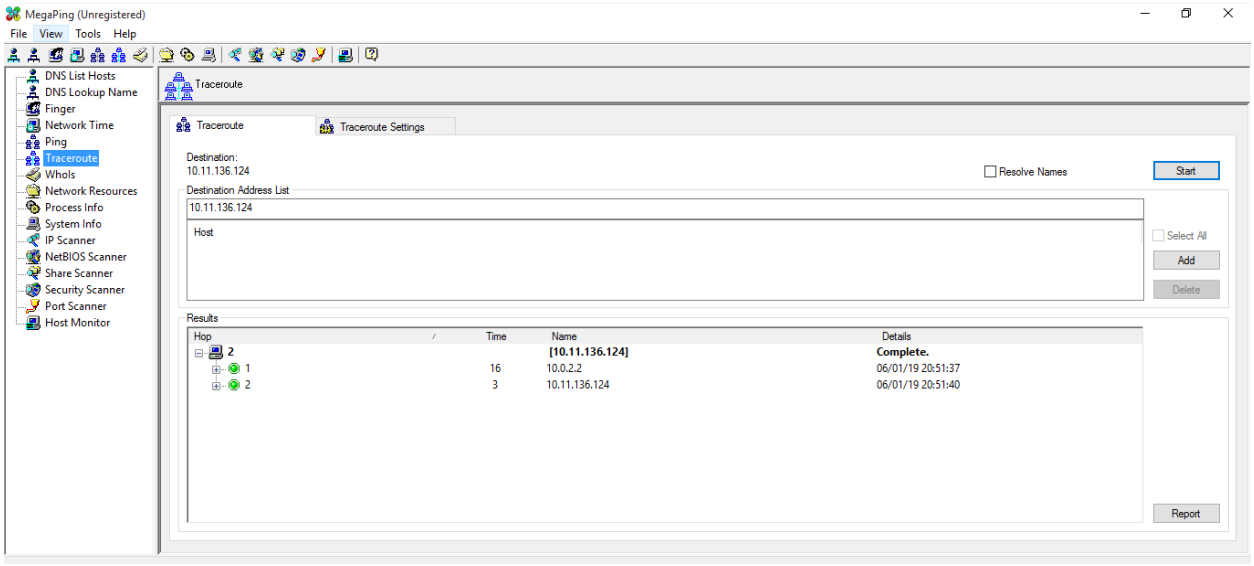
Since, when scanned all the ports are dead and there is no port alive, we were not able to connect to the proxy server.

Daisy Chaining using Proxy Workbench

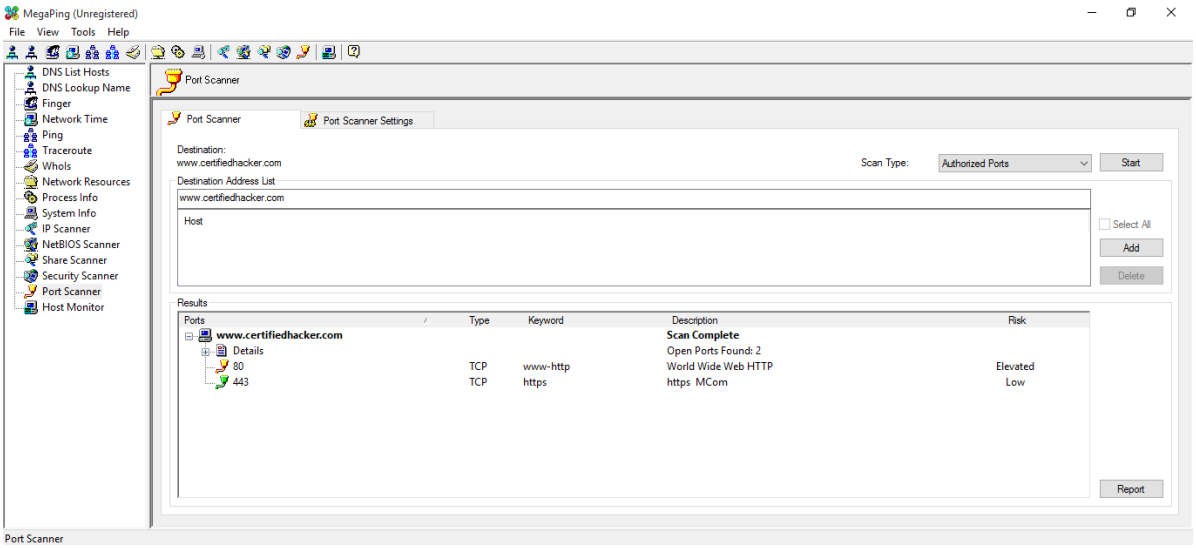
1. IP Scanner



2. Traceroute



3. Port Scanner



Tool/Utility	**Information Collected/Objective Achieved**
MegaPing	**IP Scan Range:** 10.11.136.1 – 10.11.136.254
	Performed Actions: IP Scanning NetBIOS Scanning Traceroute Port Scanning