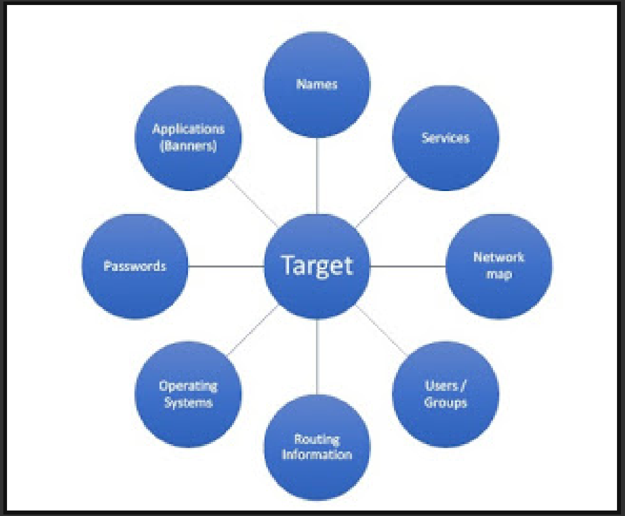
TECHNOLOGY REDEFINE

Showing posts with label **Enumeration**. Show all posts

Tuesday, November 7, 2017

ENUMERATION



SEARCH

Search

STATISTICS

33957

DON'T MISS OUR UPDATE

Email address... Submit

FOLLOW BY EMAIL

Email address... Submit

Enumeration Is More Likely A Internal Process Than External. In This Process The Attacker Establishes An Active Connection With The Victim And Tries To Discover As Much Attack Vectors As Possible, Which Can Be Used To Exploit The Systems Further.

Many Of The Protocols Do Not Encrypt Data While Traveling Across The Network So We Can Sniff In A Network In Order To Gather More Data.

Enumeration Is Used To Gather Following Data :

- Running Services
- Service Version
- Hostnames
- IP Adresses
- Operating System
- Network Resources
- SNMP Data
- IP Tables
- Passwords Policies
- Users and Groups
- Networks and shared paths
- Route Tables
- Applications and Banners
- Points Of Entry

Enumeration Depends On The Services That The Systems Offer, Following Services Is Used To Enumerate System.

LABEL

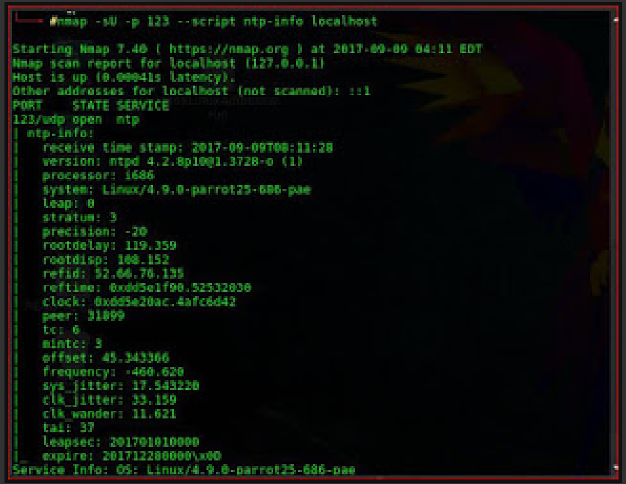
- Cracking Hashes
- CVE-2018-0802
- DNS Enumeration & Interrogation
- Dump Hashes
- Dumpster-Diving
- Enumeration
- Evasion Techniques
- Finding Open Ports
- Firewall Evasion Countermeasures
- Footprinting Tools and Techniques
- Information Gathering
- Installing And Removing Application
- Installing VirtualBox Guest Addition
- Introduction To Linux
- Least privilege
- Linux Basic Commands
- MAC Spoofing

NTP Enumeration

Network Time Protocol Is A Protocol Designed To Synchronize Clocks Of Networked Computers. Now Obviously These Computers Talking To Each Other To Synchronize Their Time, Which Opens Them Up For Enumeration. NTP Uses UDP Port 123.

Hosts & IP Adresses
Sys Name & OS

```
nmap -sU -p 123 --script=ntp-info <target>
```



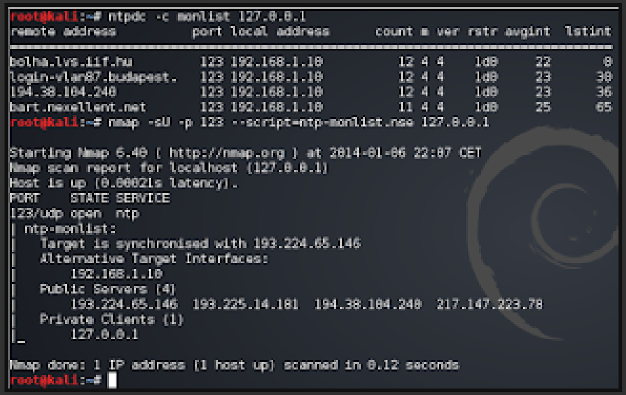
```
└──╼ #nmap -sU -p 123 --script ntp-info localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-09 04:11 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000041s latency).
Other addresses for localhost (not scanned): ::1
PORT    STATE SERVICE
123/udp open  ntp
| ntp-info:
|   receive time stamp: 2017-09-09T08:11:28
|   version: ntpd 4.2.8p10@1.3728-o (1)
|   processor: i686
|   system: Linux/4.9.0-parrot25-686-pae
|   leap: 0
|   stratum: 3
|   precision: -20
|   rootdelay: 119.359
|   rootdisp: 108.152
|   refid: 52.66.76.135
|   reftime: 0xdd5e1f90.52532030
|   clock: 0xdd5e20ac.4afc6d42
|   peer: 31099
|   tc: 6
|   mintc: 3
|   offset: 45.343366
|   frequency: -460.620
|   sys_jitter: 17.543220
|   clk_jitter: 33.159
|   clk_wander: 11.621
|   tai: 37
|   leapsec: 201701010000
|_  expire: 201712280000\x00
Service Info: OS: Linux/4.9.0-parrot25-686-pae
```

Monlist Is A Remote Command In Older Version Of NTP That Sends The Requester A List Of The Last 600 Hosts Who Have Connected To That Server. For Attackers The Monlist Query Is A Great Reconnaissance Tool. For A Localized NTP Server It Can Help To

- Network Access Control
- Nmap Cheatsheet
- Nmap Scanning
- NTLM Hashes
- Password Hacking
- Password Hacking Countermeasures
- Password Sniffing
- payload generator
- post exploitation
- Reconnaissance
- Remote Access
- Reverse Proxy Server
- Risk Assessment
- Router Attacks
- Scanning
- Scanning Types
- Social Engineering
- Surveillance
- Virtual Ports
- Zone Transfer

Build A Network Profile.

```
nmap -sU -p 123 -Pn -n --script=ntp-monlist <target>
```



```
root@kali:~# ntpdc -c monlist 127.0.0.1
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
bolha.lvs.iif.hu         123 192.168.1.10          12 4 4    1d0     22       0
login-vlan87.budapest.   123 192.168.1.10          12 4 4    1d0     23      30
194.38.104.240           123 192.168.1.10          12 4 4    1d0     23      36
bart.nexellent.net       123 192.168.1.10          11 4 4    1d0     25      65
root@kali:~# nmap -sU -p 123 --script=ntp-monlist.nse 127.0.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2014-01-06 22:07 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00021s latency).
PORT    STATE SERVICE
123/udp open  ntp
| ntp-monlist:
|   Target is synchronised with 193.224.65.146
|   Alternative Target Interfaces:
|       192.168.1.10
|   Public Servers (4)
|       193.224.65.146  193.225.14.181  194.38.104.240  217.147.223.78
|   Private Clients (1)
|_      127.0.0.1

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

SNMP Enumeration

The Simple Network Management Protocol Is Used To Manage And Monitor Hardware Devices Connected To A Network. If Passwords Are Not Changed They Can Be Used By An Attacker To Enumerate SNMP As SNMP Manager.

User Accounts And Devices

```
nmap -sU -p 137 --script snmp-brute <target>
```

SMB Enumeration

The Server Message Block Protocol Is a Network File Sharing Protocol That Allows Applications on a Computer to Read and

Write to Files and to Request Services From Server Programs in a Computer Network. The SMB Protocol Can Be Used on Top of Its TCP/IP Protocol or Other Network Protocols. Using the SMB Protocol, User Can Access Files or Other Resources at a Remote Server. This Allows Applications to Read, Create, and Update Files on the Remote Server. It Can Also Communicate With Any Server Program That Is Set Up to Receive an SMB Client Request.

```
nmap -p 445 --script smb-os-discovery 192.168.1.0/24
nmap -sV -p 445 --script smb-brute 192.168.1.101
```

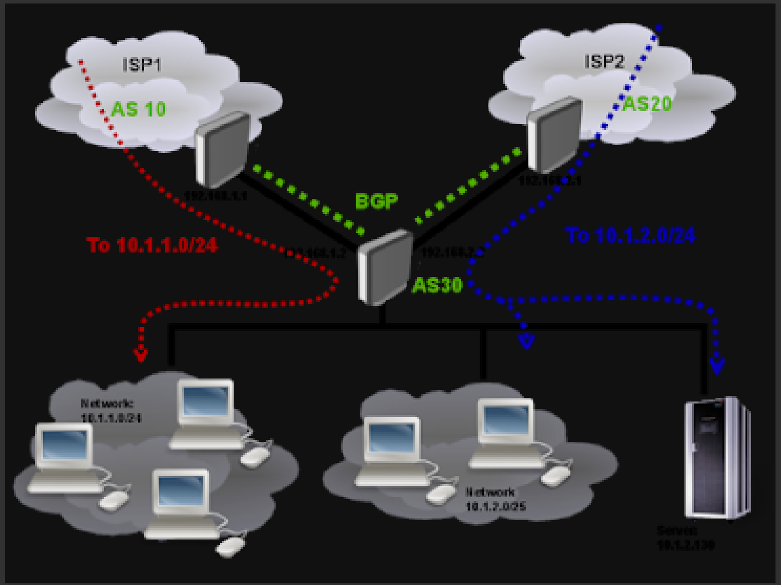
Active Directory Enumeration

Enumerating Windows Active Directory Via LDAP (Lightweight Directory Access Protocol), TCP/UDP 389 And 3268. Active Directory Contains User Accounts And Additional Information About Accounts On Windows PC's.

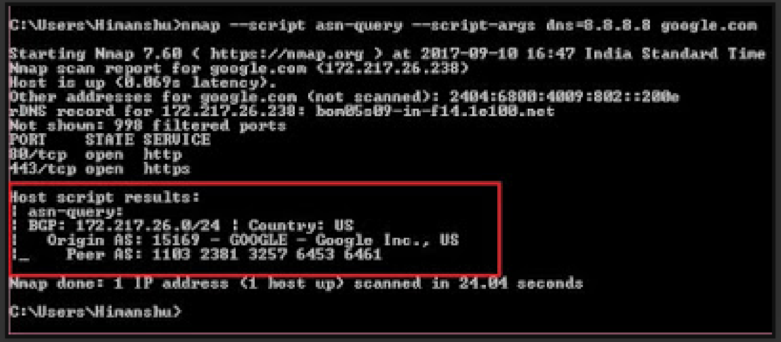
ad-ldap-enum

BGP Enumeration

BGP Is designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP Is Used By Routers To Help Them Guide Packets To Their Destinations. It makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions. It Can Be Used To Find All The Networks Associated With A Particular Corporation.



```
nmap --script asn-query --script-args dns=8.8.8.8 <target>
```



```
C:\Users\Himanshu>nmap --script asn-query --script-args dns=8.8.8.8 google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-10 16:47 India Standard Time
Nmap scan report for google.com (172.217.26.238)
Host is up (0.069s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:802::200e
rDNS record for 172.217.26.238: bom05s09-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Host script results:
| asn-query:
| BGP: 172.217.26.0/24 | Country: US
|   Origin AS: 15169 - GOOGLE - Google Inc., US
|_    Peer AS: 1103 2381 3257 6453 6461

Nmap done: 1 IP address (1 host up) scanned in 24.04 seconds

C:\Users\Himanshu>
```

BGPSimple

autonomous system scanner

SMTP Enumeration

SMTP Is A Protocol Which Is Used To Deliver Emails Across The Internet, SMTP Protocol Moves Your Email Using DNS MX Records To Identify Server That It Needs To Forward Or Store An Email, It Also Works Very Closely With MTA (Mail Transfer Agents) To Make Sure It Sends An Email To Right Computer As Well As Right Email Inbox.

Once The Email Gets Inside Of Our Network It Typically Uses Protocol (POP, IMAP) To Deliver The Email Internally, But Externally On The Internet It Uses SMTP.
By Simply Sending An Email Message To A Non-Existent Address At A Target Domain Often Reveals Useful Internal Network Information Through A Non-Delivery Notification (NDN).

Default Ports:

SMTP Server (Outgoing Messages)
Non-Encrypted - AUTH - Port: 25 (or 587)
Secure (TLS) - StartTLS - Port: 587
Secure (SSL) - SSL - Port: 465

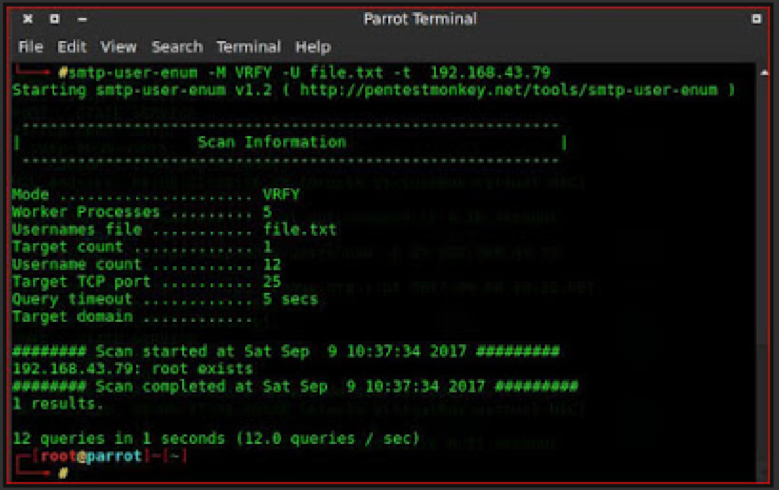
POP3 Server (Incoming Messages)
Non-Encrypted - AUTH - Port: 110

Secure (SSL) - SSL - Port: 995

VRFY Verify, If A User Exists

EXPN Expand, Show All Recipients Of An address

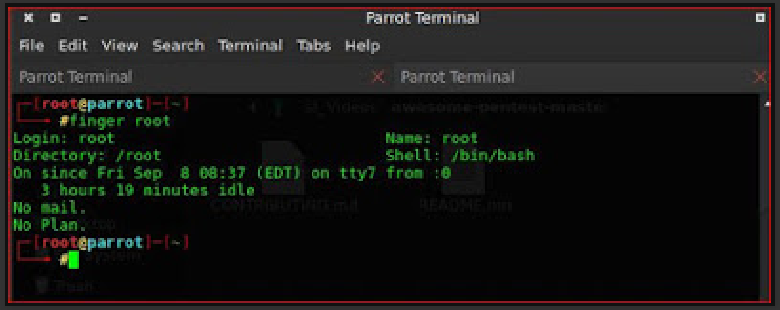
RCPT TO Sets The Destination Address Of The Email



```
└──╼ #smtp-user-enum -M VRFY -U file.txt -t  192.168.43.79
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... file.txt
Target count ............. 1
Username count ........... 12
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sat Sep  9 10:37:34 2017 #########
192.168.43.79: root exists
######## Scan completed at Sat Sep  9 10:37:34 2017 #########
1 results.

12 queries in 1 seconds (12.0 queries / sec)
┌─[root@parrot]─[~]
└──╼ #
```

FINGER Enumeration

Finger Is A Utility In Linux Operating System, By Using It You Can Check The Information Of Any User From Remote Or Local Command Line Interface.



```
┌─[root@parrot]─[~]
└──╼ #finger root
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
On since Fri Sep  8 08:37 (EDT) on tty7 from :0
   3 hours 19 minutes idle
No mail.
No Plan.
┌─[root@parrot]─[~]
└──╼ #
```

TFTP Enumeration

Trivial File Transport Protocol Uses Udp Which Is Not Secure. It Pros And Sys Admins Typically Use TFTP For Transfer Files Remotely , Remotetly Boot System And Backup Conf, Files. By Sniffing On A TFTP Traffic We Can All Of This.

RPC Enumeration

Remote Procedure Call (RPC) Is A Protocol That One Program Can Use To Request A Service From A Program Located In Another Computer On A Network Without Having To Understand The Network's Details. By Querying An MSRPC Endpoint We Can Get List Of Services That Is Running On The Target System.

RPCScan2

NetBIOS Enumeration

NetBIOS (Network Basic Input/Output System) Is A Program That

Allows Applications On Different Computers To Communicate Within A Local Area Network (LAN). NetBIOS Software Runs On Port 139 On Windows Operating System. File And Printer Service Needs To Be Enabled To Enumerate NetBIOS.

SSH Enumeration

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

osueta
ssh_user_enum

```
nmap --script ssh2-enum-algos target
```

OS Fingerprinting

The Process Of Determining The Operating System Used By A Host On A Network. By Analysing Packets From A Host On A Network By Following :

IP TTL values
IP ID values
TCP Window size
TCP Options SYN and SYN+ACK
DHCP Requests
ICMP Requests

HTTP Packets (User-Agent field).
Running Services
Open Port Patterns.

Banner Grabbing

Banner Grabbing Provides Important Information About What Type And Version Of Software Is Running. Telnet Is An Easy Way To Do This Banner Grabbong For FTP, SMTP, HTTP, And Others.

```
Telnet <Target>
```

Some Extra Enumration Scripts :

```
HOSTMAP : nmap -p 80 --script hostmap-bfk.nse scanme.nmap.org

TRACEROUTE : nmap --traceroute --script traceroute-
                 geolocation.nse -p 80  scanme.nmap.org



FTP : nmap --script ftp-brute -p 21
      ftp <ftp server ip/ftp.server.com>

SSH  : nmap --script ssh2-enum-algos <target>

HTTP : nmap -sV --script=http-userdir-enum <target>
       nmap --script http-enum 192.168.1.52
       nmap --script -http-enum --script-args http-
           enum.basepath='pub/' 192.168.1.52
       nmap --script http-title -sV -p 80 192.168.1.0/24

TELNET : nmap -p 23 <ip> --script telnet-encryption

TFTP : nmap -sU -p 69 --script tftp-enum.nse --script-args
       tftp-enum.filelist=customlist.txt <host>

RPN : nmap --script=msrpc-enum <target>
```

Enumeration Countermeasures

- Disable Directory Indexing That Don’T Contain Index.Html Or (Default.Asp).
- Use Robots.txt To Prevent Indexing On Search Engine.
- Use A Centralized Network Admin Contact Detail In WHOIS Databases To Prevent Social Engineering Attacks.
- Disallow DNS Zone Transfers To Untrusted Hosts
- Remove Nonpublic IP Address And Hostname Details In DNS Zone Files
- PTR Records Should Only Be Used If Absolutely Needed (For SMTP Mail Servers And Other CriticaL Systems That Need To Resolve Both Ways).
- Ensure That Unnecessary Records (E.G. HINFO) Don’T Appear In DNS Zone Files.

- Configure SMTP Servers To Not Send Non-Delivery Notifications To Prevent Attackers From Enumerating The Internal Mail Servers And Configuration.
- Consider And Review Your IPV6 Networks And DNS Configuration (If Any).

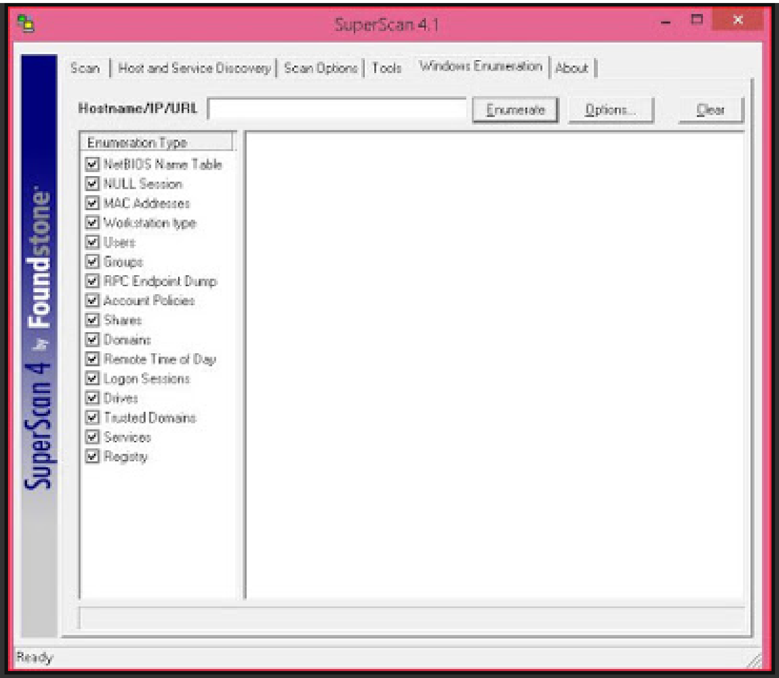
Tools :

Linux :

- NEET - Network Enumeration and Exploitation Tool
- Reconnoitre (DNS, SNMP)
- Bluto-Old (use it first)
- subdomains enumeration tool
- web-sorrow
- HTTPrint (Banner Gabing Server Fingerprinting)
- IKE scan (VPN Fingerprinting)

Windows :

SuperScan

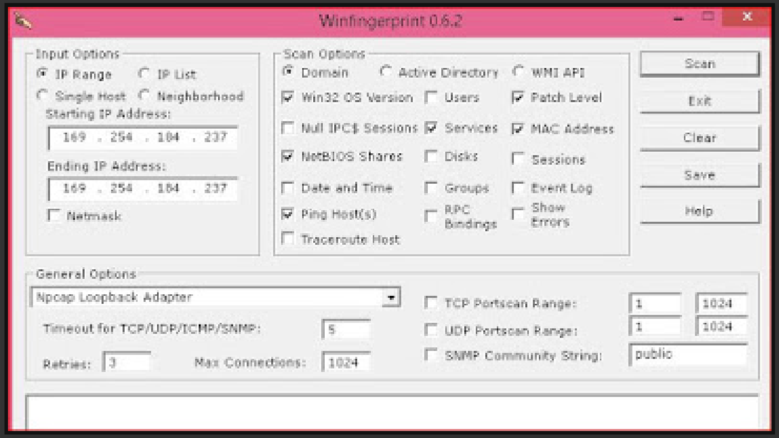

SuperScan 4.1
Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About
Enumerate
Options...
Clear
SuperScan 4 by Foundstone
Ready

Hostname/IP/URL

Enumeration Type

- ☑ NetBIOS Name Table
- ☑ NULL Session
- ☑ MAC Addresses
- ☑ Workstation type
- ☑ Users
- ☑ Groups
- ☑ RPC Endpoint Dump
- ☑ Account Policies
- ☑ Shares
- ☑ Domains
- ☑ Remote Time of Day
- ☑ Logon Sessions
- ☑ Drives
- ☑ Trusted Domains
- ☑ Services
- ☑ Registry

WinFingerprint



Input Options

● IP Range ○ IP List
○ Single Host ○ Neighborhood

Starting IP Address: 169 . 254 . 184 . 237

Ending IP Address: 169 . 254 . 184 . 237

□ Netmask

Scan Options

● Domain ○ Active Directory ○ WMI API

☑ Win32 OS Version □ Users ☑ Patch Level
□ Null IPC$ Sessions ☑ Services ☑ MAC Address
☑ NetBIOS Shares □ Disks □ Sessions
□ Date and Time □ Groups □ Event Log
☑ Ping Host(s) □ RPC Bindings □ Show Errors
□ Traceroute Host

General Options

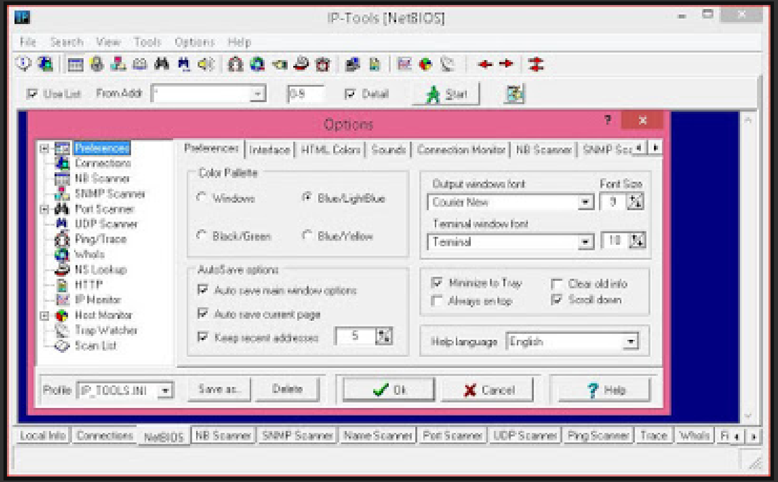
Npcap Loopback Adapter

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3 Max Connections: 1024

□ TCP Portscan Range: 1 1024
□ UDP Portscan Range: 1 1024
□ SNMP Community String: public

IP-Tools


IP-Tools [NetBIOS]
File Search View Tools Options Help
Options
Preferences
Connections
NB Scanner
SNMP Scanner
Port Scanner
UDP Scanner
Ping/Trace
WhoIs
NS Lookup
HTTP
IP Monitor
Host Monitor
Trap Watcher
Scan List
Preferences | Interface | HTML Colors | Sounds | Connection Monitor | NB Scanner | SNMP Sca
Save as..
Delete
Ok
Cancel
Help
Local Info | Connections | NetBIOS | NB Scanner | SNMP Scanner | Name Scanner | Port Scanner | UDP Scanner | Ping Scanner | Trace | WhoIs | Fi

☑ Use List   From Addr   0-9   ☑ Detail   Start

Color Pallette
○ Windows   ● Blue/LightBlue
○ Black/Green   ○ Blue/Yellow

Output windows font: Courier New   Font Size: 9
Terminal window font: Terminal   10

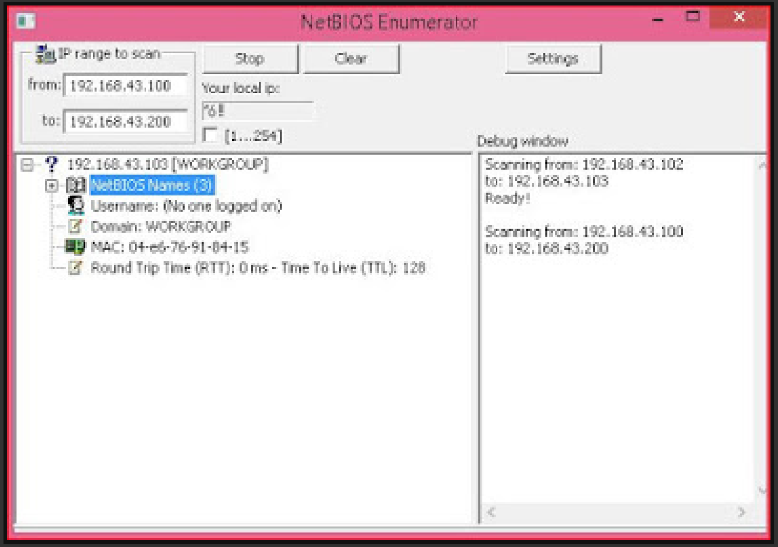
AutoSave options
☑ Auto save main window options
☑ Auto save current page
☑ Keep recent addresses 5

☑ Minimize to Tray   □ Clear old info
□ Always on top   ☑ Scroll down

Help language: English

Profile: IP_TOOLS.INI

NetBIOS Enumerator



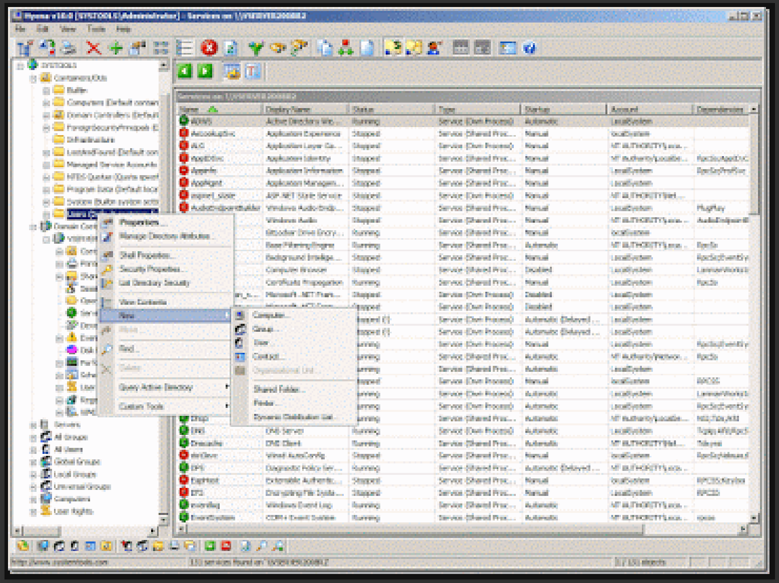
IP range to scan
from: 192.168.43.100
to: 192.168.43.200

Your local ip: ?6!!
□ [1...254]

```
⊟ 192.168.43.103 [WORKGROUP]
  ⊞ NetBIOS Names (3)
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 04-e6-76-91-84-15
    Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
```

```
Scanning from: 192.168.43.102
to: 192.168.43.103
Ready!

Scanning from: 192.168.43.100
to: 192.168.43.200
```

Hyena



Sid2Username (User2SID, SID2User)

JXplorer (Open source LDAP Browser)

MIB Browser (SNMP Managment Information Base)

By Himanshu - November 07, 2017

Ph?n ?ng: □ funny (0) □ interesting (0) □ cool (0)

2 comments

Labels: Enumeration

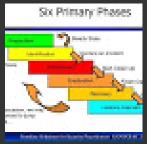
Home Older Posts

Subscribe to: Posts (Atom)

Popular Posts

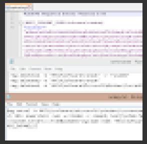
IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System • It Uses a network tap, span port, or hub to collect packets on the network • Attempts t...



INCIDENT RESPONSE PLAN

An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information...



INSTALLING PRESISTENCE BACKDOOR IN WINDOWS

USING METASPLOIT windows/local/s4u_persistence windows/local/vss_persistence windows/local/registry_persistence windows/manage...

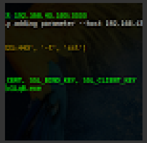
NMAP CHEAT SHEET

Target Specification 192. 168. 100. 1-50 IP Range 192. 168. 100. 1/24 CIDR Spec. -iL Filename IP Addr File -iR...

```
upy/pupy/ext
oit-suggeste
loit version
2018-01-08-m
```

WINDOWS-EXPLOIT-SUGGESTER

./windows-exploit-suggester.py --update This will download latest ms bulletin xls file pip install xlrd --upgrade to download xl...



PUPY (RAT, POST EXPLOITATION TOOL)

Installing pupy git clone https://github.com/n1nj4sec/pupy.git pupy cd pupy git submodule init git submodule update pip install -r pu...

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802   Cr...

Comment