Nmap Scripting Engine – Basic Usage

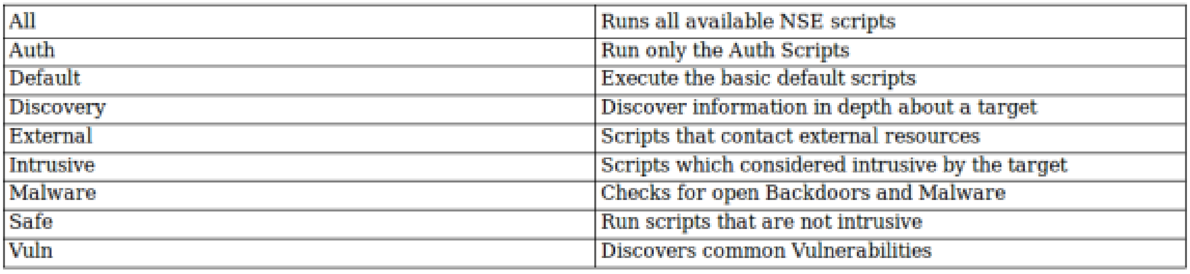
pentestlab.blog/category/information-gathering/page/11

March 8, 2012

Nmap is not only a port scanner that could be used for scanning ports on a machine but also contains a script engine that offers the ability to execute scripts that could be used for more in-depth discovery of a target.

Nmap includes a variety of ready-made scripts that could be used for that reason.You can run scripts one at a time or you can execute scripts by category.Of course Nmap offers the option to execute multiple scripts at a time.

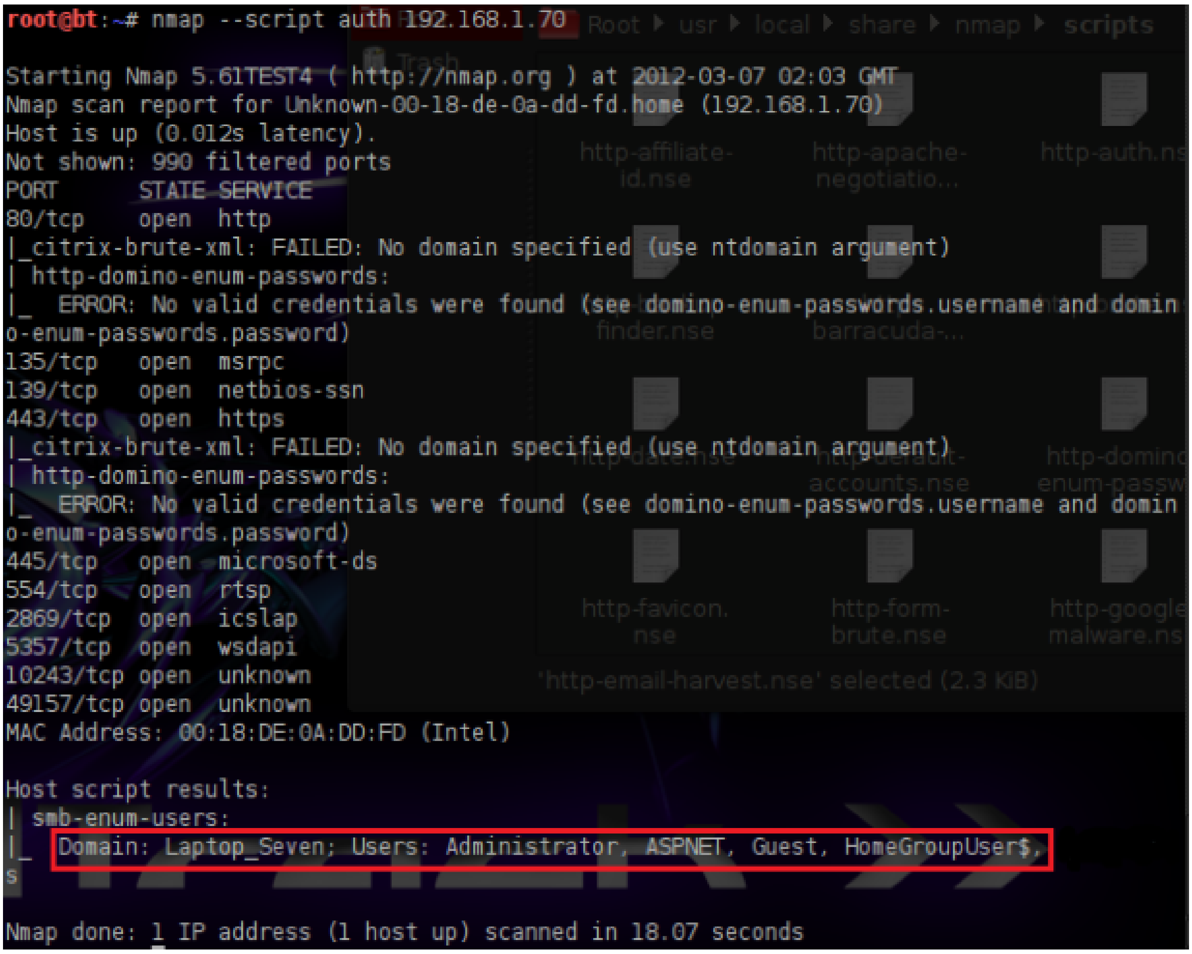
Currently the Nmap has the following Script Categories:



All	Runs all available NSE scripts
Auth	Run only the Auth Scripts
Default	Execute the basic default scripts
Discovery	Discover information in depth about a target
External	Scripts that contact external resources
Intrusive	Scripts which considered intrusive by the target
Malware	Checks for open Backdoors and Malware
Safe	Run scripts that are not intrusive
Vuln	Discovers common Vulnerabilities

Execute Scripts Related to Authentication

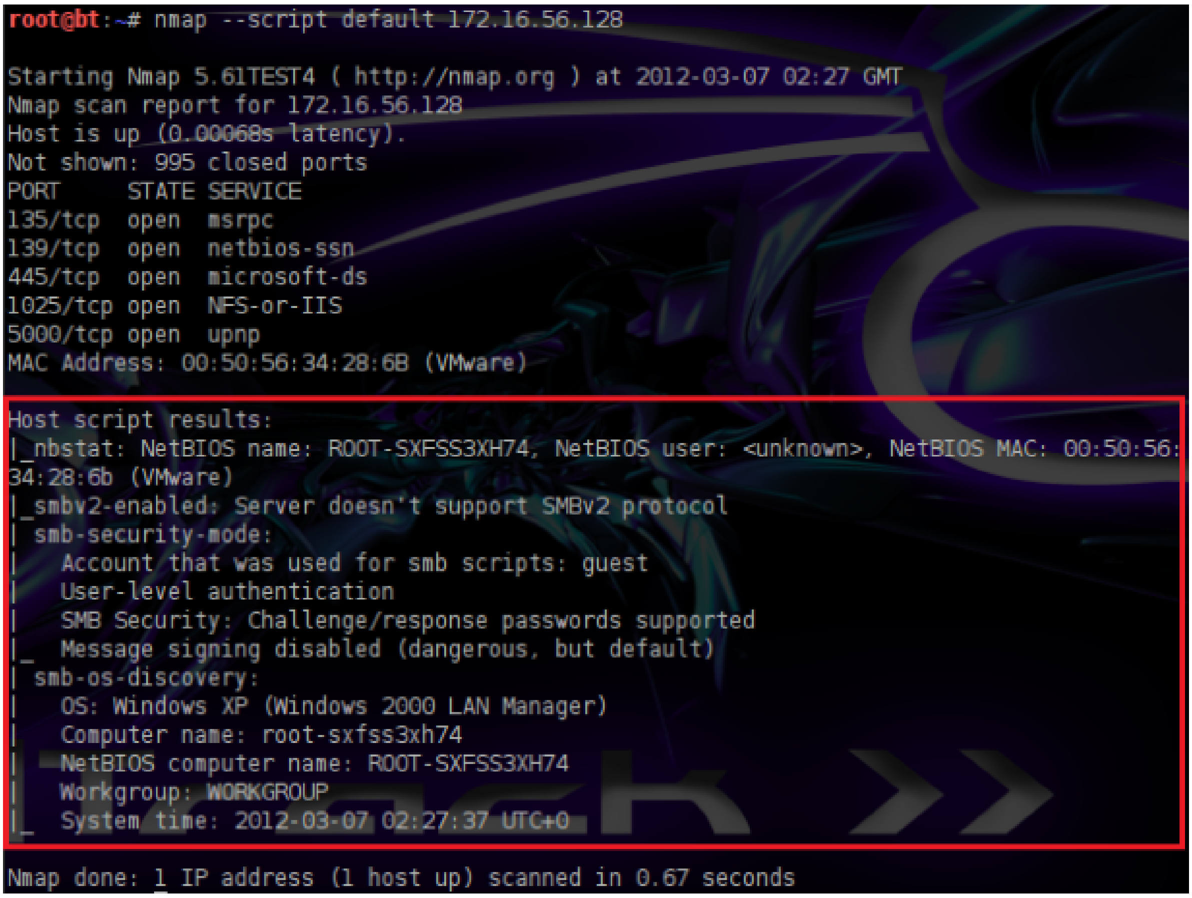
As you can see from the image below we have selected to execute the Auth scripts against a target in our network.From the results we can see that Nmap has successfully discover the users accounts on the remote machine and the Domain name.



```
root@bt:~# nmap --script auth 192.168.1.70

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-07 02:03 GMT
Nmap scan report for Unknown-00-18-de-0a-dd-fd.home (192.168.1.70)
Host is up (0.012s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-domino-enum-passwords:
|_  ERROR: No valid credentials were found (see domino-enum-passwords.username and domin
o-enum-passwords.password)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
| http-domino-enum-passwords:
|_  ERROR: No valid credentials were found (see domino-enum-passwords.username and domin
o-enum-passwords.password)
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:18:DE:0A:DD:FD (Intel)

Host script results:
| smb-enum-users:
|_  Domain: Laptop_Seven; Users: Administrator, ASPNET, Guest, HomeGroupUser$,
s

Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```

Run Default Scripts

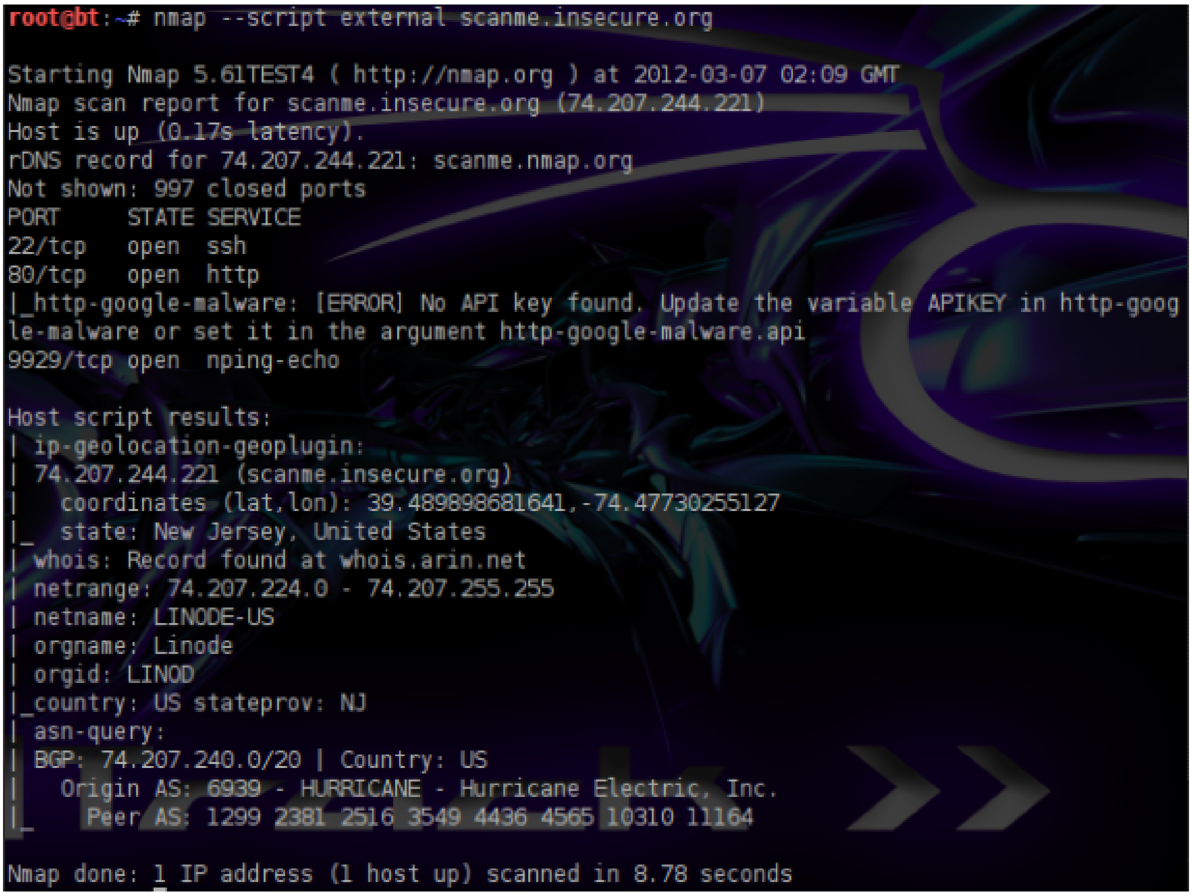
The default scripts category will expose information about the operating system,the workgroup name, the netbios names etc.You can see the image below for more details:



```
root@bt:~# nmap --script default 172.16.56.128

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-07 02:27 GMT
Nmap scan report for 172.16.56.128
Host is up (0.00068s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:50:56:34:28:6B (VMware)

Host script results:
|_nbstat: NetBIOS name: ROOT-SXFSS3XH74, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:
34:28:6b (VMware)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Computer name: root-sxfss3xh74
|   NetBIOS computer name: ROOT-SXFSS3XH74
|   Workgroup: WORKGROUP
|_  System time: 2012-03-07 02:27:37 UTC+0

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Running Scripts that contacting external sources

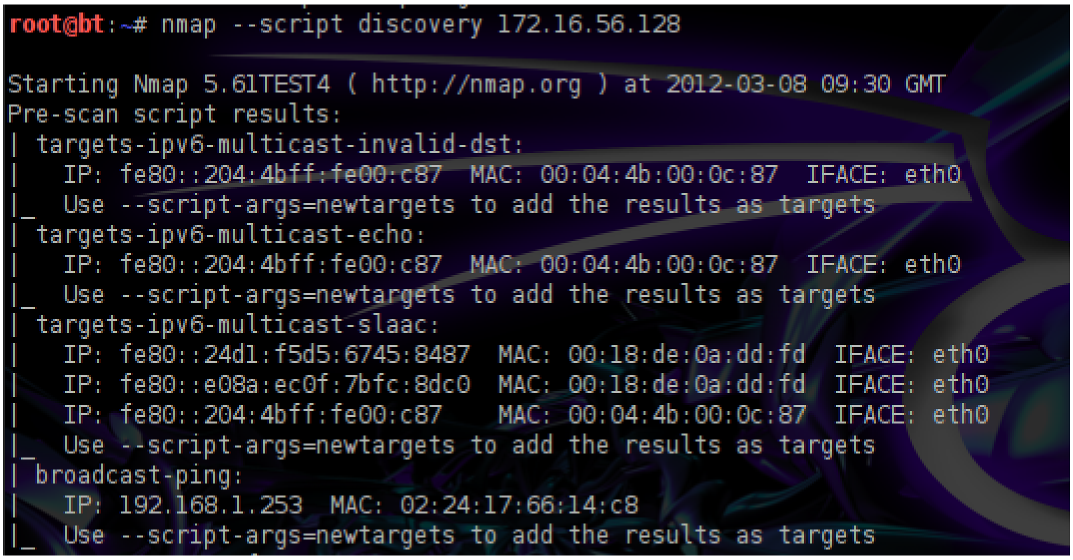
There is a category of scripts called external that performs an automatic Web Whois to the target and discovers additional information like the geographical location,the name of the organization and the net range.



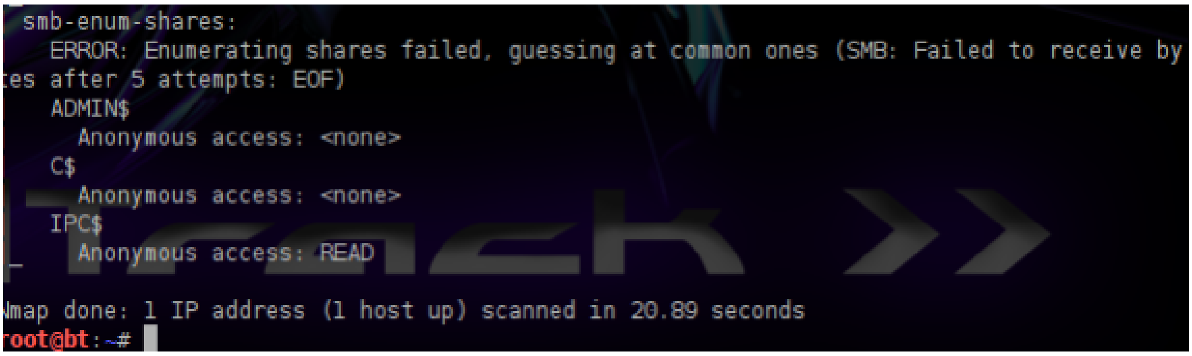
```
root@bt:~# nmap --script external scanme.insecure.org

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-07 02:09 GMT
Nmap scan report for scanme.insecure.org (74.207.244.221)
Host is up (0.17s latency).
rDNS record for 74.207.244.221: scanme.nmap.org
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-google-malware: [ERROR] No API key found. Update the variable APIKEY in http-goog
le-malware or set it in the argument http-google-malware.api
9929/tcp open  nping-echo

Host script results:
| ip-geolocation-geoplugin:
| 74.207.244.221 (scanme.insecure.org)
|   coordinates (lat,lon): 39.489898681641,-74.47730255127
|_  state: New Jersey, United States
| whois: Record found at whois.arin.net
| netrange: 74.207.224.0 - 74.207.255.255
| netname: LINODE-US
| orgname: Linode
| orgid: LINOD
|_country: US stateprov: NJ
| asn-query:
| BGP: 74.207.240.0/20 | Country: US
|   Origin AS: 6939 - HURRICANE - Hurricane Electric, Inc.
|_    Peer AS: 1299 2381 2516 3549 4436 4565 10310 11164

Nmap done: 1 IP address (1 host up) scanned in 8.78 seconds
```

Executing the Discovery Scripts

This category of scripts is ideal when we need to have as much information as possible for a specific target.The next two images are a sample of what kind of information could be delivered to us when we run the Discovery Scripts.



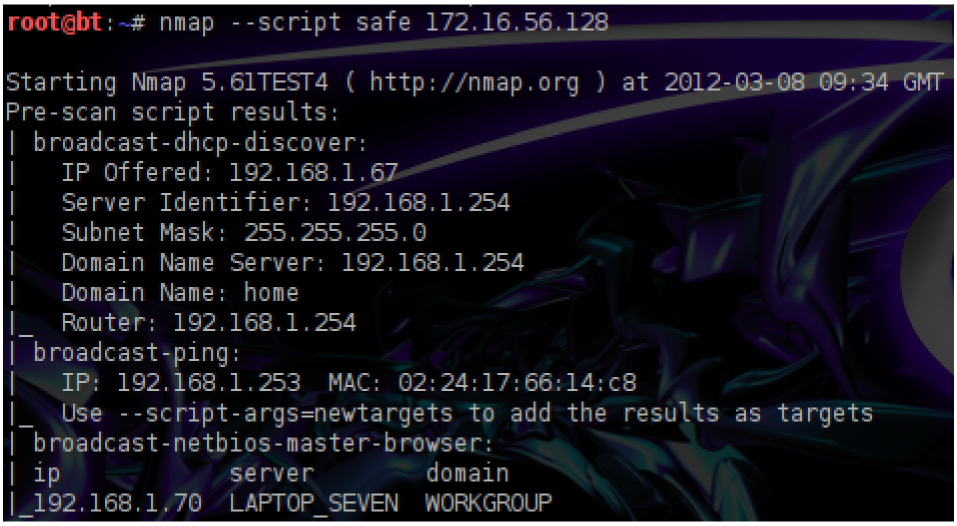
```
root@bt:~# nmap --script discovery 172.16.56.128

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-08 09:30 GMT
Pre-scan script results:
| targets-ipv6-multicast-invalid-dst:
|   IP: fe80::204:4bff:fe00:c87  MAC: 00:04:4b:00:0c:87  IFACE: eth0
|_  Use --script-args=newtargets to add the results as targets
| targets-ipv6-multicast-echo:
|   IP: fe80::204:4bff:fe00:c87  MAC: 00:04:4b:00:0c:87  IFACE: eth0
|_  Use --script-args=newtargets to add the results as targets
| targets-ipv6-multicast-slaac:
|   IP: fe80::24d1:f5d5:6745:8487  MAC: 00:18:de:0a:dd:fd  IFACE: eth0
|   IP: fe80::e08a:ec0f:7bfc:8dc0  MAC: 00:18:de:0a:dd:fd  IFACE: eth0
|   IP: fe80::204:4bff:fe00:c87    MAC: 00:04:4b:00:0c:87  IFACE: eth0
|_  Use --script-args=newtargets to add the results as targets
| broadcast-ping:
|   IP: 192.168.1.253  MAC: 02:24:17:66:14:c8
|_  Use --script-args=newtargets to add the results as targets
```



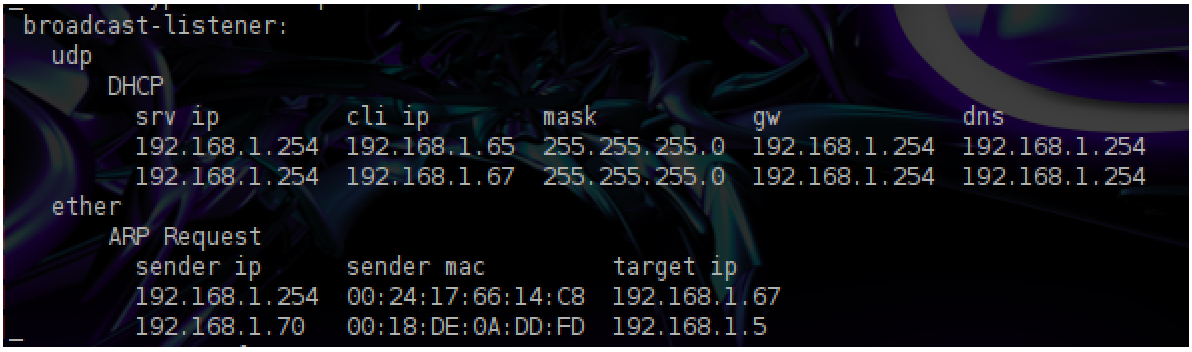
```
 smb-enum-shares:
   ERROR: Enumerating shares failed, guessing at common ones (SMB: Failed to receive by
tes after 5 attempts: EOF)
   ADMIN$
     Anonymous access: <none>
   C$
     Anonymous access: <none>
   IPC$
_    Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 20.89 seconds
root@bt:~# 
```

Scanning with Safe Scripts

This category could be used when we want to run scripts that are less intrusive to the target so it will be less likely to cause any disruption to the remote system.As we can see in the next two images the scripts have discovered the router IP address,the domain name of the network and the master browser.



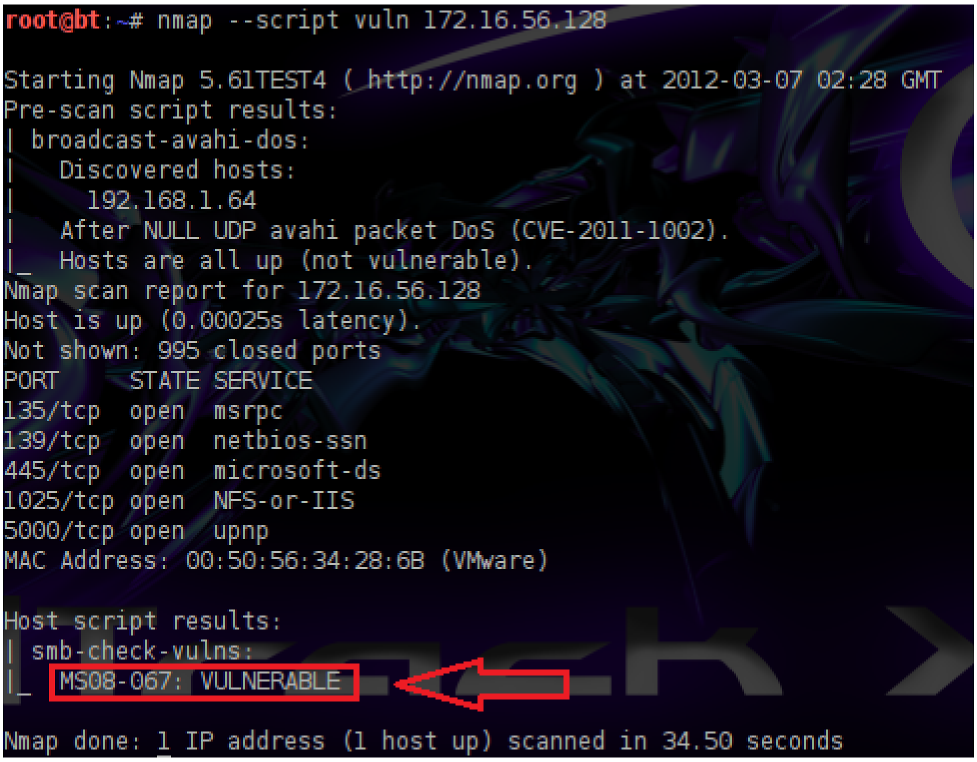
```
root@bt:~# nmap --script safe 172.16.56.128

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-08 09:34 GMT
Pre-scan script results:
| broadcast-dhcp-discover:
|   IP Offered: 192.168.1.67
|   Server Identifier: 192.168.1.254
|   Subnet Mask: 255.255.255.0
|   Domain Name Server: 192.168.1.254
|   Domain Name: home
|_  Router: 192.168.1.254
| broadcast-ping:
|   IP: 192.168.1.253  MAC: 02:24:17:66:14:c8
|_  Use --script-args=newtargets to add the results as targets
| broadcast-netbios-master-browser:
| ip            server       domain
|_192.168.1.70  LAPTOP_SEVEN  WORKGROUP
```



```
 broadcast-listener:
   udp
       DHCP
         srv ip        cli ip        mask           gw             dns
         192.168.1.254  192.168.1.65  255.255.255.0  192.168.1.254  192.168.1.254
         192.168.1.254  192.168.1.67  255.255.255.0  192.168.1.254  192.168.1.254
   ether
       ARP Request
         sender ip      sender mac         target ip
         192.168.1.254  00:24:17:66:14:C8  192.168.1.67
_        192.168.1.70   00:18:DE:0A:DD:FD  192.168.1.5
```

Check targets for common vulnerabilities

Another category of scripts is the vuln.These kind of scripts will check your target host for common vulnerabilities.In the example below the target is running Windows XP.

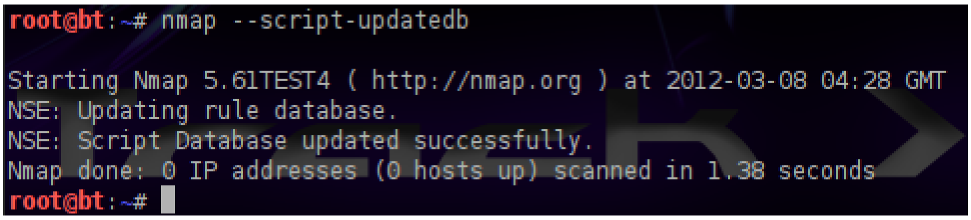


```
root@bt:~# nmap --script vuln 172.16.56.128

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-07 02:28 GMT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     192.168.1.64
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 172.16.56.128
Host is up (0.00025s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:50:56:34:28:6B (VMware)

Host script results:
| smb-check-vulns:
|_  MS08-067: VULNERABLE

Nmap done: 1 IP address (1 host up) scanned in 34.50 seconds
```

As we can see the Nmap scripts have successfully discovered the vulnerability that affects Windows XP operating systems.With those kind of scripts we can have an early indication of vulnerable targets and what exploits we should use as a start.

Update the Script Database

You can use the command ***nmap –script-updatedb*** in order to update the scripts database.



```
root@bt:~# nmap --script-updatedb

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-08 04:28 GMT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.38 seconds
root@bt:~#
```

Have in mind that you can browse the database scripts in order to find the ones you need.The default storage location of the scripts in Windows is at:

C:\Program Files\Nmap\scripts

and in Unix Versions

/usr/share/nmap/scripts or

/usr/local/share/nmap/scripts

Conclusion

The drawback of executing scripts by category is that the scan will take longer because the Nmap Scripting Engine will run all the scripts in the category.From the other hand this is the easiest way and you will not tangle with hundreds of scripts.

However the best option is to know what kind of information you want to retrieve in order to select the appropriate scripts from each category.Also it is always good to know how to produce your own scripts that will cover exactly your needs.