专注APT攻击与防御

https://micropoor.blogspot.com/

netbios简介：

IBM公司开发，主要用于数十台计算机的小型局域网。该协议是一种在局域网上的程序可以使用的应用程序编程接口（API），为程序提供了请求低级服务的同一的命令集，作用是为了给局域网提供网络以及其他特殊功能。

系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名-——特指基于NETBIOS协议获得计算机名称——解析为相应IP地址，实现信息通讯，所以在局域网内部使用NetBIOS协议可以方便地实现消息通信及资源的共享。

nmap扫描：

root@John:~# nmap -sU --script nbstat.nse -p137 192.168.1.0/24 -T4

```
root@John:~# nmap -sU --script nbstat.nse -p137 192.168.1.0/24 -T4

Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-03 22:32 EST
Nmap scan report for 192.168.1.1
Host is up (0.017s latency).
PORT    STATE  SERVICE
137/udp closed netbios-ns
MAC Address: [redacted]

Nmap scan report for 192.168.1.100
Host is up (0.032s latency).
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: [redacted]

Host script results:
|_nbstat: NetBIOS name: JOHN-PC, NetBIOS user: <unknown>, NetBIOS MAC: [redacted]

Nmap scan report for 192.168.1.107
Host is up (0.000079s latency).
PORT    STATE  SERVICE
137/udp closed netbios-ns

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.89 seconds
```

msf扫描：

msf > use auxiliary/scanner/netbios/nbname

```
msf > use auxiliary/scanner/netbios/nbname
msf auxiliary(nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      137              yes       The target port (UDP)
   THREADS    10               yes       The number of concurrent threads

msf auxiliary(nbname) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(nbname) > run

[*] Sending NetBIOS requests to 192.168.1.0->192.168.1.255 (256 hosts)
[+] 192.168.1.100 [JOHN-PC] OS:Windows Names:(JOHN-PC, WORKGROUP) Addresses:(192.168.136.1, 192.168.1.1, 192.168.1.100, 10.11.3.18)
6:48
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

nbtscan扫描：

项目地址：http://www.unixwiz.net/tools/nbtscan.html

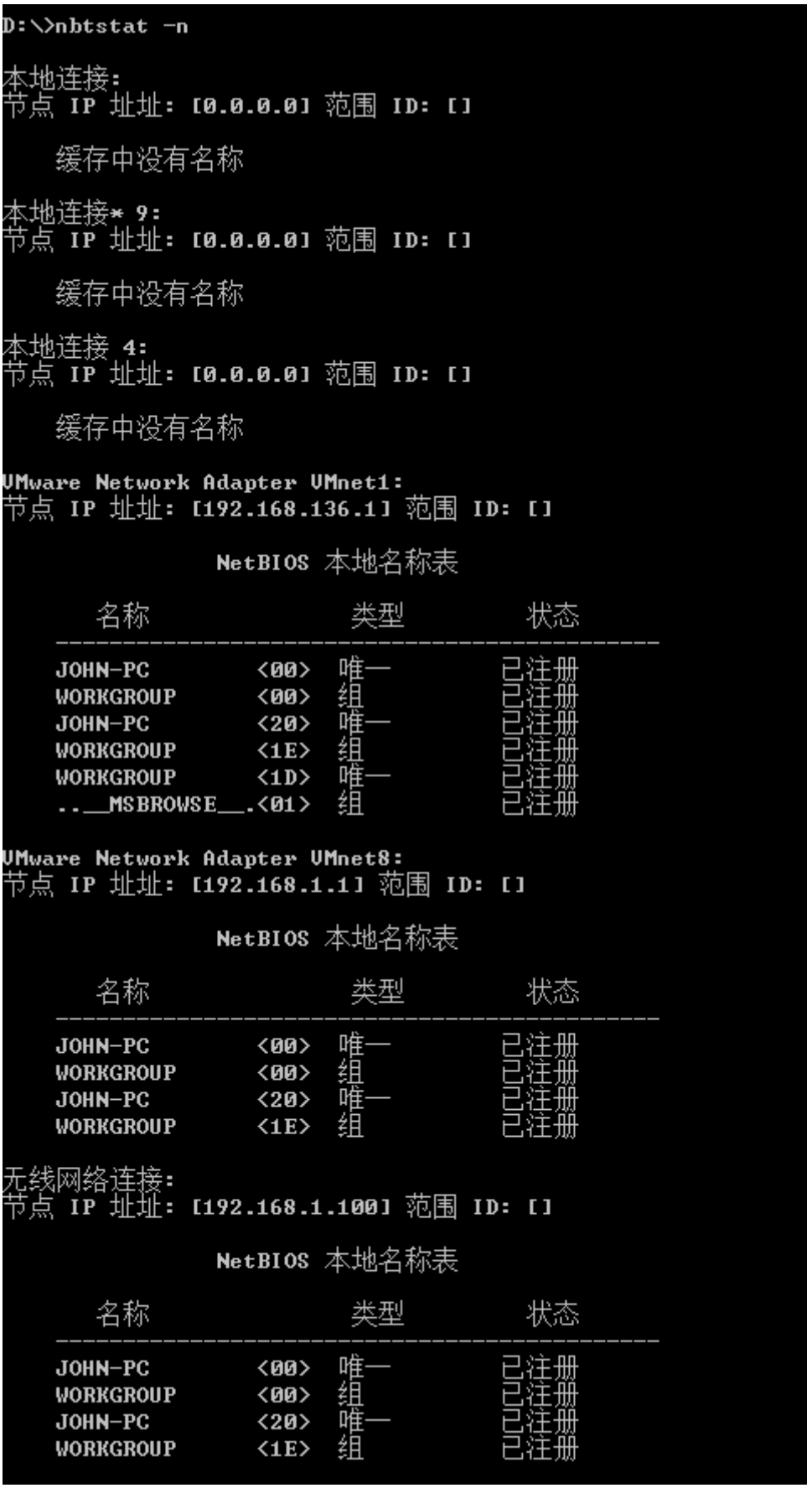
Windows:

D:\>nbtscan-1.0.35.exe -m 192.168.1.0/24

```
D:\>nbtscan-1.0.35.exe -m  192.168.1.0/24
192.168.1.100   WORKGROUP\JOHN-PC
```

D:\>nbtstat -n　　（推荐）

```
D:\>nbtstat

显示协议统计和当前使用 NBI 的 TCP/IP 连接
(在 TCP/IP 上的 NetBIOS)。

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (适配器状态)     列出指定名称的远程机器的名称表
  -A   (适配器状态)     列出指定 IP 地址的远程机器的名称表。
  -c   (缓存)           列出远程[计算机]名称及其 IP 地址的 NBT 缓存
  -n   (名称)           列出本地 NetBIOS 名称。
  -r   (已解析)         列出通过广播和经由 WINS 解析的名称
  -R   (重新加载)       清除和重新加载远程缓存名称表
  -S   (会话)           列出具有目标 IP 地址的会话表
  -s   (会话)           列出将目标 IP 地址转换成计算机 NETBIOS 名称的会话表。
  -RR  (释放刷新)       将名称释放包发送到 WINS, 然后启动刷新

  RemoteName    远程主机计算机名。
  IP address    用点分隔的十进制表示的 IP 地址。
  interval      重新显示选定的统计、每次显示之间暂停的间隔秒数。
                按 Ctrl+C 停止重新显示统计。
```


D:\>nbtstat -n
本地连接:
节点 IP 址址: [0.0.0.0] 范围 ID: []
缓存中没有名称
本地连接* 9:
节点 IP 址址: [0.0.0.0] 范围 ID: []
缓存中没有名称
本地连接 4:
节点 IP 址址: [0.0.0.0] 范围 ID: []
缓存中没有名称
VMware Network Adapter VMnet1:
节点 IP 址址: [192.168.136.1] 范围 ID: []
NetBIOS 本地名称表
名称 类型 状态
JOHN-PC <00> 唯一 已注册
WORKGROUP <00> 组 已注册
JOHN-PC <20> 唯一 已注册
WORKGROUP <1E> 组 已注册
WORKGROUP <1D> 唯一 已注册
..__MSBROWSE__.<01> 组 已注册
VMware Network Adapter VMnet8:
节点 IP 址址: [192.168.1.1] 范围 ID: []
NetBIOS 本地名称表
名称 类型 状态
JOHN-PC <00> 唯一 已注册
WORKGROUP <00> 组 已注册
JOHN-PC <20> 唯一 已注册
WORKGROUP <1E> 组 已注册
无线网络连接:
节点 IP 址址: [192.168.1.100] 范围 ID: []
NetBIOS 本地名称表
名称 类型 状态
JOHN-PC <00> 唯一 已注册
WORKGROUP <00> 组 已注册
JOHN-PC <20> 唯一 已注册
WORKGROUP <1E> 组 已注册

Linux：

（推荐）

root@John:~/Desktop/nbtscan# tar -zxvf ./nbtscan-source-1.0.35.tgz （1.5.1版本在附录）

root@John:~/Desktop/nbtscan# make

root@John:~/Desktop/nbtscan# nbtscan -r 192.168.1.0/24

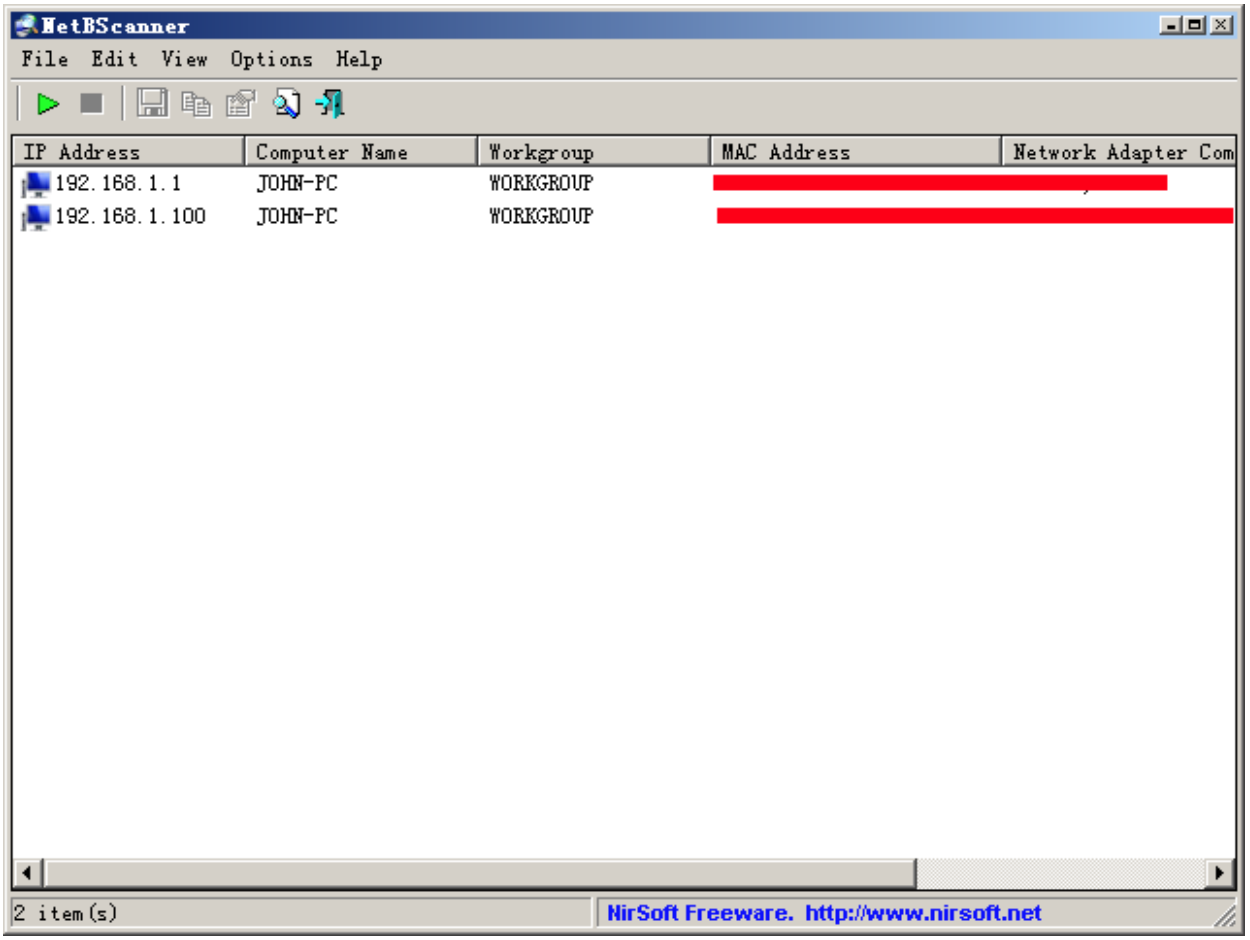
```
root@John:~/Desktop/nbtscan# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.1.0     Sendto failed: Permission denied
192.168.1.107    <unknown>                  <unknown>
192.168.1.100    JOHN-PC          <server>  <unknown>        [redacted]
192.168.1.255   Sendto failed: Permission denied
```

root@John:~/Desktop/nbtscan# nbtscan -v -s: 192.168.1.0/24

```
root@John:~/Desktop/nbtscan# nbtscan -v -s: 192.168.1.0/24
192.168.1.0     Sendto failed: Permission denied
192.168.1.100:JOHN-PC        :00U
192.168.1.100:WORKGROUP      :00G
192.168.1.100:JOHN-PC        :20U
192.168.1.100:WORKGROUP      :1eG
192.168.1.100:MAC:0c:82:68:0d:e6:48
192.168.1.255   Sendto failed: Permission denied
```

NetBScanner：

项目地址：https://www.nirsoft.net/utils/netbios_scanner.html



附录：

nbtscan：

链接：https://pan.baidu.com/s/1hs8ckmg 密码：av40

NBTscan version 1.5.1. Copyright (C) 1999-2003 Alla Bezroutchko.

This is a free software and it comes with absolutely no warranty.

You can use, distribute and modify it under terms of GNU GPL.

Usage:

nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits] (-f filename)|(<scan_range>)

-v verbose output. Print all names received from each host

-d dump packets. Print whole packet contents.

```
    -e          Format output in /etc/hosts format.
    -l          Format output in lmhosts format.
                Cannot be used with -v, -s or -h options.
    -t timeout      wait timeout milliseconds for response.
                Default 1000.
    -b bandwidth    Output throttling. Slow down output
                so that it uses no more that bandwidth bps.
                Useful on slow links, so that ougoing queries
                don't get dropped.
    -r          use local port 137 for scans. Win95 boxes
                respond to this only.
                You need to be root to use this option on Unix.
    -q          Suppress banners and error messages,
    -s separator    Script-friendly output. Don't print
                column and record headers, separate fields with separator.
    -h          Print human-readable names for services.
                Can only be used with -v option.
    -m retransmits  Number of retransmits. Default 0.
    -f filename     Take IP addresses to scan from file filename.
                -f - makes nbtscan take IP addresses from stdin.
    <scan_range>    what to scan. Can either be single IP
                like 192.168.1.1 or
                range of addresses in one of two forms:
                xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
    nbtscan -r 192.168.1.0/24
        Scans the whole C-class network.
    nbtscan 192.168.1.25-137
        Scans a range from 192.168.1.25 to 192.168.1.137
    nbtscan -v -s : 192.168.1.0/24
        Scans C-class network. Prints results in script-friendly
        format using colon as field separator.
        Produces output like that:
        192.168.0.1:NT_SERVER:00U
        192.168.0.1:MY_DOMAIN:00G
```

192.168.0.1:ADMINISTRATOR:03U

192.168.0.2:OTHER_BOX:00U

...

nbtscan -f iplist

Scans IP addresses specified in file iplist.

NBTscan version 1.5.1:

项目地址：https://github.com/scallywag/nbtscan

- Micropoor