专注APT攻击与防御

https://micropoor.blogspot.com/

UDP简介：

UDP（User Datagram Protocol）是一种无连接的协议，在第四层-传输层，处于IP协议的上一层。UDP有不提供数据包分组、组装和不能对数据包进行排序的缺点，也就是说，当报文发送之后，是无法得知其是否安全完整到达的。

UDP显著特性：

1.UDP 缺乏可靠性。UDP 本身不提供确认，超时重传等机制。UDP 数据报可能在网络中被复制，被重新排序，也不保证每个数据报只到达一次。

2.UDP 数据报是有长度的。每个 UDP 数据报都有长度，如果一个数据报正确地到达目的地，那么该数据报的长度将随数据一起传递给接收方。而 TCP 是一个字节流协议，没有任何（协议上的）记录边界。

3.UDP 是无连接的。UDP 客户和服务器之前不必存在长期的关系。大多数的UDP实现中都选择忽略源站抑制差错，在网络拥塞时，目的端无法接收到大量的UDP数据报

4.UDP 支持多播和广播。

1.nmap扫描

root@John:~# nmap -sU -T5 -sV --max-retries 1 192.168.1.100 -p 500

慢的令人发指

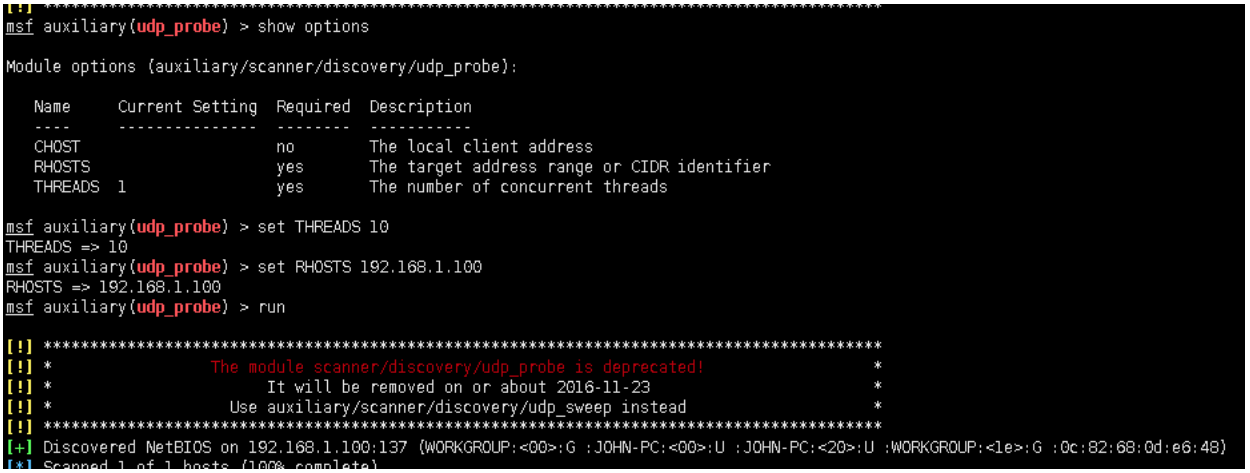
```
root@John:~# nmap -sU -T5 -sV --max-retries 1 192.168.1.100 -p 500

Starting Nmap 7.40 ( https://nmap.org ) at 2017-11-27 00:48 EST
Nmap scan report for 192.168.1.100
Host is up (0.024s latency).
PORT    STATE         SERVICE VERSION
500/udp open|filtered isakmp
MAC Address: 0C:82:68:0D:E6:48 (Tp-link Technologies)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.44 seconds
root@John:~#
```

2.msf扫描

msf > use auxiliary/scanner/discovery/udp_probe

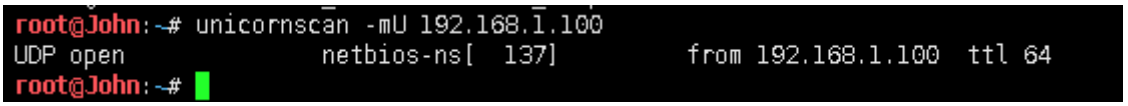


msf > use auxiliary/scanner/discovery/udp_sweep

3.unicornscan扫描

linux下使用推荐

root@John:~# unicornscan -mU 192.168.1.100



4.ScanLine扫描

项目地址：https://www.mcafee.com/ca/downloads/free-tools/scanline.aspx

网盘地址：http://pan.baidu.com/s/1i4A1wLR 密码：hvyx

McAfee出品，win下使用推荐。管理员执行。

```
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

sl [-?bhijnprsTUvz]
   [-cdgmq <n>]
   [-flLoO <file>]
   [-tu <n>[,<n>-<n>]]
   IP[,IP-IP]

 -?  - Shows this help text
 -b  - Get port banners
 -c  - Timeout for TCP and UDP attempts (ms). Default is 4000
 -d  - Delay between scans (ms). Default is 0
 -f  - Read IPs from file. Use "stdin" for stdin
 -g  - Bind to given local port
 -h  - Hide results for systems with no open ports
 -i  - For pinging use ICMP Timestamp Requests in addition to Echo Requests
 -j  - Don't output "------..." separator between IPs
 -l  - Read TCP ports from file
 -L  - Read UDP ports from file
 -m  - Bind to given local interface IP
 -n  - No port scanning - only pinging (unless you use -p)
 -o  - Output file (overwrite)
 -O  - Output file (append)
 -p  - Do not ping hosts before scanning
 -q  - Timeout for pings (ms). Default is 2000
 -r  - Resolve IP addresses to hostnames
 -s  - Output in comma separated format (csv)
 -t  - TCP port(s) to scan (a comma separated list of ports/ranges)
 -T  - Use internal list of TCP ports
 -u  - UDP port(s) to scan (a comma separated list of ports/ranges)
 -U  - Use internal list of UDP ports
 -v  - Verbose mode
 -z  - Randomize IP and port scan order

Example: sl -bht 80,100-200,443 10.0.0.1-200
```

```
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Mon Nov 27 14:29:09 2017

-------------------------------------------------
192.168.1.100
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes

UDP ports: 500
```

附录：

在线基于Nmap的udp扫描：https://pentest-tools.com/network-vulnerability-scanning/udp-port-scanner-online-nmap

- Micropoor