BT5 2011

作者：现任明教教主

北京Yeslab安全实验室出品

1.信息收集

2.扫描工具

3.漏洞发现

4.社会工程学工具

5.运用层攻击MSF

6.局域网攻击

7.密码破解

8.维持访问

内容简介

第一部分:DNS信息收集

第二部分:路由信息收集

第三部分:All-in-one智能收集

第一部分

DNS信息收集

1.Dnsmap介绍

1.Get extra names and subdomains utilizing the Google search engine.（使用**google**搜索引擎获取额外的名字与子域名）

2.Find out subdomain names by brute forcing the names from the text file. The dnsenum included in BackTrack comes with a file (dns.txt) containing 95 subdomain names.（使用一个TXT文件暴力破解子域名）

3.Carry out Whois queries on C-class domain network ranges and calculate its network ranges.（使用**Whois**查询**C**类网络范围，并且计算网络范围）

4.Carry out reverse lookup on network ranges.（反向查询）

5.Use threads to do different queries.（支持多重查询）

1.Dnsenum命令

root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl -f dns.txt -dnsserver 8.8.8.8 cisco.com -o cisco.txt

1.-f dns.txt指定暴力破解文件，可以换成dns-big.txt

2.-dnsserver指定dns服务器

3.cisco.com为目标域

4.-o cisco.txt输出到文件cisco.txt

2.Dnsmap介绍

The dnsmap tool uses an approach similar to that of dnsenum to find out subdomains. It comes with a built-in wordlist for brute forcing, and it can also use a user-supplied wordlist. Additional features provided by dnsmap are that the results can be saved in the Comma Separated Value (CSV) format for further processing and it doesn't need a root privilege to run.

（非常类似于**dnsenum**，可以使用内建的“**wordlist**”来暴力破解子域，也可以使用用户自定义的“**wordlist**”。**Dnsmap**支持把结果输出为**CSV**格式。并且运行时不需要**root**权限。

2.Dnsmap命令

root@bt:/pentest/enumeration/dns/dnsmap# ./dnsmap cisco.com -w wordlist_TLAs.txt -c cisco.csv

1.-w wordlist_TLAs.txt 指定暴力破解文件

2.-c cisco.csv 输出文件

3.cisco.com为目标域

第二部分

路由信息收集

1. tcptraceroute介绍（1）

The tcptraceroute can be used as a complement to the traditional traceroute command. While the traceroute is using UDP or ICMP ECHO to send out the packet with a Time To Live (TTL) of one, and incrementing it until reaching the target, the tcptraceroute is using TCP SYN to send out the packet to the target.

（传统traceroute技术发送UDP或者ICMP ECHO，但是tcptraceroute发送TCP SYN包到目标。）

1. tcptraceroute介绍（2）

The advantage of using tcptraceroute is that if there is a firewall sitting between the penetration tester and the target and it's blocking traceroute it still allows incoming TCP packet to certain TCP ports, and so by using tcptraceroute we will still be able to reach the target behind the firewall.

（使用**tcptraceroute**的好处在于，就算在目标之前存在防火墙，它阻止了普通的**traceroute**的流量，但是适当**TCP**端口的流量，防火墙是放行的，所以**tcptraceroute**能够穿越防火墙抵达目标）

tcptraceroute will receive a SYN/ACK packet if the port is open, and it will receive a RST packet if the port is closed.

（**tcptraceroute**收到**SYN/ACK**表示端口是开放的，收到**RST**表示端口是关闭的）

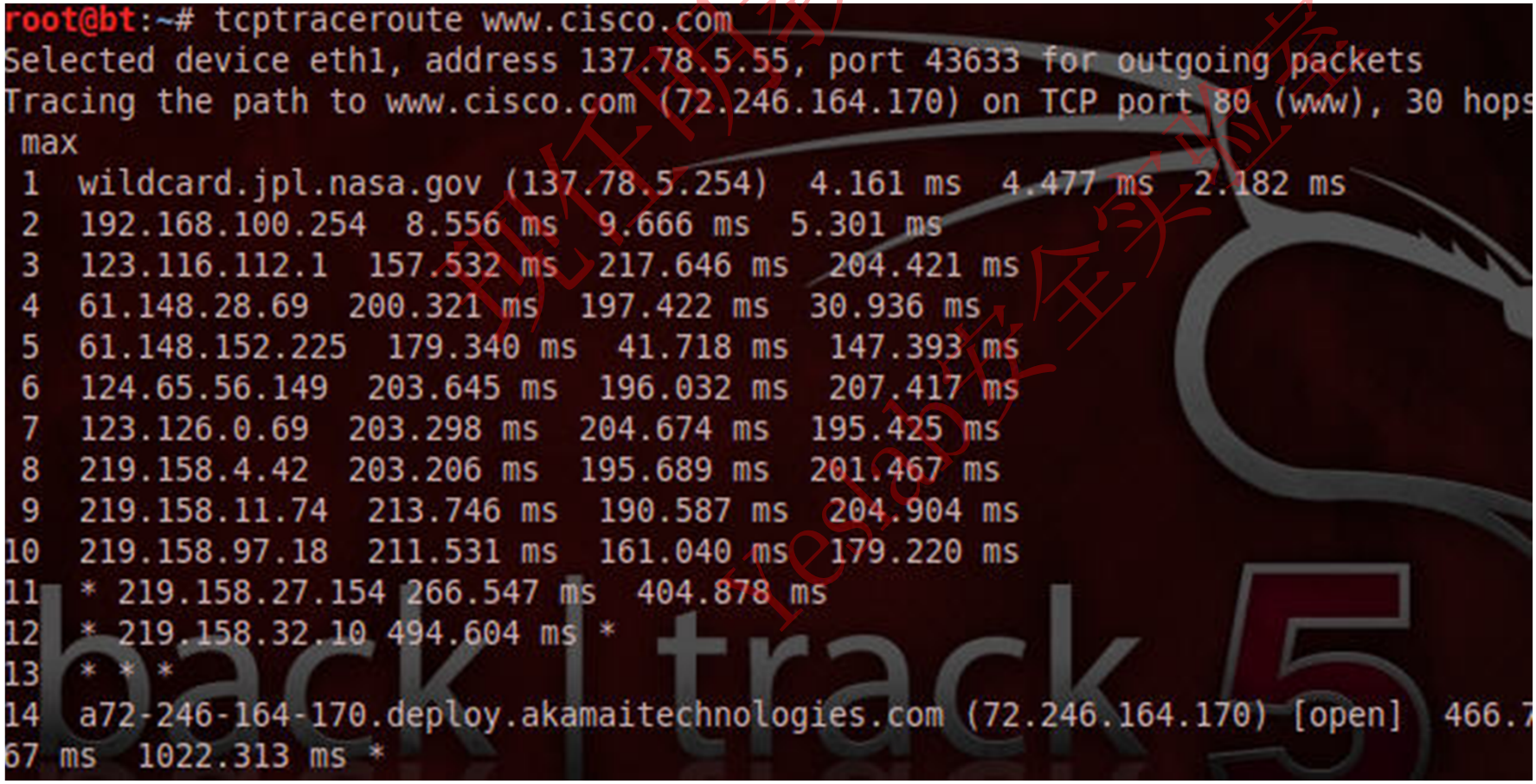
第二部分

路由信息收集

传统traceroute效果

```
root@bt:~# traceroute www.cisco.com
traceroute to www.cisco.com (72.246.164.170), 30 hops max, 60 byte packets
 1  wildcard.jpl.nasa.gov (137.78.5.254)  5.164 ms  5.281 ms  4.936 ms
 2  192.168.100.254 (192.168.100.254)  21.708 ms  21.222 ms  21.931 ms
 3  123.116.112.1 (123.116.112.1)  61.713 ms  63.766 ms  196.235 ms
 4  61.148.28.69 (61.148.28.69)  44.279 ms  43.934 ms  45.386 ms
 5  61.148.152.225 (61.148.152.225)  46.520 ms  57.708 ms  58.975 ms
 6  124.65.56.149 (124.65.56.149)  60.757 ms  60.054 ms  65.141 ms
 7  123.126.0.69 (123.126.0.69)  64.835 ms  164.483 ms  164.047 ms
 8  219.158.4.42 (219.158.4.42)  165.326 ms  153.639 ms  153.141 ms
 9  219.158.11.74 (219.158.11.74)  151.994 ms  150.726 ms  139.334 ms
10  219.158.97.18 (219.158.97.18)  132.134 ms  131.852 ms  131.362 ms
11  * 219.158.27.154 (219.158.27.154)  329.895 ms  326.180 ms
12  * * 219.158.32.10 (219.158.32.10)  235.217 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
```

Tcptraceroute效果



2. tctrace介绍

The tctrace tool is similar to tcptraceroute, but instead of using ICMP ECHO it uses the TCP SYN packet.

（tctrace工具非常类似于tcptraceroute，它不使用ICMP ECHO而是使用TCP SYN数据包）

Tctrace效果

```
root@bt:/pentest/enumeration/irpas# ./tctrace -i eth2 -d www.cisco.com
 1(1)   [196.21.5.254]
 2(1)   [114.249.240.1]
 3(1)   [125.35.65.105]
 4(1)   [202.106.227.117]
 5(1)   [124.65.56.121]
 6(1)   [202.96.12.53]
 7(1)   [219.158.4.82]
 8(1)   [219.158.11.18]
 9(1)   [219.158.97.10]
10(2)   [219.158.29.170]
11(1)   [219.158.32.10]
12(all) Timeout
13(1)   [72.246.164.170] (reached; open)
```

第三部分

All-in-one智能收集

Maltego介绍（1）

Maltego is an open source intelligence and forensics application. It allows you to mine and gather information, and represent the information in a meaningful way.

（**Maltego**是一个开放源的智能信息收集工具）

Maltego allows you to enumerate Internet infrastructure information, such as:

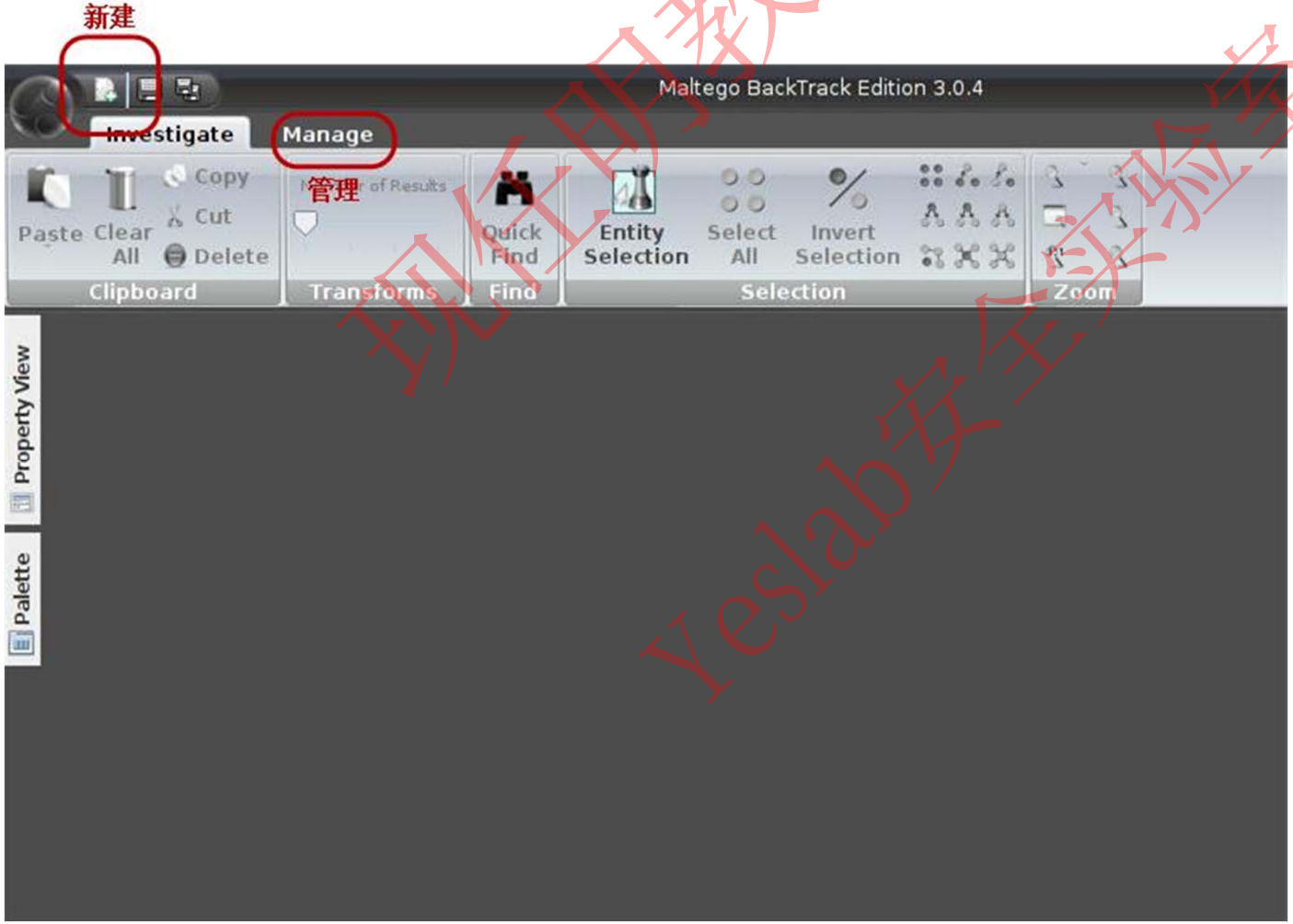
1. Domain names （域名）
2. DNS names （DNS名）
3. Whois information （Whois信息）
4. Network blocks （网段）
5. IP addresses （IP地址）

Maltego介绍（2）

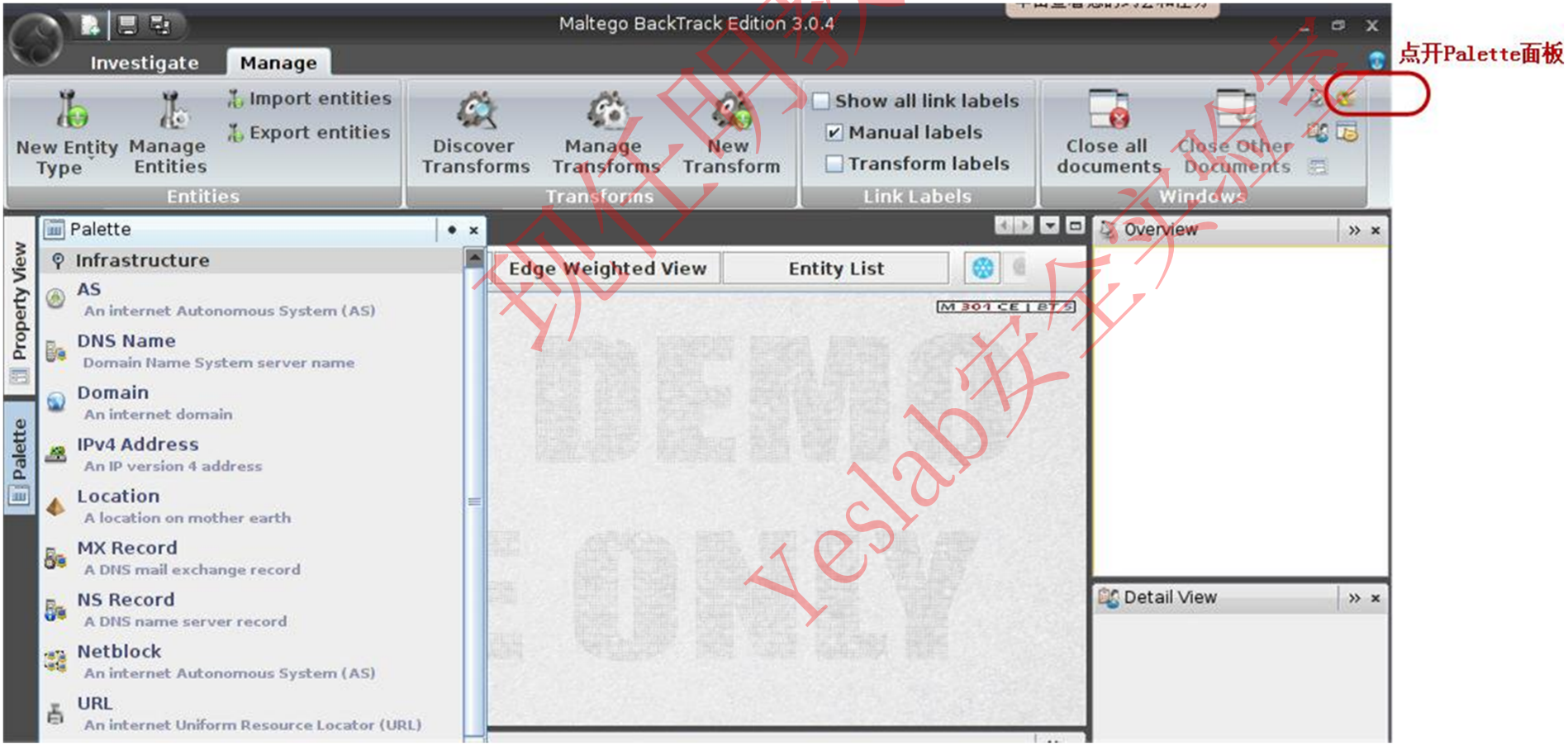
It can also be used to gather information about people, such as:（还能够收集人的信息）

1. Companies and organizations related to the person
   （公司或者组织关联到的人）
2. E-mail address related to the person（电邮地址关联到的人）
3. Websites related to the person（网站关联到的人）
4. Social networks related to the person（社区网络关联到的人）
5. Phone numbers related to the person（电话号码关联到的人）

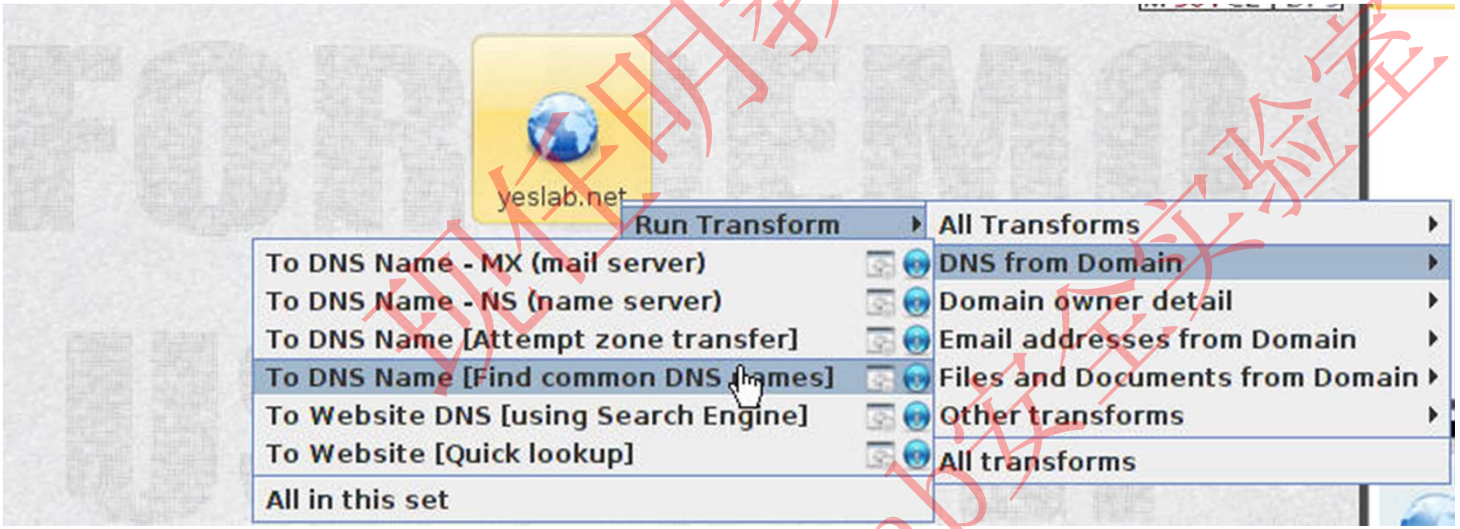
Maltego使用（1）



Maltego使用（2）



Maltego使用（3）



Maltego使用（4）