禪

15 – [illegible] CEH [illegible]

[illegible] CEH [illegible] :([illegible])

[illegible] UDP [illegible] TCP [illegible] 65 [illegible] UDP [illegible] TCP [illegible] 1024 [illegible].

[illegible] CEH [illegible].

[illegible]

[illegible] Whois [illegible] https://www.arin.net [illegible] ARIN Whois [illegible] 192.17.170.17 [illegible]:

OrgName: target network

OrgID: Target-2

Address: 1313 Mockingbird Road

City: Anytown

StateProv: Tx

PostalCode: 72341

Country: US

ReferralServer: rwhois://rwhois.exodus.net:4321/

NetRange: 192.17.12.0 - 192.17.12.255

CIDR: 192.17.0.0/24

NetName: SAVVIS

NetHandle: NET-192-17-12-0-1

Parent: NET-192-0-0-0-0

[illegible] 254 [illegible] 192.17.12.1 [illegible] 192.17.12.254/24 [illegible] traceroute [illegible].

[illegible] Mapping Networks

[illegible] (subnetting) [illegible] B [illegible] A [illegible] C [illegible] C [illegible] 192.168.5.0 [illegible] 255.255.255.0 [illegible].

192.168.5.0 - 11001100.10101000.00000101.00000000

255.255.255.224 - 11111111.11111111.11111111.11100000

---|subnet|----

[illegible] 255.255.255.0 [illegible] 255.255.255.224 [illegible] 3 [illegible] 3 [illegible] 5 [illegible] 32 [illegible].

Subnet Host Range

192.168.5.0 255.255.255.224 host address range 1 to 30

192.168.5.32 255.255.255.224 host address range 33 to 62

192.168.5.64 255.255.255.224 host address range 65 to 94

192.168.5.96 255.255.255.224 host address range 97 to 126

192.168.5.128 255.255.255.224 host address range 129 to 158

192.168.5.160 255.255.255.224 host address range 161 to 190

192.168.5.192 255.255.255.224 host address range 193 to 222

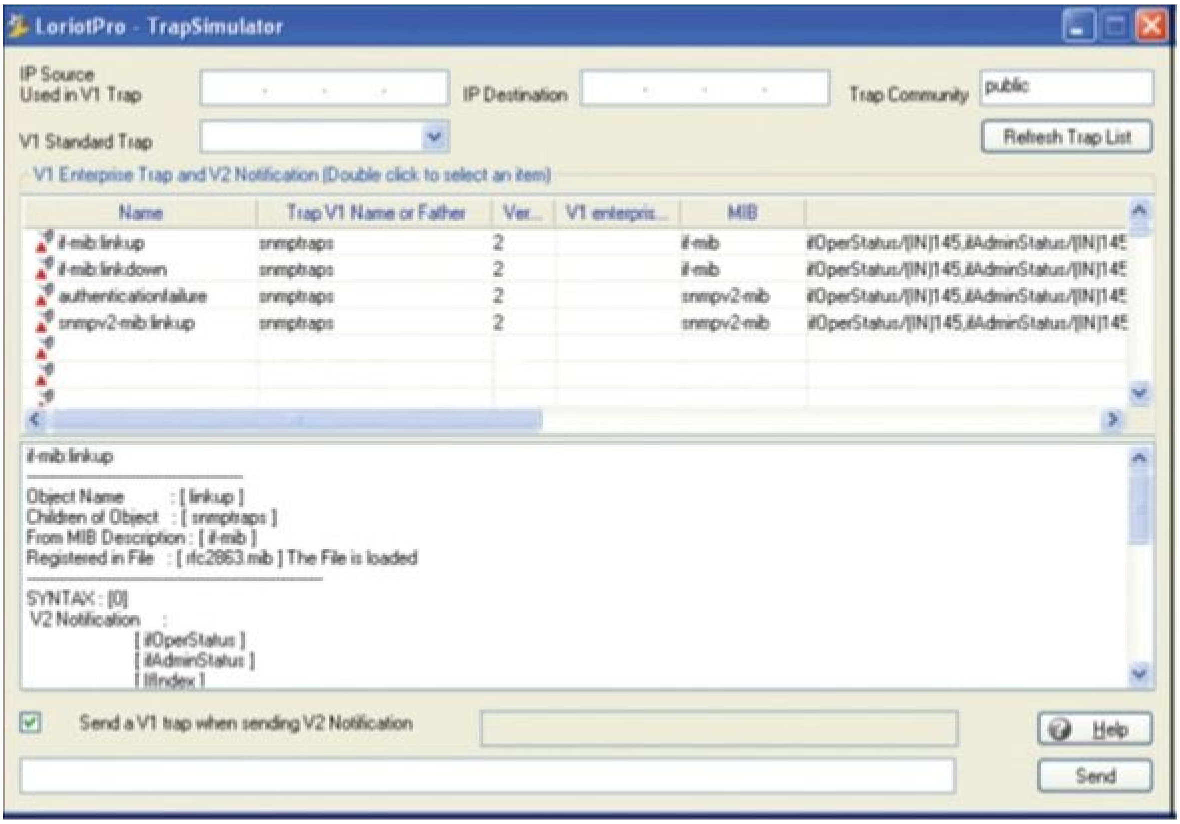
192.168.5.224 255.255.255.224 host address range 225 to 254

[illegible]

Traceroute

[illegible]

■ LoriotPro [illegible]: LoriotPro [illegible] SNMP [illegible]



Trap Community: public

Name	Trap V1 Name or Father	Ver...	V1 enterpris...	MIB	
if-mib:linkup	snmptraps	2		if-mib	ifOperStatus/[IN]145,ifAdminStatus/[IN]145
if-mib:linkdown	snmptraps	2		if-mib	ifOperStatus/[IN]145,ifAdminStatus/[IN]145
authenticationfailure	snmptraps	2		snmpv2-mib	ifOperStatus/[IN]145,ifAdminStatus/[IN]145
snmpv2-mib:linkup	snmptraps	2		snmpv2-mib	ifOperStatus/[IN]145,ifAdminStatus/[IN]145

```
if-mib:linkup
------------------------------
Object Name        : [ linkup ]
Children of Object  : [ snmptraps ]
From MIB Description : [ if-mib ]
Registered in File  : [ rfc2863.mib ] The File is loaded
-----------------------------------------
SYNTAX : [0]
 V2 Notification     :
                [ ifOperStatus ]
                [ ifAdminStatus ]
                [ ifIndex ]
```

☑ Send a V1 trap when sending V2 Notification

■ Trout: ابزار Trout یکی دیگر از برنامههای بصری است که ترکیبی از قابلیتهای Whois و traceroute را ارائه میکند . خوشبختانه این برنمه سرعت زیادی دارد . بر خلاف برنامههای سنتی ردیابی، Trout پینگهای موازی انجام میدهد . با ارسال بستههایی با بیش از یک TTL بهطور همزمان، میتواند به سرعت مسیر یک دستگاه هدف را تعیین کند.

■ VisualRout: ابزار VisualRoute یکی دیگر از ردیابهای گرافیکی مبتنی بر ویندوز است . VisualRoute نه تنها یک نقشه جهانی گرافیکی را نشان میدهد که مسیر بستهها را به خوبی نشان میدهد، بلکه اطلاعات مربوط به هر هاپ از جمله آدرس آیپی، نام گره و موقعیت جغرافیایی را نیز نشان میدهد .

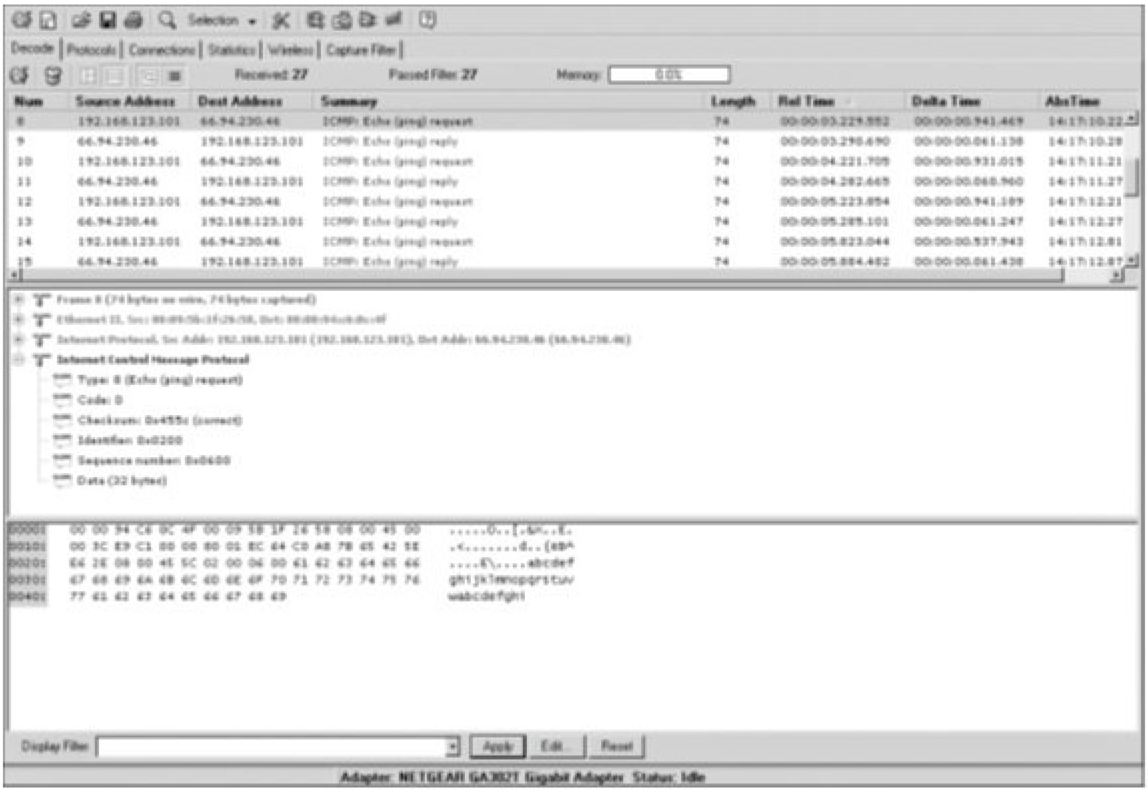
نکته : Traceroute و ping ابزارهای مفیدی برای شناسایی سیستمهای فعال، نقشهبرداری از مکان دستگاهها و کسب اطلاعات بیشتر در مورد مکان دستگاهها است.

شناسایی ماشینهای فعال

مهاجمان همواره به دنبال این پاسخ هستند که آیا ماشینها قبل از آنکه حمله خود را پیادهسازی کنند فعال هستند یا خیر . یکی از اساسیترین روشهای شناسایی ماشینهای فعال انجام ping sweep است. اگرچه پینگ تقریباً در مورد هر سیستم TCP / IP قابل اجرا است، اما توسط بسیاری از سازمانها محدود شده است. پینگ از ICMP استفاده میکند و با ارسال یک درخواست اکو به یک سیستم صبر میکند تا پاسخ اکو را دریافت کند . اگر دستگاه هدف غیرقابل دستیابی باشد عبارت request timeout بازگردانده میشود . پینگ یک ابزار مفید برای شناسایی ماشینهای فعال و اندازهگیری سرعت انتقال بستهها از یک میزبان به میزبان دیگر یا به دست آوردن جزئیاتی همچون TTL است. شکل زیر پینگ دریافت شده از یک کامپیوتر ویندوزی را نشان میدهد .

اگر چند لحظهای از وضعیت خود را صرف رمزگشایی کدهای اسکی کندی که در پایین سمت چپ نشا داده شده، متوجه خواهید شد که دادههای موجود در بسته ping از حروف الفبا تشکیل شدهاند که بر خلاف پینگ لینوکس است که حاوی مقادیر عددی است. این بدان دلیل است که RFC که حاوی پینگ است ، مشخص نمی کند چه باردادهایی باید در بستهها تحویل داده شود . به همین دلیل ارائه اطلاعات به نوع نگرش تولیدکنندگان بستگی دارد . متأسفانه، رویکرد فوق میتواند به عنوان کانال مخفی در اختیار هکرها قرار گیرد . هکرها میتوانند از برنامههای متنوعی استفاده کنند تا اطلاعات موجود در بستههای رایج را تغییر دهند .

ابزارهایی مانند Loki و icmpsend فقط برای این منظور طراحی شدهاند تا نشان دهند همه چیز در قالب یک پینگ عادی انجام شده و در واقع یک سری پیام به شبکه وارد شده یا از آن خارج شده است .



```
Num  Source Address   Dest Address     Summary                    Length  Rel Time          Delta Time        AbsTime
8    192.168.123.101  66.94.230.46     ICMP: Echo (ping) request  74      00:00:03.229.552  00:00:00.941.469  14:17:10.22
9    66.94.230.46     192.168.123.101  ICMP: Echo (ping) reply    74      00:00:03.290.690  00:00:00.061.138  14:17:10.28
10   192.168.123.101  66.94.230.46     ICMP: Echo (ping) request  74      00:00:04.221.705  00:00:00.931.015  14:17:11.21
11   66.94.230.46     192.168.123.101  ICMP: Echo (ping) reply    74      00:00:04.282.665  00:00:00.060.960  14:17:11.27
12   192.168.123.101  66.94.230.46     ICMP: Echo (ping) request  74      00:00:05.223.854  00:00:00.941.189  14:17:12.21
13   66.94.230.46     192.168.123.101  ICMP: Echo (ping) reply    74      00:00:05.285.101  00:00:00.061.247  14:17:12.27
14   192.168.123.101  66.94.230.46     ICMP: Echo (ping) request  74      00:00:05.823.044  00:00:00.537.943  14:17:12.81
15   66.94.230.46     192.168.123.101  ICMP: Echo (ping) reply    74      00:00:05.884.482  00:00:00.061.438  14:17:12.87
```

```
Frame 8 (74 bytes on wire, 74 bytes captured)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x455c (correct)
    Identifier: 0x0200
    Sequence number: 0x0600
    Data (32 bytes)
```

```
0000:  00 00 94 C6 0C 4F 00 09 5B 1F 26 58 08 00 45 00   ......O..[.&X..E.
0010:  00 3C E9 C1 00 00 80 01 EC 64 C0 A8 7B 65 42 5E   .<........d...{eB^
0020:  E6 2E 08 00 45 5C 02 00 06 00 61 62 63 64 65 66   ....E\....abcdef
0030:  67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76   ghijklmnopqrstuv
0040:  77 61 62 63 64 65 66 67 68 69                     wabcdefghi
```

پینگ دو مشکل دارد، اول آنکه تنها به یک سیستم در یک زمان پینگ میکند و دوم اینکه، همه شبکهها اجازه پینگ نمیدهند . برای پینگ به تعداد زیادی از میزبانها معمولا باید از تکنیک ping sweep استفاده کرد . برنامههایی که از تکنیک ping sweep استفاده میکنند، معمولا به طیف وسیعی از دستگاهها پینگ انجام میدهند تا هر کدام که فعال هستند را پیدا کنند . از مهمترین برنامههایی که از فرآیند فوق استفاده میکنند به موارد زیر میتوان اشاره کرد :

- Angry IP Scanner: http://angryip.org/
- Hping: http://www.hping.org/
- WS_Ping ProPack: https://ws-ping-propack.en.softonic.com/
- SuperScan: http://www.mcafee.com/us/downloads/free-tools/superscan.aspx
- Nmap: https://nmap.org/

یافتن پورتهای باز و اکسسپویینتها

اسکن پورت فرآیند اتصال به پورتهای TCP و UDP به منظور پیدا کردن سرویسها و برنامههای کاربردی در دستگاه هدف است. پس از کشف برنامههای در حال اجرا، پورتهای باز و سرویسها به هکرها اجازه میدهند بهترین راه حمله به سامانهها را مشخص کنند . همانگونه که پیشتر اشاره کردیم، در مجموع 65535 پورت TCP و UDP وجود دارد . این شماره پورتها برای شناسایی یک فرآیند خاص که یک پیام از آن وارد میشود یا به آن وارد میشوند استفاده میشود . از مهمترین پورتهای رایج به موارد زیر میتوان اشاره کرد :

Port	Protocol	Service/Transport
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

نکته : آزمون CEH ممکن است در مورد پورتهای رایج یا نه چندان رایج مانند 514 در ارتباط (syslog)⬚⬚ ، پورت 2381 در ارتباط با (Compaq Insight Manager) یا حتا 179 (پروتکل چاپ اینترنتی) سؤال کند. به همین دلیل بهتر است اطلاعات خوبی در ارتباط با این پورتها داشته باشید .

همانگونه که متوجه شدهاید، برخی از این برنامهها با TCP و برخی دیگر از UDP استفاده میکنند . اگرچه مطمئناً اسکن کردن تمامی 65 هزار درگاه در ارتباط با پروتکلهای TCP و UDP امکانپذیر است، اما بسیاری از هکرها این کار را نمیکنند . آنها عمدتا روی 1024 درگاه اول روی سامانهها متمرکز میشوند، زیرا پورتهای معروفی هستند که بیشتر برنامههای رایج از آنها استفاده میکنند . برای کسب اطلاعات بیشتر در خصوص این پورتها پیشنهاد میکنم به آدرس **portnumbers** بروید .

دقت کنید که ما نمیگوییم از پورتهای بالاتر صرفنظر کنید، زیرا این احتمال وجود دارد که هکرها برای ورود به یک سامانه از پورت شماره بالا شبیه به 31337 استفاده کرده و آن پورت را به عنوان درب پشتی در نظر بگیرند . پرسش مهم دیگری که برخی کاربران مطرح میکنند این است که آیا اسکن یک پروتکل نسبت به دیگری آسانتر است؟ پاسخ مثبت است. TCP به نسبت UDP فرصتهای بیشتری برای دستکاری در اختیار هکرها قرار میدهد . چرا این گونه است؟ TCP ارتباطات پایداری ارائه میکند و به عنوان یک پروتکل اتصالگرا شناخته میشود . TCP با انتشار یک ارتباط از یک رویکرد دستدهی سه مرحلهای استفاده میکند . این سه مرحله به شرح زیر است:

1. کلاینت یک بسته TCP را با مجموعهای از شمارههای ترتیب اولیه (ISN) و تعدادی پرچم دنبالهدار (SYN flag) برای سرور ارسال میکند .

2. سرور با ارسال یک بسته با پرچم SYN / ACK به کلاینت پاسخ میدهد که بیانگر تمایل به برقراری ارتباط است. در این حالت پرچم تصدیق در سمت کلاینت که فلگ act نام دارد مقداردهی اولیه میشود . شماره تأیید یک رقم بالاتر از فلگ ISN کلاینت خواهد بود . سرور همچنین ISN را برای پیگیری هر بایت ارسالی به کلاینت ایجاد میکند .

3. هنگامی که کلاینت بسته سرور را دریافت میکند یک بسته ACK ایجاد میکند تا تأیید کند که دادهها از سرور دریافت شده است. در این مرحله ارتباطات آغاز میشود .

سرآیند TCP شامل یک فیلد 1 بایتی برای فلگها است . از مهمترین و پر کاربردترین فلگها به موارد زیر

میتوان اشاره کرد :

SYN: شماره ترتیبی را مقداردهی و همگامسازی میکند .

ACK: بیانگر تایید بستههای دریافتی است .

FIN: این فلگ نشان دهنده یک فرآیند چهار مرحلهای پایان یک نشست است.

RST: بیتی که برای خاتمه دادن به یک ارتباط غیرمعمول استفاده شده را ریست میکند .

PSH: اگر به 1 باشد، دادهها باید بدون بافر شدن برای یک برنامه ارسال شوند .

URG: اگر 1 باشد، اعلام میدارد که فیلد اشارهگر Urgent درون سگمنت اطلاعاتی قرار داده که گیرنده باید آنرا پردازش کند . اگر 0 باشد، گیرنده از فیلد اشارهگر Urgent صرفنظر خواهد کرد .

در پایان ارتباط، TCP نشست را در یک فرآیند چهار مرحلهای پایان میدهد .

1. کلاینت یک بسته با مجموعهای از فلگهای FIN / ACK به سرور ارسال میکند .

2. سرور یک بسته که شامل مجموعهای از فلگهای ACK است را برای تأیید به سمت کلاینت ارسال میکند .

3. سرور در ادامه بسته دیگری با مجموعه فلگهای FIN/ACK را تنظیم میکند تا به کلاینت اطلاع دهد آماده خاتمه دادن به نشست است.

4- کلاینت به سمت سرور بستهای که حاوی فلگ ACK است را ارسال میکند که بیانگر پایان نشست است .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره **CEH**

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
10:40 - 28/12/1398
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - هک اخلاقی

نشانی
:https://www.shabakeh-mag.com/security/16682/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%85%D8%AD%D8%AF%D9%88%D8%AF%D9%87-%DB%8C%DA%A9-%D8%B4%D8%A8%DA%A9%D9%87-%D9%88-%D8%B2%DB%8C%D8%B1%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7-%D8%B1%D8%A7-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%DA%A9%D9%86%DB%8C%D9%85%D8%9F