پویش به روش Idle / نهایت پنهان بودن در Prot Scanning

اواسط دسامبر سال 1998 بود که یک محقق امنیتی به نام Antirez نوع و شیوه جدیدی در Port Scanning را معرفی کرد. در این روش که مبتنی بر TCP است حتی یک Packet هم از طرف مهاجم (با هویت واقعی مهاجم) به هدف ارسال نمی گردد به همین دلیل است که از محبوبیت خاصی در بین نفوذگران حرفه ای برخوردار است. اساس این حمله بر متهم جلوه دادن ماشین بی گناهی است که در اینجا به آن زامبی/zombie می گوییم. این عمل را اصطلاحاً bounce کردن گوییم. در این هنگام است که سیستم های تشخیص نفوذ (IDS) ماشین زامبی را به عنوان مهاجم شناسایی می کنند!

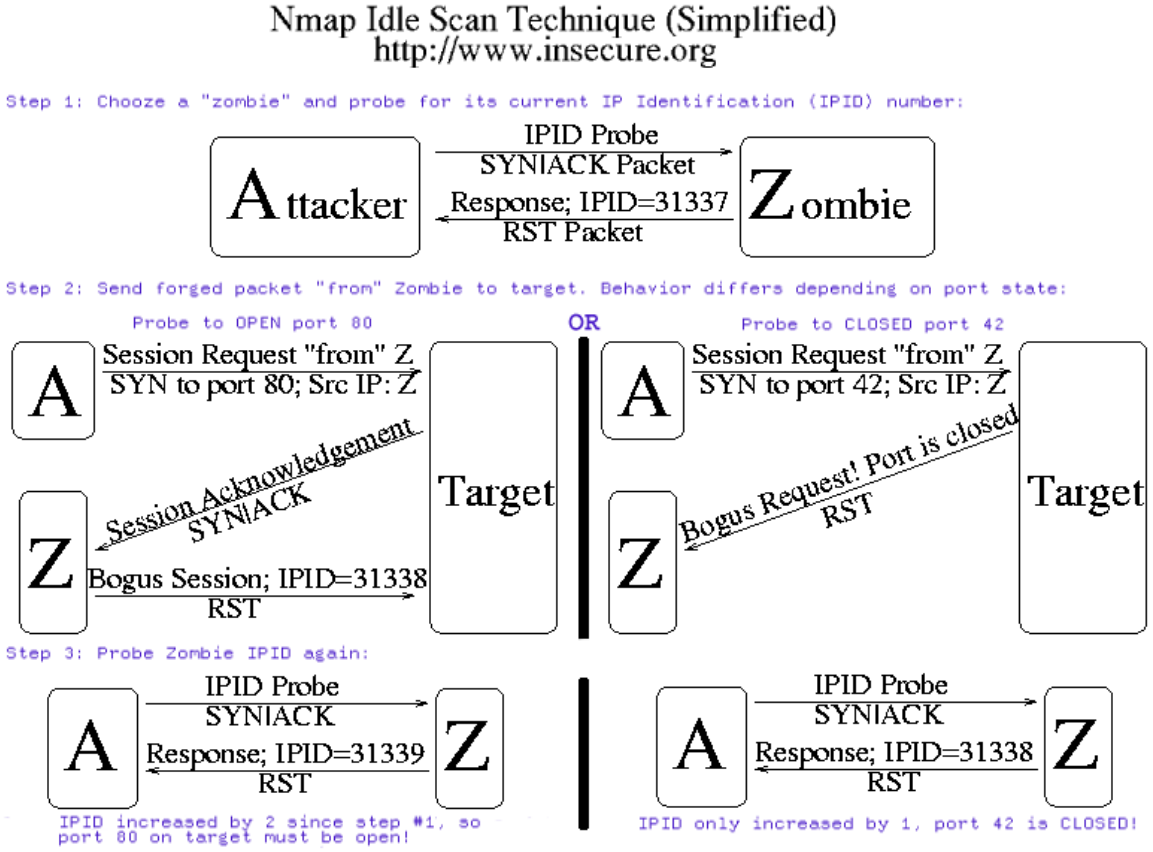
* گاهی به این روش scan کردن Blind هم می گویند.

برخلاف فوق العاده پیشرفته و موثر بودن این نوع پویش برای فهم و یادگیری آن به دانش و مهارت های زیادی نیاز ندارید. فقط کافیست مواردی پایه ای از اصول شبکه های TCP/IP را بدانید:

- بیشتر سرویس های شبکه ای به پورت های TCP گوش می دهند. (Listening Mode). به عنوان مثال وب سرور ها بر روی پورت 80 و سرویس های e-Mail بر روی پورت 25 گوش می دهند. زمانی که برنامه یا سرویسی در پشت یک پورت متصل باشد و در Listening Mode قرار گرفته باشد، می گوییم آن پورت باز/open است، در غیر این صورت پورت بسته است.
- یکی از راه های تشخیص یک پورت باز، ارسال یک Packet با فلگ "SYN" یا همان SYN Flag به آن پورت است. وظیفه این فلگ Session Establishment است. اگر پورت مورد نظر ما روی ماشین هدف باز باشد، ماشین مورد نظر با یک پکت با فلگ های SYN/ACK پاسخ می دهد (Session Request Acknowledgment) و در صورتی که پورت مورد نظر بسته باشد یک پکت RST (Reset) از طرف ماشین هدف ارسال می گردد. (برای فهم بیشتر این اصل، اصول 3-way-handshak را مطالعه نمایید)
- هر ماشینی که یک Packet ناخواسته SYN/ACK را دریافت نماید با یک RST به آن پاسخ می دهد (منظور از ناخواسته در اینجا زمانی است که ماشین پکت SYN را ارسال نکرده است ولی یک SYN/ACK دریافت کرده است!).
- هنگامی که یک ماشین یک پکت RST ناخواسته دریافت کند آن را در نظر نمی گیرد و هیچ جوابی به آن نمی دهد (Ignore).
- هر پکت IP در اینترنت شامل یک شماره به نام Fragment Identification است. برخی از سیستم عامل ها/OS با ارسال هر پکت یک شماره به این عدد اضافه می کنند. نفوذگر با تعیین و دنبال کردن این عدد قادر به تشخیص تعداد پکت های ارسالی هدف خواهد بود.

اگر مقداری زیرکانه به این خصائص نگاه کنید در خواهید یافت که با ترکیب این خصوصیت ها قادر خواهیم بود شبکه هدف خود را پویش کرده و همزمان گناه این کار را به گردن شخص بی گناه دیگری به نام زامبی/zombie بیاندازیم و هویت خود را کاملاً جعل نماییم! برای فهم بهتر این مطلب به شکل زیر توجه کنید. در شکل زیر مهاجم با A مشخص شده است که مشغول پویش سیستم هدف یا همان Target است که گناه این کار را به گردن شخص ثالثی به نام Zombie می اندازد. در شکل زیر جعبه ها/Box ها نمایانگر ماشین ها بوده و خطوط، نشانگر Packet های ارسالی هستند. توضیح کوتاهی از هر Packet را نیز روی همان خط مشاهده می کنید (به صورت انگلیسی)، Flag های TCP نیز در زیر خطوط مشخص شده اند.

همانطورکه در شکل زیر نمایش داده شده است، ماشین هدف با اشکال متفاوتی به ماشین زامبی پاسخ می دهد که این پاسخ بستگی به باز یا بسته بودن پورت مورد نظر دارد.



در قدم اول مهاجم یک پکت SYN/ACK برای زامبی/Z ارسال می کند که طبق اصول تعریف شده در TCP که در قبل به آن اشاره شد زامبی با یک پکت RST به مهاجم/A پاسخ می دهد. حتماً می پرسید که هدف از این کار چیست؟ به وسیله این عمل که به آن IPID Probe می گویند مهاجم عدد مربوط به IPID را از داخل Header پکت RST که دریافت می کند، برداشت می کند. به این دلیل پکت SYN/ACK ارسال شده است چون هدف بر قراری ارتباط با زامبی نبوده و هدف فقط گرفتن یک پکت از طرف زامبی بوده است. برای این که کار را سخت نکرده باشیم فرض می کنیم که این عدد (همان IPID) مساوی با 100 باشد.

در قدم بعدی مهاجم یک پکت با فلگ SYN برای ماشین هدف ارسال می کند با این تفاوت که در فیلد Source IP به جای IP خود (مهاجم) IP زامبی را قرار می دهد. این کار باعث می شود که ماشین هدف اینطور برداشت نماید که این پکت را ماشین زامبی ارسال کرده است و طبیعتاً جواب را نیز به زامبی خواهد داد. SYN Packet send to Target: Flag SYN, Des Port 80, Src IP Z

اگر پورت مورد نظر (مثلاً 80) در ماشین هدف باز باشد، ماشین هدف یک پکت SYN/ACK برای ماشین زامبی ارسال می کند (ماشین هدف این طور تصور می کند که پکت SYN را زامبی فرستاده است و به همین دلیل به آن جواب می دهد) و چون یک پکت ناخواسته SYN/ACK (در مفاهیم قبل توضیح داده شد) برای ماشین زامبی ارسال شده است، ماشین زامبی با یک RST به ماشین هدف پاسخ می دهد. نکته مهم اینجا است که با ارسال این پکت RST، عدد IPID که در مرحله اول مشخص شده بود یک عدد افزایش می یابد. حال اگر پورت مود نظر (مثلاً 80) بسته باشد، ماشین هدف با یک پکت RST به ماشین زامبی پاسخ خواهد داد که در ادامه چون یک پکت RST ناخواسته به دست زامبی رسیده است و طبق قوانین وی باید از آن صرف نظر کند (Ignore) پس عدد IPID ثابت مانده و تغییری نمی کند چون پکتی از سمت زامبی ارسال نشده است.

در مرحله آخر مهاجم یک بار دیگر عملیات IPID Probe را برای زامبی تکرار می کند (درست مثل مرحله یک). یعنی یک پکت SYN/ACK برای زامبی ارسال می کند که زامبی نیز در جواب یک پکت RST ارسال می کند. مهاجم بار دیگر عدد IPID را از داخل Header پکت IP دریافت و ذخیره می کند.

حال مهاجم باید به بررسی فرآیند ها و پاسخ های دریافت شده بپردازد. برای این کار از تغییرات ایجاد شده بر روی IPID استفاده می کند. به یاد دارید که در مرحله اول عدد IPID مربوط به زامبی کشف شد و در مرحله آخر نیز این کار تکرار شد. فرض کنید عددی که در مرحله اول بدست آمده بود به عنوان مثال 100 بوده است. اگر پورت مورد نظر روی ماشین هدف باز باشد باید یک پکت RST از سمت زامبی برای ماشین هدف (در جواب SYN/ACK) ارسال شده باشد که نتیجه آن اضافه شدن یک عدد به IPID است یعنی 101=1+100. در مرحله آخر نیز یک پکت RST دیگر برای مهاجم ارسال شد (در جواب IPID Probe) که نتیجه آن اضافه شدن یک عدد دیگر به IPID است یعنی 102=1+101. پس اگر مقدار IPID دو عدد اضافه شده باشد یعنی پورت مورد نظر روی ماشین هدف باز است.
حال اگر پورت مورد نظر بر روی ماشین هدف بسته باشد، هیچ پکتی از طرف زامبی برای ماشین هدف ارسال نمی شود (چون از RST صرف نظر می کند) و فقط یک پکت در مرحله آخر برای مهاجم ارسال می کند (در جواب IPID Probe) که نتیجه آن اضافه شدن فقط یک عدد به عدد IPID است یعنی 101=1+100. پس اگر مقدار IPID یک عدد افزایش یافته باشد پورت مورد نظر بر روی ماشین هدف بسته است.

مزایای پویش به طریق Idle

پویش در نهایت محرمانگی؛ اگر با دیگر شیوه های پورت اسکن کردن آشنایی داشته باشید حتماً روش ها و تکنیک هایی را می شناسید که درجه خطر شناسایی شما را پایین می آورند مثل Decoy کردن (به وسیله سوئیچ "-D" در nmap) که آدرس حقیقی شما را بین یک سری از آدرس های دروغی گم می کند که نتیجه آن سخت تر شدن شناسایی شما در مراجعه به log فایل ها است که باز هم آدرس حقیقی شما قابل کشف شدن است. و یا استفاده از روش های دیگر اسکن کردن مثل half-open (با استفاده از سوئیچ "-sS" در nmap) که چون در این ورش از پویش 3-way-handshak تکمیل نمی شود معمولاً در log فایل ها ثبت نمی شود و در واقع یک ارتباط باز و ناقص است که در این روش نیز آدرس حقیقی شما به ناچار برای هدف ارسال می شود و شما در ارتباط مستقیم با ماشین هدف هستید.
اما در Idle Scan شما به هیچ وجه تماس مستقیم با هدف خود نداشته و هویت واقعی خود را فاش نمی کنید! همین دلیل یکی از موارد محبوبیت این روش در بین افراد حرفه ای در کارهای بزرگ است!
و اما خصوصیت دوم ...
عبوز از سد فایروال ها؛ بدون شک شما نیز فیلتر کردن و پالایش نمودن تماس ها و ارتباطات بر اساس Source IP Address را یکی از مکانیسم های ایجاد امنیت برای ماشین های حساس خود می دانید. به عنوان مثال می توانید یک Database Server را فقط محدود به Web Server نمایید تا از پتانسیل های خطر ساز در ارتباط با دیگر ماشین ها کم کرده باشید (به این عمل ایجاد Trust Relationship می گوییم). حال در نظر بگیرید که با یک هدف در پشت چند Filtering Device رو به رو هستید. به وسیله Idle Scan و استفاده از یک Trust Relation به عنوان زامبی می توانید عملاً ابزار های مشکل ساز پیش روی خود را Bypass کنید!

Idle Scan با Nmap

در اولین مرحله از Idle Scan، شما باید یک ماشین مناسب برای زامبی شدن پیدا کنید. یک زامبی خوب نباید دارای ترافیک بالایی باشد و ضمناً قابلیت تشخیص IPID از طریق مقادیر قابل حدس را داشته باشد. سیستم های Print Servers، ماشین های ویندوزی، سیستم های لینوکسی قدیمی، FreeBSD و حتی Mac OS Box ها انتخاب های خوبی هستند ولی سیستم ها و ورژن های جدید لینوکس و solaris و OpenBSD قادر به زامبی شدن نمی باشند ولی هر یک از آنها را می توان به عنوان هدف مورد پویش قرار داد. یکی از قابلیت های جالب در nmap امکان بررسی ماشین مورد نظر به عنوان زامبی است که پس از آزمایش زامبی جواب را اعلام می کند.
انجام Idle Scan فوق العاده ساده می باشد، کافیست نام سیستم زامبی را به وسیله سوئیچ "-sI" در اختیار nmap قرار دهید:

```
# nmap -P0 -p- -sI Zombie.com www.Target.com

Starting nmap V. 3.10ALPHA3 ( www.insecure.org/nmap/ )
Idlescan using zombie Zombie.com (192.150.13.111:80); Class:
Incremental
Interesting ports on 208.225.90.120:
```

```
(The 65522 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
135/tcp    open        loc-srv
443/tcp    open        https
1027/tcp   open        IIS
1030/tcp   open        iad1
2306/tcp   open        unknown
5631/tcp   open        pcanywheredata
7937/tcp   open        unknown
7938/tcp   open        unknown
36890/tcp  open        unknown
```

Nmap run completed -- 1 IP address (1 host up) scanned in 2594.472 seconds

توجه داشته باشید که استفاد از سوئیچ "-P0" فوق العاده مهم است. همانطور که می دانید وظیفه این سوئیچ جلوگیری از ارسال پکت های ICMP به منظور Ping Sweep کردن، محاسبه Time و موارد دیگر است. در صورتیکه این سوئیچ را فراموش کنید تعدادی پکت ICMP از IP حقیقی شما برای هدف ارسال می شود که همین چند Packet می تواند در آینده ای نه چندان دور کار دست شما بدهد! در ضمن سوئیچ "-p-" به منظور اعمال پویش بر روی تمام 65535 پورت انتخاب شده است.
* توصیه شخصی بنده به شما دوست عزیز این است که هرگز (هرگز!) اقدام به Scan کردن بر روی یک رنج بزرگ از پورت ها را نکنید مخصوصاً در Idle Scan یا Half-Open Scan.

مقابله با حملات مبتنی بر IPID

به گفته Fyodor (برنامه نویسی Nmap) :"خوشبختانه راه های متعددی برای مبارزه و مقابله با حملات مبتنی بر IPID وجود دارد". در ادامه به مرور این راه ها خواهیم پرداخت.
مدیران شبکه:

- فایروال ها یا روتر های مرزی/Border Router های خود را به گونه ای پیکربندی نمایید تا جلوی ورود Packet هایی با Source IP Address جعلی و ساختگی را بگیرند. به عنوان مثال آدرس های منبعی با رنج های 10.X.X.X یا 192.168.X.X و یا IP مربوط به Localhost یعنی 127.X.X.X و غیره می توانند جزء اولین انتخاب ها برای drop شدن باشند!)
- Stateful Firewall ها نیز می توانند به شما در مقابل با این دسته از حملات کمک کنند. مطمئن شوید که Firewall شما از چنین خصوصیتی پشتیبانی می کند و این خصوصیت فعال شده است. (در مورد Stateful Firewall ها همین قدر بگوییم که یکی از مهمترین خصوصیات آنها نگهداری سوابق Packet های ارسال شده است که امکان مقابله با پکت های به ظاهر مجاز را می دهد. مصون بودن در مقابل ACK Scan یکی از خصوصیات این نوع فایروال ها است)
- نسبت به اجرای سیستم عامل هایی که در مقابل حملات IPID و زامبی شدن مصون شده اند اقدام نمایید. آخرین نسخه ها از لینوکس، سولاریس و OpenBSD انتخاب های خوبی برای این مورد هستند. این سیستم عامل ها در حال حاضر در مقابل زامبی شدن به وسیله Nmap مصون هستند.
- مکانیسم های مقابله با Packet های جعل شده/Spoofed Packets از قبیل پالایش خروجی/Egress Filtering را برای ترافیک خروجی از شبکه شما پیاده سازی و اعمال نمایید.

شرکت های خدمات دهنده اینترنتی/ISP:

- یکی از مهمترین مکانیسم های مقابله در ISP ها، اعمال پالایش خروجی/Egress Filtering در برابر پکت هایی با آدرس منبع جعل شده یا تقلبی بر روی ترافیک خرجی از شبکه شما است. این عمل

باعث می شود که از ایجاد و شکل گیری بسیاری از حملات (از طرف کاربران ISP ها) جلوگیری شود.

تولید کنندگان سیستم عامل:

- یکی از راه های خوب استفاده از شیوه ابداعی در OpenBSD یعنی رندوم (اتفاقی) کردن IPID ها است که امکان پیگیری آنها را غیر ممکن می سازد. البته روش های دیگری هم وجود دارد که هم اکنون توسط برخی سیستم عامل ها از قبیل خانواده لینوکس و سولاریس استفاده می شود که از صحبت در مورد آنها صرف نظر می کنیم.

برخی چالش ها در Idle Scan

کارائی/Performance: پویش برای یک پورت به صورتی که در شکل فوق نشان داده شد، جایی که هدف پویش کردن هزاران پورت باشد، سرعت کار را به طرز فوق العاده وحشتناکی کاهش می دهد. برای حل این مشکل می توانید از قابلیت ارسال پکت ها به صورت همزمان (موازی) در Nmap استفاده کنید که قابلیت ارسال 100 پکت به صورت همزمان را به شما می دهد اما در صورتیکه ترافیک شبکه مناسب نباشد تمام پورت ها بسته نشان داده خواهند شد چون IPID در سیستم زامبی افزایش نمی یابد.

* باز هم بنده parallel کردن را توصیه نمی کنم. حتی در موارد عادی اسکن کردن از قبیل TCP Connect Scan موازی کردن بیشتر از 6 پکت را جایز نمی دانم، چه برسد به 100 عدد پکت آن هم در Idle Scan !

میزبانان غیر Non-Idle hosts/Idle: همانطورکه متوجه شده اید اساس کار مدل پویش Idle بر شمارش تعداد پکت های ارسالی توسط سیستم زامبی است و به صورت پیش فرض، فرض بر این است که تمام پکت های ارسال شده از طرف زامبی برای سیستم هدف شما می باشد در صورتیکه این فقط در شرایط آزمایشگاهی امکان پذیر است و در عمل پکت های زیادی از طرف سیستم زامبی برای سیستم های مختلف ارسال می شود که نتیجه آن تغییر در عدد IPID است. Nmap با سعی های مجدد در وارسی و دیگر مکانیسم های خود بر این مشکلات فائق آمده است و سعی در بالا بردن دقت در نتیجه خروجی دارد ولی به هر شکل در شرایطی که با زامبی پر ترافیکی رو به رو هستید، بهترین راه افزایش اطمینان تکرار عملیات Scan کردن می باشد.

* مواظب تکرار دفعات پویش و همچنین رنج پورت های خود باشید! IDS ها از این نوع پویش به عنوان حمله معروف DoS Attack به نام SYN Flood برداشت می کنند.

پالایش خروجی/Egress Filtering: در مواقعی که ISP شما اقدام به Filtering بر روی ترافیک خروجی می کند و جلوی خروج پکت های Spoof شده را می گیرد، بهترین راه عوض کردن ISP است و یا استفاده از IP Tunneling که مخصوص افراد حرفه ای است. راه دیگر انتخاب ماشین زامبی از داخل شبکه ISP است (در صورت وجود و داشتن شرایط لازم) که امکان عبور پکت های جعل شده را افزایش می دهد.

* انتخاب ISP یکی از مهمترین قسمت ها در هر حمله یا تست نفوذ پذیری است که متاسفانه به آن توجه چندانی نمی شود. اکثراً مشاهده می کنم که فرد در حال Ping Sweep کردن است در حالی که ISP آن به طور کامل پکت های ICMP (و یا Type هایی از این پروتکل) را از بین می برد و یا اجازه عبور نمی دهد. در موارد دیگر هم همین رابطه صدق می کند، چطور TCP Traceroute می کنید در حالی که ISP شما از آن پشتیبانی نمی کند ؟! و یا چطور Idle Scan انجام می دهید در حالی که پکت های Spoof شده شما از شبکه ISP شما خارج نمی شوند؟! در انتخاب ISP خود دقت کنید و حتماً قبل از هر کاری آن را آزمایش کنید. توصیه من به شما استفاده از ISP های کوچک است. در ضمن سعی کنید برای هر فعالیتی یک یا چند حساب از ISP های مختلف داشته باشید.

زامبی نامناسب/Unsuitable Zombie: برخی از زامبی ها به دلیل شرایط خاص سیستم عامل خود (که در برابر زامبی شدن مصون شده اند) و یا به دلیل ترافیک بالا و نامناسب، امکان زامبی شدن را ندارند و یا دقت نتایج را فوق العاده کاهش می دهند. برای حل این مشکل بهترین راه رفتن به سراغ یک زامبی دیگر است.

کار عملی ...

بدون شک شما هم به این نتیجه رسیده اید که اکنون زمان کار عملی فرا رسیده است و برای شروع باید یک زامبی خوب پیدا کنیم.

حتماً می پرسید "حال برای پیدا کردن یک زامبی خوب از کجا شروع کنیم؟"

و من در جواب به شما می گویم که "متاسفانه در حال خواندن آخرین خطوط این مقاله هستید!! پیدا کردن زامبی باشد برای مباحث بعد ..."

امیدوارم که مطالبی که ارائه شد، ارزش خواندن و وقت گذاشتن برای آنها را داشته باشد. تمامی مطالبی که مطالعه نمودید بر گرفته از سایت http://www.insecure.com بود که با تغییراتی که در ترجمه آن داده شده است به شما ارائه گردید. توجه داشته باشید که مطلب فوق صرفاً یک ترجمه ساده نیست و تمام سعی بنده بر این بوده تا تجربیاتی که داشته ام و همچنین سوالات و مشکلاتی که معمولاً دانشجویان سر کلاس هایم با آن برخورد می کنند را در قالب این مقاله جای دهم.

موفق باشید،
محمودی مدیر تیم امنیتی SecureNET
Admin@IranSecureNET.com
HTTP://IranSecureNET.com