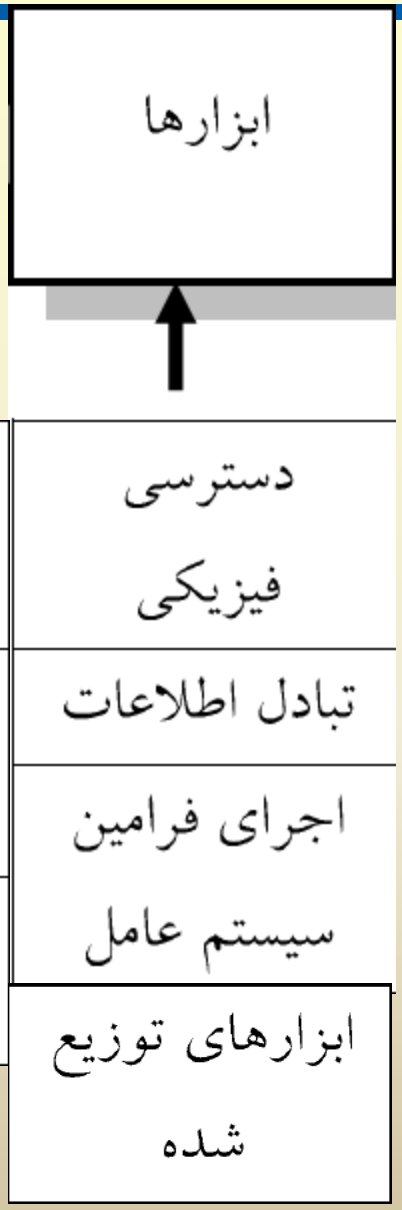
# مروری بر نفوذگری و امنیت در سیستم‌های کامپیوتری

# مدل کلی حمله

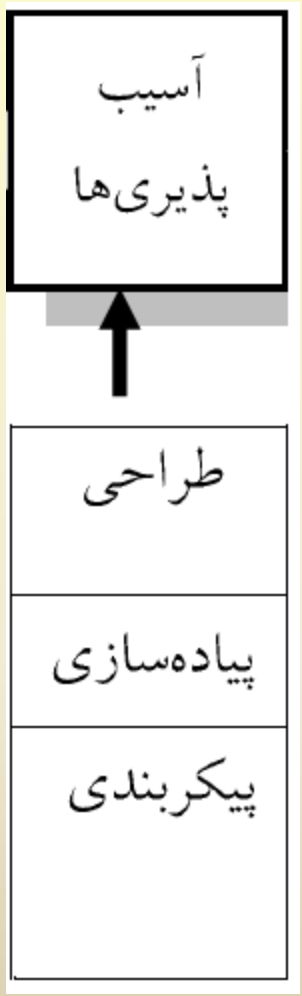
- نفوذگر با بکارگی‌ری ابزارهای حمله و ی‌ا سوء استفاده از آسی‌ب پذی‌ری های سی‌ستم هدف سعی در دراختی‌ار گرفتن سی‌ستم می کند

# رابطه بی‌ن اجزای ی‌ک تهاجم اطلاعاتی

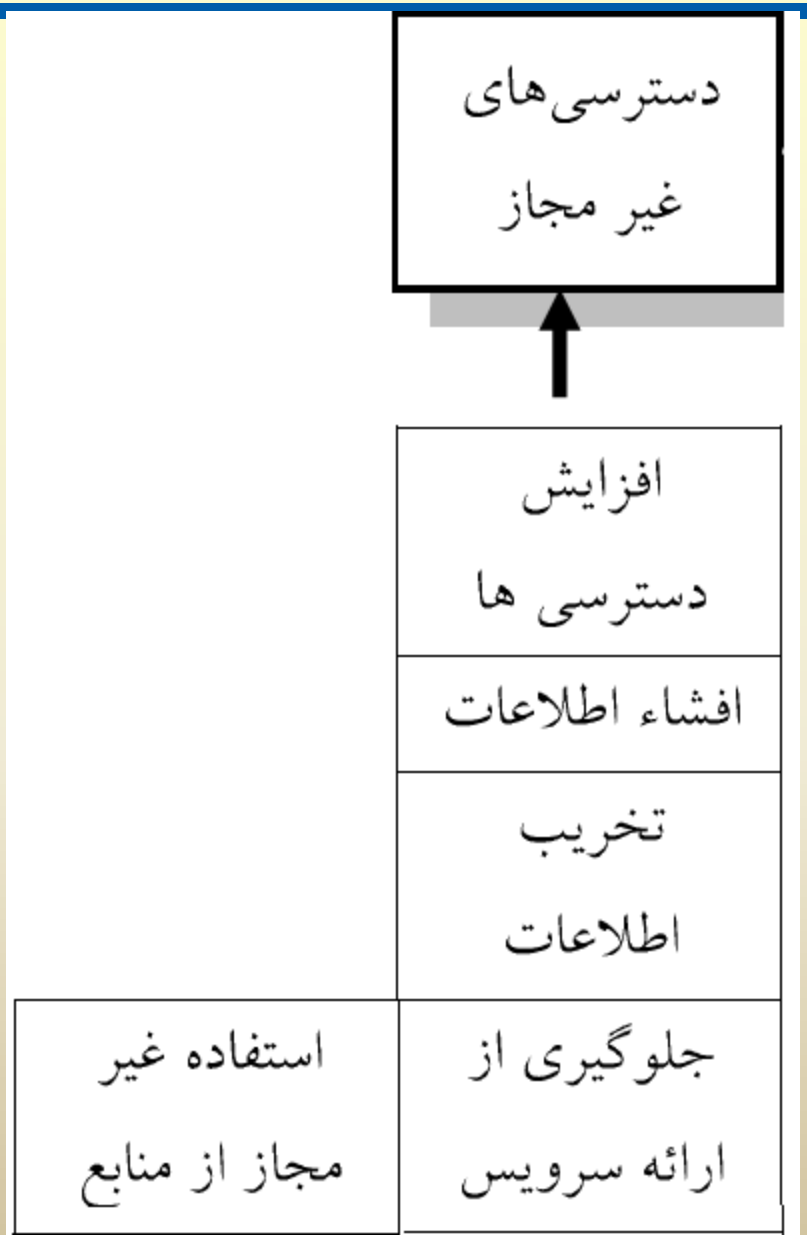



- تبادل اطلاعات: بهره برداری اطلاعات از نحوه ارتباط ی‌ک سی‌ستم با دنی‌ای خارج
- عوامل خودمختار: برنامه های‌ی که از طری‌ق شبکه به سی‌ستم وارد می شوند تا اقدامات تعی‌ی‌ن شده را انجام دهند. مانند Wormو Trojan horse ها
- ابزارهای توزی‌ع شده : استفاده نفوگر از تعداد زی‌ادی از سی‌ستم در سطح شبکه جهت اجرای ی‌ک حمله به ی‌ک ماشی‌ن. ای‌ن ابزارها ممکن است به صورت سلسه مراتبی استفاده شود (ابزارهای DDoS)

# رابطه بی‌ن اجزای ی‌ک تهاجم اطلاعاتی

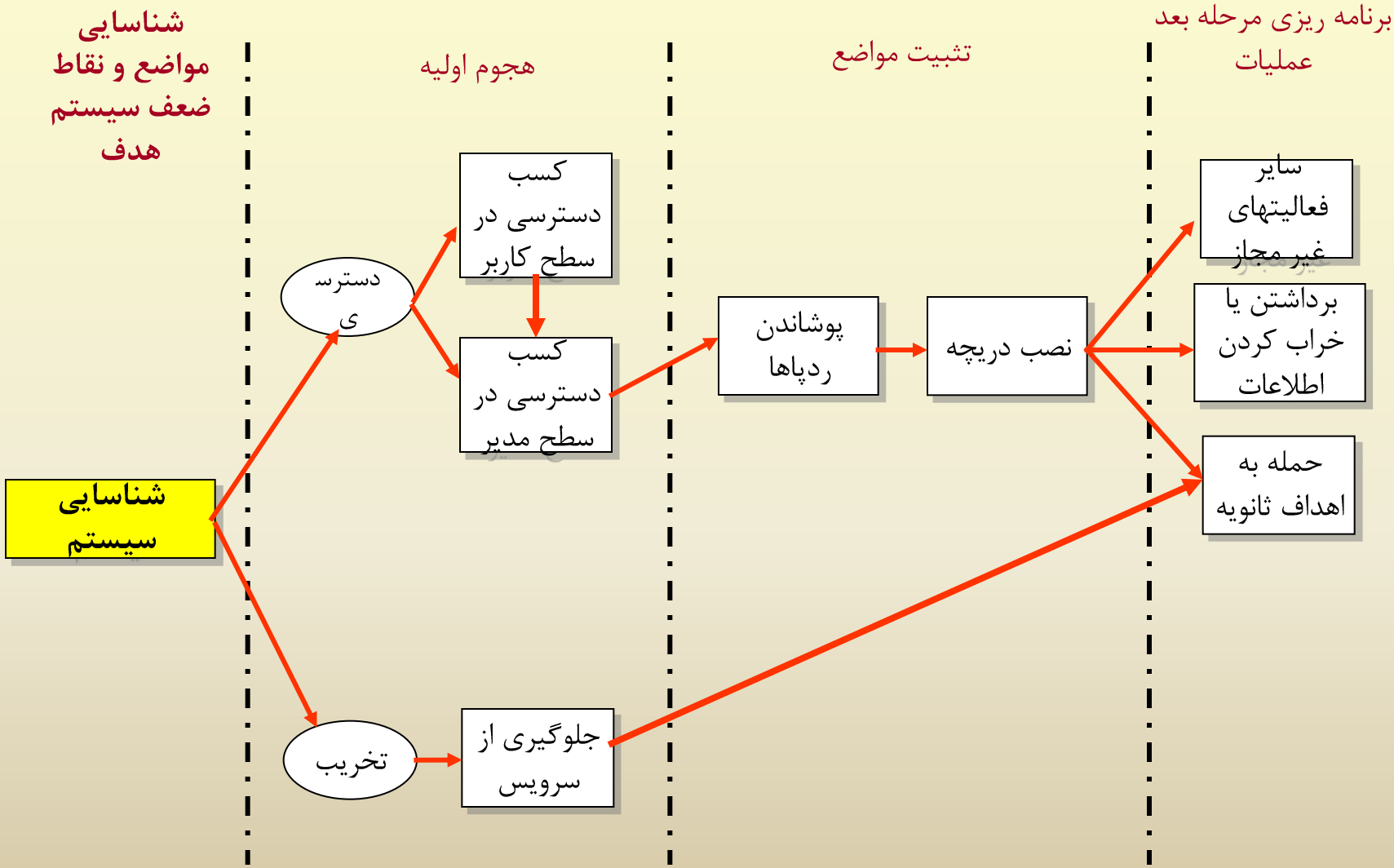
# رابطه بی‌ن اجزای ی‌ک تهاجم اطلاعاتی




# مراحل انجام تهاجم اطلاعاتی

- تعی‌ی‌ن اهداف
- فراهم نمودن ملزومات
- انجام عملی‌ات
- تحلی‌ل نتای‌ج بدست آمده

# روند نمای کلی انجام یک حملهٔ کامپیوتری



# شناسایی‌ی سی‌ستم هدف

- توپولوژی شبکه
- آدرس های IP سی‌ستم هدف
- مسی‌رهای مورد استفاده در دستی‌ابی به ای‌ن آدرس
- تعی‌ی‌ن پورت های باز
- تعی‌ی‌ن سروی‌س های موجود
- شناسایی‌ی آسی‌ب پذی‌ری سروی‌سها، سی‌ستم عامل، نرم افزارها و ... مورد استفاده در سی‌ستم هدف

ابزارهای در دسترس: whois، Nslookup، Ping، Traceroute، Telnet، Scanning

# هجوم اولی‌ه

- با استفاده از اطلاعات بدست آمده از مرحله قبول هجوم انجام می شود
- به دو منظور هجوم ممکن است انجام شود
  - هجوم به قصد تخری‌ب و از کار اندازی سی‌ستم
  - هجوم به قصد کسب دسترسی به سی‌ستم اطلاعاتی

# هجوم به قصد تخری‌ب و از کار اندازی سی‌ستم

- هدف ای‌جاد اختلال در شبکه و سی‌ستم ها
  - بکارگی‌ری ابزارهای مخربی مانند وی‌روسها ، کرم ها، اسب های تراوا و بمب های منطقی
- حذف و دستکاری داده های حساس  برای ای‌جاد اخلال
  - ارسال سی‌ل آسا Email
- حملات DoS و DDoS

# هجوم به قصد کسب دسترسی به سی‌ستم اطلاعاتی

- هدف دستی‌ابی به سی‌ستم و بهره برداری از آن
  - دستی‌ابی به کلمه های عبور
  - استفاده از آسی‌ب پذی‌ری سی‌ستم به منظور تعری‌ف دسترسی و ی‌ا افزای‌ش قابلی‌ت آن
    - حمله سری‌ز بافر

# تثبی‌ت مواضع

- هدف حفظ نتای‌ج بدست آمده در مرحله قبل
  - حفظ و استمرار دسترسی ها به سی‌ستم ی‌ا توانای‌ی های تخری‌بی بدست آمده
  - تقوی‌ت سطح دسترسی ها و توانای‌ی ها
  - مخفی ماندن و از بی‌ن رد پاهای انجام عملی‌ات

# برنامه ری‌زی برای مرحله بعدی عملی‌ات

- هدف تمکی‌ل اهداف حمله

  – انجام حملات پی‌چی‌ده ممکن است از چندی‌ن مرحله تشکی‌ل شده باشد

  – حمله به چندی‌ن می‌زبان آسی‌ب پذی‌ر برای انجام حمله واقعی

# روشهای شناسایی‌ی سی‌ستم هدف

- اشغال گردی(dumpster diving): در این روش جمع آوری اطلاعات از طریق جستجو در فلاپی ها ،CD ها و کاغذ های سازمان هدف است که ناآگاهانه دور ریخته شده اند.

- جستجو در وب: جمع آوری اطلاعاتی از قبیل سرویسهای شرکت ، آدرس پست الکترونیکی افراد شرکت و کاربران شبکه و ... با مراجعه سایت شرکت

# روشهای شناسایی‌ی سی‌ستم هدف

- ✓ انک اطلاعات whois: در اینترنت مراکزی با عنوان Whois وجود دارد که با دادن آدرس یک سایت می توان اطلاعاتی از جمله ip، domain، مسئول شبکه، آدرس پست الکترونیکی و ... را به دست آورد.از جمله این مراکز می توان به www.who.is اشاره کرد.

- ✓ استفاده از مو تورهای جستجو: جمع آوری اطلاعات اولیه از طریق موتورهای جستجو مثل Google،yahoo و...

# تشخیص مودمهای فعال و سرویس دهنده های مودم در شبکه

- نفوذ به شبکه از طریق مودم در دو مرحله صورت می گیرد :
  - ✓ War dialing: جستجو در بین مجموعه ی بسیار عظیمی از شماره های تلفن برای یافتن مودم های متصل و فعال در شبکه یا ماشین هدف.
  - ✓ Demon dialing: حمله بر علیه یک شماره تلفن (که اتصال آن به مودم محرز شده است) برای یافتن کلمه ی عبور و راهی جهت نفوذ به ماشینی که به آن مودم متصل است.
- بعد از شناسایی نوع مودم و نوع سرویس دهنده اگر سرویس دهنده نیاز به کلمه عبوری نداشته باشد کار تمام است ولی اگر نفوذگر با مودمی مواجه شود که برای ورود او کلمه ی عبور تقاضا کند اقدام بعدی او حدس زدن کلمه عبور و یا ورود به زور(brute force) به آن سیستم است.
- یک خط آزاد و متصل به مودم (در شبکه داخلی) تاثیر تمام ابزارهای پیشرفته ی امنیتی مثل دیوار آتش و IDS را از بین خواهد برد.

# تشخیص میزبان های هدف

- در این بخش فعال یا غیر فعال بودن یک میزبان که آدرس IP آن معتبر و مشخص است مورد نظر می باشد. این میزبان ها یا کامپیوترهای مستقر در ناحیه ی DMZ می باشد و یا خود دروازه ی شبکه.
- در صورتی که میزبان های داخلی شبکه دارای آدرس IP معتبر باشند آن ها نیز قابل شناسایی خواهند بود.
- روش های تشخیص میزبان های فعال در شبکه را می توان به دو گروه کلی تقسیم بندی کرد.

✓ بررسی پاسخ گویی میزبان ها به بسته های پروتکل های مختلف:

- با در نظر گرفتن ویژگی های پروتکل های معروفی نظیر TCP UDP، ICMP میزبان های فعال شبکه شناسایی می گردند.

✓ بررسی پاسخ های آنها به بسته های نامتعارف:

- مثلاً انتساب مقادیر ناصحیح به بعضی از فیلد های سرآیند و بررسی رفتار متقابل میزبان هدف.

# برخی روش های تشخیص میزبان های هدف

- Echo Port Method
  - ✓ یکی از سرویس های قدیمی TCP/IP می باشد. از آنجایی که این سرویس به پورت 7 گوش می دهد می توان از طریق فرمان های مربوطه یا استفاده از فرمان Telnet فعال یا غیر فعال بودن میزبان مورد نظر را بررسی نمود.
- UDP Method
  - ✓ میزبان به درخواست های ارتباطی که برای پورت های بسته ی UDP می آید پیام ICMP_PORT_UNREACH را ارسال می کند. اگر پیام فوق دریافت نشد نشان دهنده ی این است که یا توسط دیواره ی آتش فیلتر شده و یا پورت مورد نظر فعال می باشد
- TCP Flag method
  - ✓ در این حالت از بسته های TCP SYN، TCP ACK، TCP SYN ACK، TCP FIN و TCP FULL می توان بهره گرفت.

# برخی روش های تشخیص میزبان های هدف

- ICMP Method
  - ✓ در این حالت یک بسته یICMP echo request ارسال می شود ودر جواب بسته ی ICMP echo reply ارسال می گردد که بیانگر فعال بودن میزبان مورد نظر است.
- Timeout packet Fragmentation
  - ✓ یک بسته ی IP را با offset دلخواه، Fragment نموده و به پرچم MF موجود در سرآیند مقدار (1) را انتساب می دهیم. با ارسال این بسته به سمت میزبان هدف، آنرا در حالت انتظار برای دریافت بسته های بعدی قرار می دهیم. در این صورت اگر بسته های بعدی ارسال نگردد یک پیام ICMP از نوع time exceeded fragment برای نفوذگر ارسال می نماید که نشان دهنده ی فعال بودن آن است.
- Invalid Header Length
  - ✓ نفوذگر با ارسال یک بسته ی IP با طول نادرست (که آنرا در فیلد IHLسرایند قرار می دهد) به سمت میزبان هدف عملیات را شروع می کند. میزبان هدف با دریافت بسته ی IP ناصحیح از این طریق اقدام به ارسال یک بسته ی ICMP می نماید. بدین روش می توان تشخیص داد که میزبان هدف فعال می باشد.

# تهیه نقشه شبکه

- نقشه برداری از شبکه شامل تشخیص میزبان های فعال شبکه ی هدف و تعیین نحوه ی ارتباط بین هر یک می باشد. به عبارت دقیقتر پس از تشخیص میزبان های فعال یک شبکه لازم است هم بندی کل شبکه بررسی و ارزیابی شود.

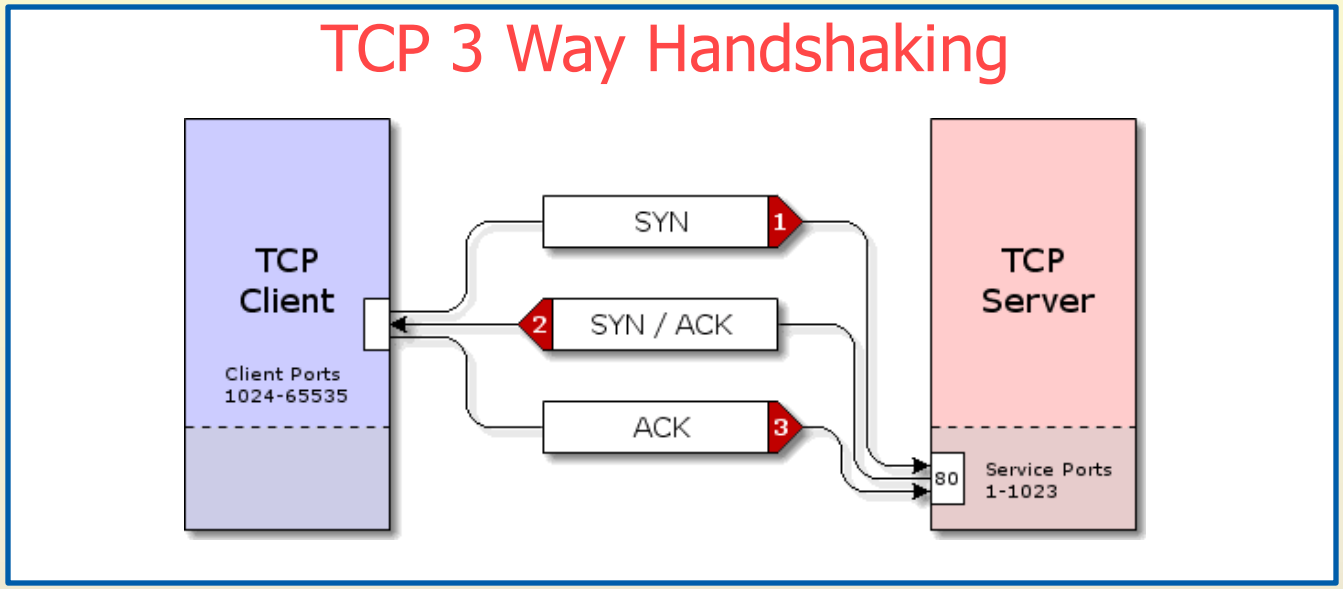
- نقشه برداری از یک شبکه برای پی ریزی یک حمله شامل مراحل زیر خواهد بود:
  - ✓ مشخص کردن ماشین های فعال
    - با روش های مختلفی که توضیح داده شد می توان میزبان های فعال موجود در DMZ را شناسایی نمود. در این حالات بهتر است تمامی آدرس های domain مربوطه بررسی شوند تا بتوان آدرس های IP میزبان های IDS وپروکسی را نیز بدست آورد.
  - ✓ تعقیب مسیر ها در شبکه
    - نفوذ گر پس از تشخیص ماشین های فعال سعی خواهد کرد تا توپولوژی کل شبکه را ارزیابی کند . مراحل مقدماتی این کار با عملیات Trace Route انجام می شود تا ترکیب مسیریاب ها و دروازه هایی که ستون فقرات آن شبکه را تشکیل داده اند مشخص شوند. این عملیات بر فیلد TTL از بسته ی IP متکی است.

- از ابزارهای معروف برای توپولوژی شبکه Cheops می باشد. این نرم افزار که تحت لینوکس اجرا می شود عمل استخراج توپولوژی شبکه را به صورت خودکار و دقیق انجام می دهد.

# تعیین پورت های باز بر روی یک ماشین

- پس از شناسایی ماشین های فعال شبکه و توپولوژی آن نفوذگر می خواهد بداند هر ماشین چه وظیفه ای بر عهده دارد و چه خدماتی ارائه می کند و هر کدام از این سرویس ها به چه نحو در اختیار کاربران قرار می گیرد .
  - ✓ پورت های باز و فعال TCP یا UDP روی هر ماشین سرویس هایی را که آن ماشین ارائه می دهد و پروسه هایی را که روی آن اجرا شده اند، مشخص می کنند.
- عمل پویش پورت توسط نرم افزارهایی که به نام Port Scanner مشهورند انجام می شود.

# برخی روش های تعیین پورت های باز بر روی یک ماشین



# برخی روش های تعیین پورت های باز بر روی یک ماشین

- TCP Connect Scanning
  - ✓ در این روش نفوذگر سعی می کند یک ارتباط سه مرحله ای و کامل TCP با پورت مورد نظر کامپیوتر هدف برقرار کند. در صورتیکه این ارتباط بر قرار شد نشان دهنده ی باز بودن پورت مورد نظر می باشد.
  - ✓ این روش زمان زیادی از نفوذگر می گیرد. از طرف دیگر اکثر سرویس دهنده ها به محض ایجاد ارتباط TCP آدرس و مشخصات طرف ارتباط را ثبت می نماید .
- TCP SYN Scanning
  - ✓ در این روش به جای ایجاد یک ارتباط کامل سه مرحله ای تنها اقدام به ارسال بسته ی SYN می کند. در صورتی که بسته ی SYN/ACK دریافت شد نشان دهنده ی باز بودن پورت مورد نظر می باشد. در این حالت نفوذگر در جواب بسته ی RST را ارسال نموده و بدین مرحله خاتمه می دهد.
  - ✓ اگرجواب دریافت نشد نمی توان مطمئن بود که پورت مورد نظر بسته است چرا که ممکن است از ناحیه ی دیواره آتش بسته شده باشد.
  - ✓ سرعت عملیات در این روش افزایش می یابد. ضمنا در این حالت اکثر سرویس دهنده ها از ثبت اطلاعات مربوطه خودداری می نمایند .

# برخی روش های تعیین پورت های باز بر روی یک ماشین

- TCP FIN Scan
  - ✓ از بسته ی TCP FIN در حالت معمول برای خاتمه دادن به یک ارتباط TCP استفاده می شود.
  - ✓ در صورتی که بدون ارتباط قبلی چنین بسته ای ارسال شود اگر پورت هدف باز باشد هیچ پاسخی به ارسال کننده نخواهد داد در غیر این صورت یک بسته ی TCP RST برای ارسال کننده می فرستد.
- Null Scan
  - ✓ در این مکانیزم برنامه ی پویشگر بدون آنکه ارتباط TCP با مقصد برقرار کرده باشد یک بسته ی TCP برای یک پورت خاص ارسال می کند. ویژگی این بسته آن است که هیچ یک از بیتهای SYN، FIN و ACK آن یک نیست.
  - ✓ این بسته طبق تعریف پروتکل TCP هیچ معنای خاصی ندارد و اگر پورت مربوطه باز باشد بسته حذف می شود و هیچ پاسخی برنخواهد گشت در حالیکه اگر پورت مربوطه بسته باشد در پاسخ بسته RST برمی گردد.

# برخی روش های تعیین پورت های باز بر روی یک ماشین

- Xmas Tree
  - در این روش نفوذگر بسته ای را به پورت هدف ارسال می کند که هر سه پرچم FIN، PUSH،URG آن با یک تنظیم شده است در صورتی که پورت هدف باز باشد این بسته حذف می شود. در غیر این صورت پاسخ TCP RST برای ارسال کننده فرستاده خواهد شد.
  - سه مکانیزم پویش اخیر که هر سه از نقض اصول پروتکل استفاده می کنند به جز در ماشین های با سیستم عامل ویندوز در سایر سیستم عامل ها به خوبی کار می کنند.
    - در ویندوز هر گاه بسته ای غیر متعارف دریافت شود چه پورت باز باشد و چه بسته در جواب RST باز خواهد گشت.

# برخی روش های تعیین پورت های باز بر روی یک ماشین

- TCP SYN ACK Scanning
  - ✓ نفوذگر به سمت پورت هدف بسته های TCP SYN ACK ارسال می کند. از آنجایی که در مراحل handshaking سه مرحله ای ارسال بسته ی SYN/ACK جزء مرحله ی دوم محسوب می شود بعضی از دیواره ی آتش آن را عبور داده و بدین ترتیب بسته به درون شبکه نفوذ می کند.
  - ✓ اگر پورت هدف باز باشد بسته ی TCP RST را در جواب باز می گرداند در غیر این صورت بسته ای در جواب ارسال نمی گردد.
  - ✓ دیواره آتش Stateful این روش پویش پورت را تشخیص داده و مانع اجرای آن خواهد شد. معمولا اگر بسته ای در جواب بازگردانده نشود نمی توان به صراحت از بسته یا باز بودن پورت اطمینان حاصل نمود چرا که ممکن است توسط دیواره آتش Statefull حذف شده باشد.
- پویش پورت های UDP
  - ✓ جهت پویش پورت های باز UDP می توان دنباله ای از بسته های UDP را به پورت های هدف ارسال نمود. اگر در پاسخ بسته ICMP port unreachable دریافت شد می توان اطمینان حاصل کرد که پورت مورد نظر بسته است در غیر این صورت نمی توان به صورت قطعی اظهار نظر داشت.
  - ✓ معمولا بهترین روش جهت پویش پورت ها ی UDP آن است که با توجه به نوع سرویس دهنده بسته های تقاضا به پورت هدف ارسال شود.

# برخی روش های تعیین پورت های باز بر روی یک ماشین

- **تنظیم زیرکانه شماره ی پورت مبدا برای پویش موفق**

- فیلد source port از هر بسته ی ارسال شده به سمت هدف پارامتر تعیین کننده ای برای فیلتر ها و دیواره آتش است. بعضی شماره پورت ها اگر در فیلد source port از یک بسته ی TCP تنظیم شود قادر به عبور از دیوارآتش خواهد بود. مثلا پورت 80و25، بسته ای که با این شماره ی پورت به سمت ماشین هدف ارسال شود شانس زیادی برای عبور از فیلترها و دیوارهای آتش دارد چرا که به نظر می رسد این بسته از طرف یک سرویس دهنده ی وب ارسال شده و ناشی از تقاضای قبلی آن ماشین بوده است، در اینجا فیلتر به ناچار بسته را عبور خواهد داد.

# تشخیص سیستم عامل میزبان های هدف

- یکی از روش های تشخیص سیستم عامل هدف جواب هایی است که سیستم های عامل مختلف در مواجهه با بسته های دریافتی نامتعارف TCP/IP به ارسال کننده می فرستند.به این روش اصطلاحا TCP Stack Fingerprinting گویند.

- موارد مشخص شده در مستندات RFC مربوط به TCP/IP جزئیات ارتباطات و اتفاقات مجاز را مشخص نموده ولی هیچ یک از RFC ها تعیین نکرده اند که وقتی اتفاق نامعمولی مثل ارسال یک بسته ی SYN/ACK به یک پورت بسته رخ می دهد سیستم باید چه پاسخی دهد.
  - ✓ نفوذگر با استفاده از ابزارهای مختلف بسته های گوناگونی با تنظیم پرچم های سرآیند آنها به سمت مقصد ارسال می کند. بدین ترتیب بر اساس جوابی که در هر مرحله سیستم به بسته های دریافتی می دهد می توا ن نوع آن را تشخیص داد.
  - ✓ ابزارهای معروفی نظیر NMAP در تشخیص سیستم عامل هدف استفاده می گردند.

# Operating System Detection

- Don’t Fragment Bit
  - Some OS use this bit to enhance performance
- TCP Initial Window
  - Some OS stack implementations have a unique initial window size on their returned packets
  - AIX returns Ox3F25, OpenBSD, FreeBSD use 0x402E

# Operating System Detection

- ICMP Error Message Quenching
  - RFC 1812 suggests limits on various error message rates. Only a few OS follow the RFC.
  - Send UDP packets to random, high, UDP port and count the number of unreachable messages received within a given amount of time.

# Operating System Detection

- ICMP Message Quoting
  - ICMP error messages should quote a small amount of info from the ICMP message that caused the error.
  - Example: Host unreachable
  - This is quoted when the PORT UNREACHABLE message is received in the IP Header + 8 bytes.
  - Solaris and Linux provide more info than is needed

# Vulnerabilityچیست؟

- Vulnerability یا به صورت مختصر Vul را حفره، سوراخ امنیتی و یا آسیب پذیری می‌گوییم.
- سایت‌هایی هستند که کارشان به‌طور عمده گزارش جدیدترین Vul های کشف شده است مثل securitytracker.com یا securityfocus.com و...
- کشف Vul معمولا فقط در حد یک گزارش می‌ماند تا اینکه روشی برای exploit کردن آن Vul درست شود. پس Vul جنبه تئوری قضیه است و exploit قسمت عملی آن!

# پویش نقاط آسیب پذیر

- معمولا نفوذگر از نرم افزارهایی برای پویش نقاط آسیب پذیر استفاده می کند که یک پایگاه داده از نقاط ضعف  بنیادی سیستم های عامل و نرم افزارهای معروف در اختیار دارند و چون در مرحله ی قبلی نوع سیستم عامل مشخص گردیده است، ابتدا با استفاده از این پایگاه داده به دنبال اشکالات و نقاط ضعف بنیادی سیستم می گردد.
- ابزارهای پویش نقاط آسیب پذیر، به دنبال کشف موارد زیر روی ماشین هدف می گردند:
  - ✓ ضعف در پیکربندی پیش فرض یک سرویس دهنده
  - ✓ ضعف در پیکربندی سرویس دهنده
  - ✓ نقاط آسیب پذیر شناخته شده

# اجزاء اساسی ابزارهای پویش آسیب پذیری

- پایگاه اطلاعاتی از نقاط ضعف و آسیب پذیری سیستم ها
  - ✓ در این پایگاه اطلاعاتی فهرستی از نقاط ضعف سیستم های مختلف ذخیره شده است و نحوه ی آزمایش این نقاط ضعف نیز تعیین گردیده است.
- واسط کاربر
  - ✓ این قسمت از نرم افزار،برای دریافت فرامین کاربر از طریق یک واسط گرافیکی است. از طریق این واسط ، نفوذگر شبکه هدف و نوع آزمایشی را که باید انجام شود مشخص می نماید.
- موتور پویش
  - ✓ موتور پویش بر اساس بانک اطلاعاتی نقاط ضعف و همچنین تنظیماتی که نفوذگر انجام داده است، بسته های خاص و مشخصی را تولید و به سمت ماشین هدف ارسال می نماید تا بتواند تعیین کند که آیا نقطه ی ضعف مورد آزمایش واقعا وجود دارد یا خیر؟

# اجزاء اساسی ابزارهای پویش آسیب پذیری

- پایگاه اطلاعاتی از نقاط ضعف سیستم که در پویش های اخیر کشف شده است
  - ✓ این قسمت در حقیقت ذخیره کننده ی نتایج هر مرحله از پویش سیستم و نقاط ضعف کشف شده می باشد. نتایج حاصل ازاین مرحله می تواند مجددا در خدمت موتور پویش برای بررسی های جدید قرار بگیرد.
- بخش گزارشگیری و ثبت نتایج پویش
  - ✓ این قسمت از نرم افزار گزارش های نهایی از فهرست بررسی های انجام شده و نتیجه ی پویش ماشین هدف را ارائه می دهد.