مروري بر نفوذگري و امنيت در سيستم‌هاي كامپيوتري

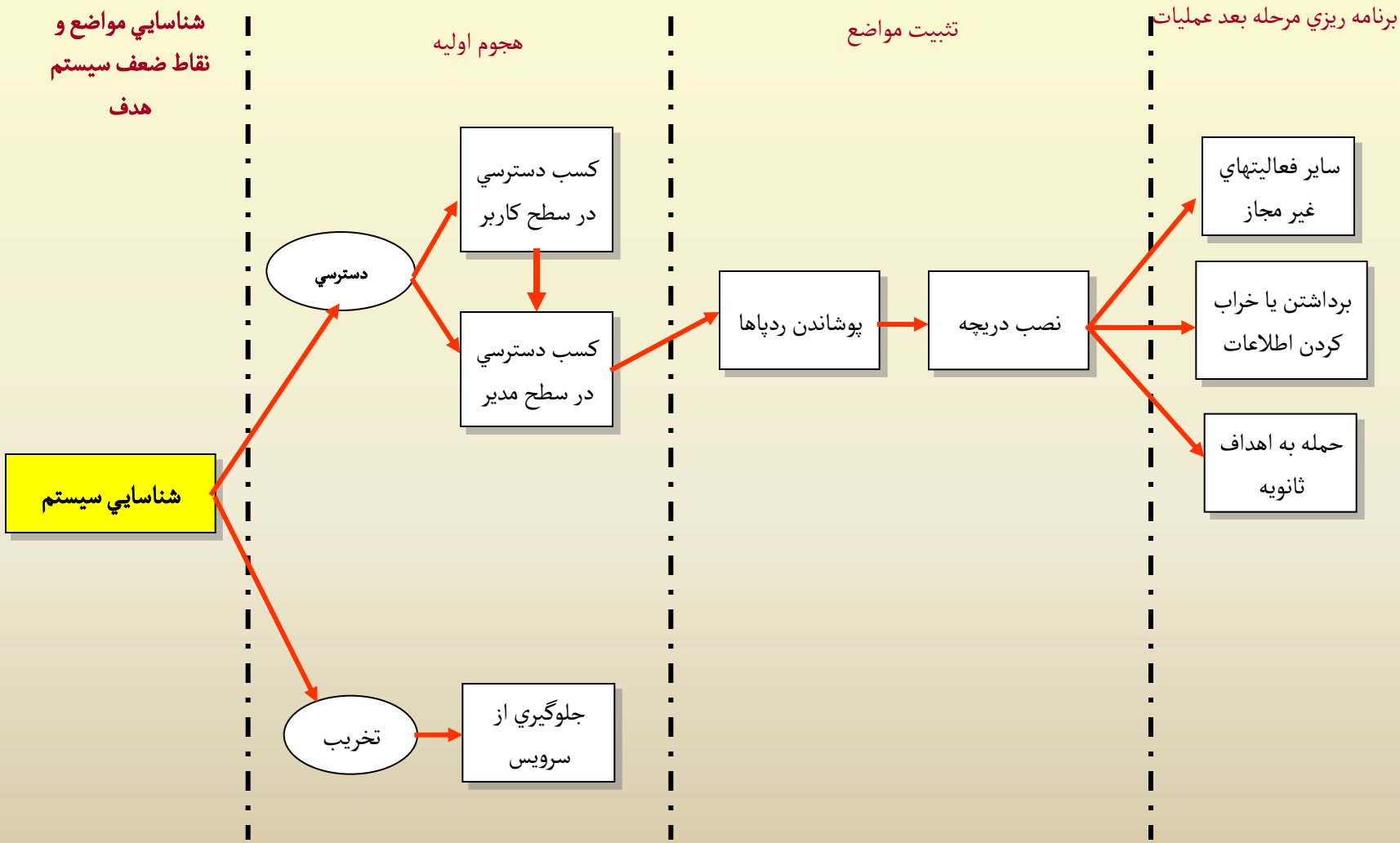
مدل كلي حمله

- نفوذگر با بكارگيري ابزارهاي حمله و يا سوء استفاده از آسيب پذيري هاي سيستم هدف سعي در دراختيار گرفتن سيستم مي كند

مراحل انجام تهاجم اطلاعاتي

- تعيين اهداف
- فراهم نمودن ملزومات
- انجام عمليات
- تحليل نتايج بدست آمده

روند نماي كلي انجام يک حملة كامپيوتري

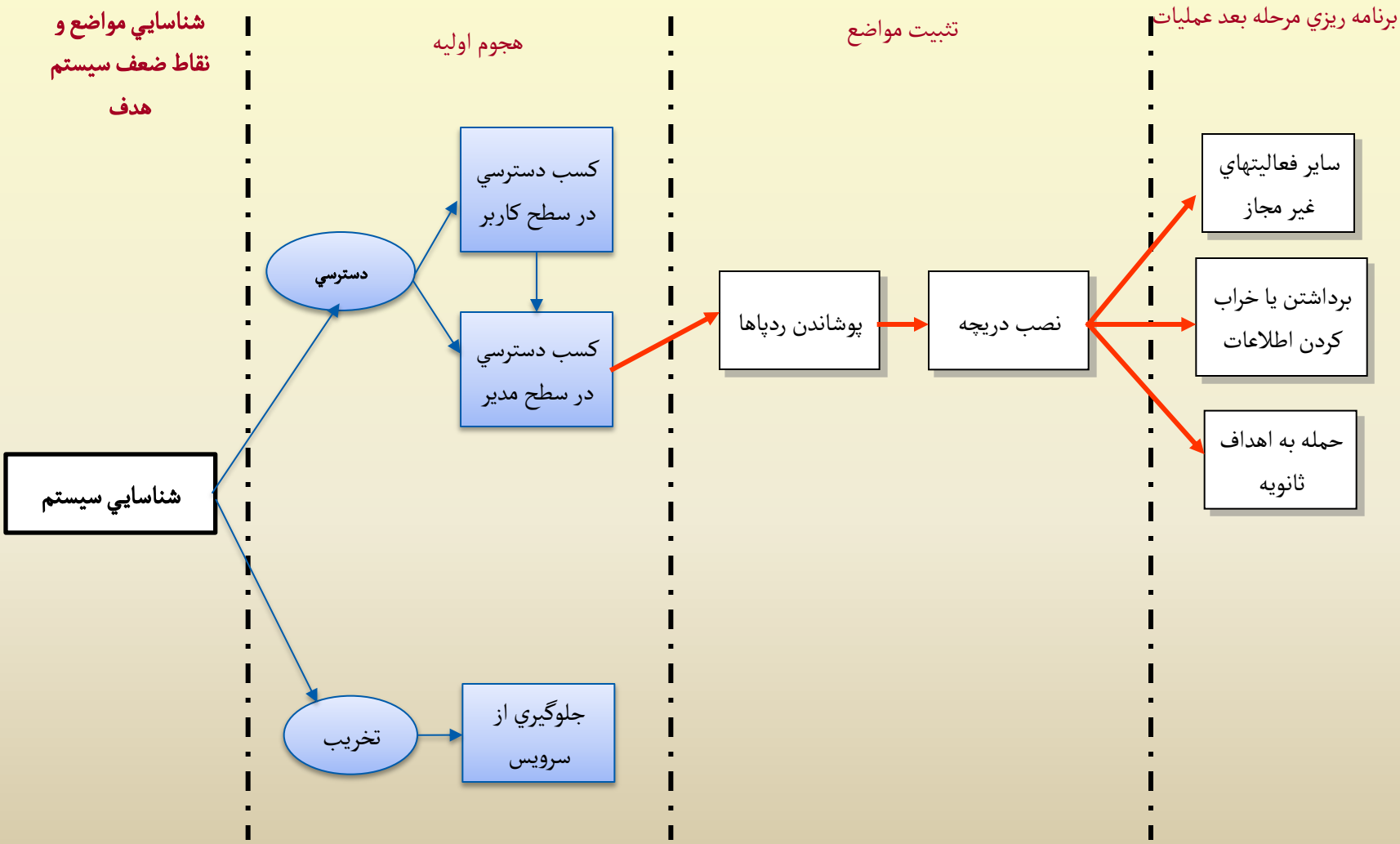


شناسايي سيستم هدف

- توپولوژي شبكه
- آدرس هاي IP سيستم هدف
- مسيرهاي مورد استفاده در دستيابي به اين آدرس
- تعيين پورت هاي باز
- تعيين سرويس هاي موجود
- شناسايي آسيب پذيري سرويسها ، سيستم عامل ، نرم افزارها و ... مورد استفاده در سيستم هدف

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

روند نماي كلي انجام يک حملة كامپيوتري



هجوم اوليه

- با استفاده از اطلاعات بدست آمده از مرحله قبل هجوم انجام مي شود
- به دو منظور هجوم ممكن است انجام شود
  - هجوم به قصد تخريب و از كار اندازي سيستم
  - هجوم به قصد كسب دسترسي به سيستم اطلاعاتي

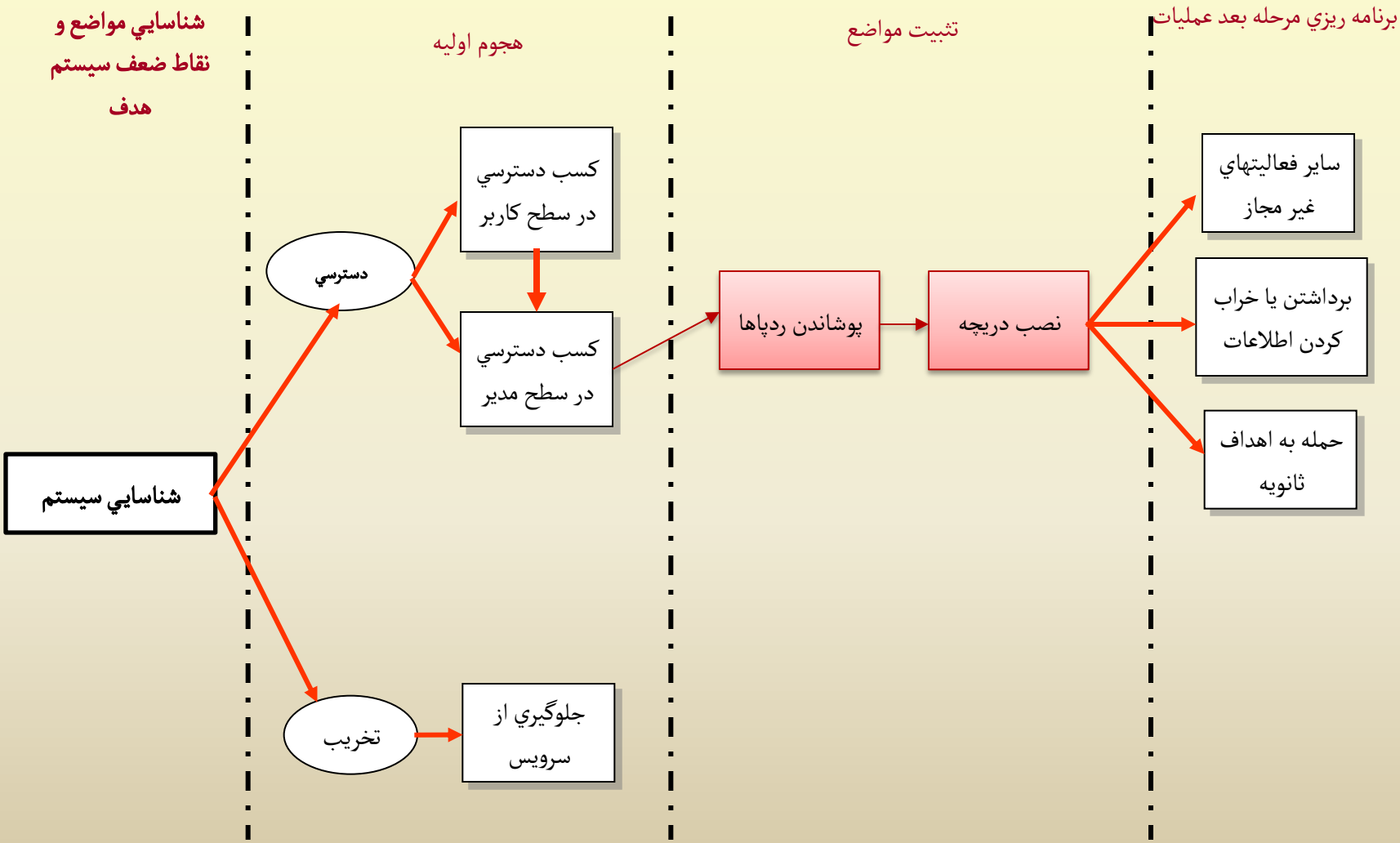
هجوم به قصد تخريب و از كار اندازي سيستم

- ايجاد اختلال در شبكه و سيستم ها
  - بكارگيري ابزارهاي مخربي مانند ويروسها ، كرم ها ، اسب هاي تراوا و بمب هاي منطقي
- حذف و دستكاري داده هاي حساس براي ايجاد اخلال
  - ارسال سيل آسا Email
- حملات DoS و DDoS

هجوم به قصد كسب دسترسي به سيستم اطلاعاتي

- هدف دستيابي به سيستم و بهره برداري از آن
  - دستيابي به كلمه هاي عبور
  - استفاده از آسيب پذيري سيستم به منظور تعريف دسترسي و يا افزايش قابليت آن
    - حمله سريز بافر

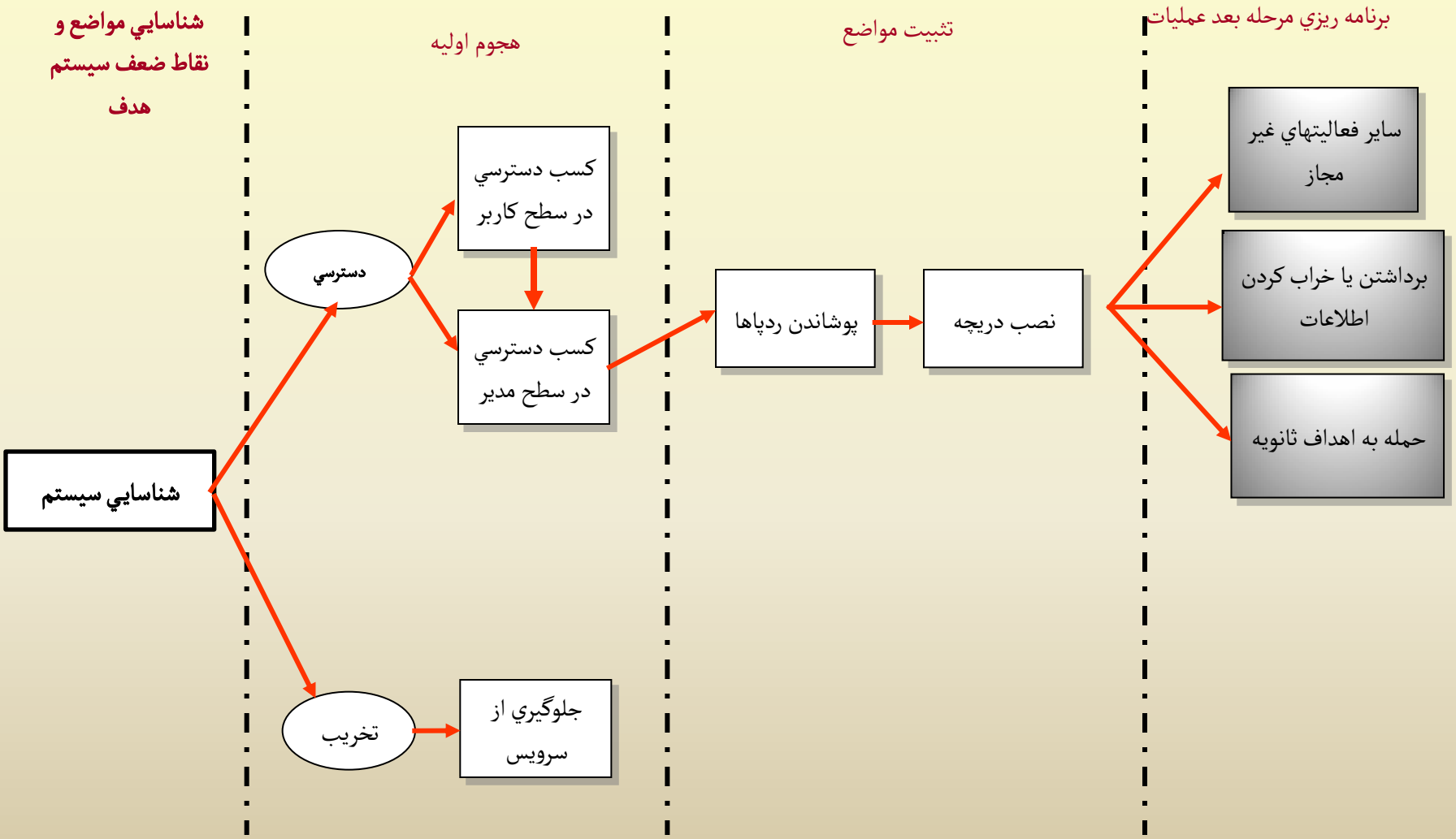
روند نماي كلي انجام يک حملة كامپيوتري



تثبيت مواضع

- هدف حفظ نتايج بدست آمده در مرحله قبل
  - حفظ و استمرار دسترسي ها به سيستم يا توانايي هاي تخريبي بدست آمده
  - تقويت سطح دسترسي ها و توانايي ها
  - مخفي ماندن و از بين رد پاهاي انجام عمليات

روند نماي كلي انجام يک حملة كامپيوتري



برنامه ريزي براي مرحله بعدي عمليات

- هدف تكميل اهداف حمله
  - انجام حملات پيچيده ممكن است از چندين مرحله تشكيل شده باشد
  - حمله به چندين ميزبان آسيب پذير براي انجام حمله واقعي

روشهاي شناسايي سيستم هدف

- ✓ اشغال گردي(dumpster diving): در اين روش جمع آوري اطلاعات از طريق جستجو در فلاپي ها ،CD ها و كاغذ هاي سازمان هدف است كه ناآگاهانه دور ريخته شده اند.

- ✓ جستجو در وب: جمع آوري اطلاعاتي از قبيل سرويسهاي شركت ، آدرس پست الكترونيكي افراد شركت و كاربران شبكه و ... با مراجعه سايت شركت

روشهاي شناسايي سيستم هدف

- ✓ بانک اطلاعات whois: در اينترنت مراکزي با عنوان Whois وجود دارد که با دادن آدرس يک سايت مي توان اطلاعاتي از جمله ip ، domain ، مسئول شبکه ، آدرس پست الکترونيکي و ... را به دست آورد.از جمله اين مراکز مي توان به www.who.is اشاره کرد.

- ✓ استفاده از مو تورهاي جستجو: جمع آوري اطلاعات اوليه از طريق موتورهاي جستجو مثل Google،yahoo و...

تشخيص مودمهاي فعال و سرويس دهنده هاي مودم در شبكه

- نفوذ به شبكه از طريق مودم در دو مرحله صورت مي گيرد :
  - ✓ War dialing: جستجو در بين مجموعه ي بسيار عظيمي از شماره هاي تلفن براي يافتن مودم هاي متصل و فعال در شبكه يا ماشين هدف.
  - ✓ Demon dialing: حمله بر عليه يک شماره تلفن (كه اتصال آن به مودم محرز شده است) براي يافتن كلمه ي عبور و راهي جهت نفوذ به ماشيني كه به آن مودم متصل است.
- يک خط آزاد و متصل به مودم (در شبكه داخلي) تاثير تمام ابزارهاي پيشرفته ي امنيتي مثل ديوار آتش و IDS را از بين خواهد برد.

تشخيص ميزبان هاي هدف

- در اين بخش فعال يا غير فعال بودن يک ميزبان که آدرس IP آن معتبر و مشخص است مورد نظر مي باشد. اين ميزبان ها يا کامپيوترهاي مستقر در ناحيه ي DMZ مي باشد و يا خود دروازه ي شبکه.
- در صورتي که ميزبان هاي داخلي شبکه داراي آدرس IP معتبر باشند آن ها نيز قابل شناسايي خواهند بود.
- روش هاي تشخيص ميزبان هاي فعال در شبکه را مي توان به دو گروه کلي تقسيم بندي کرد.

✓ بررسي پاسخ گويي ميزبان ها به بسته هاي پروتکل هاي مختلف:

- با در نظر گرفتن ويژگي هاي پروتکل هاي معروفي نظير ICMP ، UDP TCP ميزبان هاي فعال شبکه شناسايي مي گردند.

✓ بررسي پاسخ هاي آنها به بسته هاي نامتعارف:

- مثلاً انتساب مقادير ناصحيح به بعضي از فيلد هاي سرآيند و بررسي رفتار متقابل ميزبان هدف.

برخي روش هاي تشخيص ميزبان هاي هدف

- Echo Port Method
  - ✓ يكي از سرويس هاي قديمي TCP/IP مي باشد. از آنجايي كه اين سرويس به پورت ۷ گوش مي دهد مي توان از طريق فرمان هاي مربوطه يا استفاده از فرمان Telnet فعال يا غير فعال بودن ميزبان مورد نظر را بررسي نمود.
- UDP Method
  - ✓ ميزبان به درخواست هاي ارتباطي كه براي پورت هاي بسته ي UDP مي آيد پيام ICMP_PORT_UNREACH را ارسال مي كند. اگر پيام فوق دريافت نشد نشان دهنده ي اين است كه يا توسط ديواره ي آتش فيلتر شده و يا پورت مورد نظر فعال مي باشد
- TCP Flag method
  - ✓ در اين حالت از بسته هاي TCP SYN، TCP ACK، TCP SYN ACK، TCP FIN و TCP FULL مي توان بهره گرفت.

برخي روش هاي تشخيص ميزبان هاي هدف

- ICMP Method
  - ✓ در اين حالت يک بسته ي ICMP echo request ارسال مي شود ودر جواب بسته ي ICMP echo reply ارسال مي گردد که بيانگر فعال بودن ميزبان مورد نظر است.
- Timeout packet Fragmentation
  - ✓ يک بسته ي IP را با offset دلخواه ، Fragment نموده و به پرچم MF موجود در سرآيند مقدار (۱) را انتساب مي دهيم. با ارسال اين بسته به سمت ميزبان هدف ، آنرا در حالت انتظار براي دريافت بسته هاي بعدي قرار مي دهيم. در اين صورت اگر بسته هاي بعدي ارسال نگردد يک پيام ICMP از نوع time exceeded fragment براي نفوذگر ارسال مي نمايد که نشان دهنده ي فعال بودن آن است.
- Invalid Header Length
  - ✓ نفوذگر با ارسال يک بسته ي IP با طول نادرست (که آنرا در فيلد IHLسرايند قرار مي دهد) به سمت ميزبان هدف عمليات را شروع مي کند. ميزبان هدف با دريافت بسته ي IP ناصحيح از اين طريق اقدام به ارسال يک بسته ي ICMP مي نمايد. بدين روش مي توان تشخيص داد که ميزبان هدف فعال مي باشد.

تهيه نقشه شبكه

- نقشه برداري از شبكه شامل تشخيص ميزبان هاي فعال شبكه ي هدف و تعيين نحوه ي ارتباط بين هر يک مي باشد. به عبارت دقيقتر پس از تشخيص ميزبان هاي فعال يک شبكه لازم است هم بندي كل شبكه بررسي و ارزيابي شود.

- نقشه برداري از يک شبكه براي پي ريزي يک حمله شامل مراحل زير خواهد بود:

✓ مشخص كردن ماشين هاي فعال

- با روش هاي مختلفي كه توضيح داده شد مي توان ميزبان هاي فعال موجود در DMZ را شناسايي نمود. در اين حالات بهتر است تمامي آدرس هاي domain مربوطه بررسي شوند تا بتوان آدرس هاي IP ميزبان هاي IDS وپروكسي را نيز بدست آورد.

✓ تعقيب مسير ها در شبكه

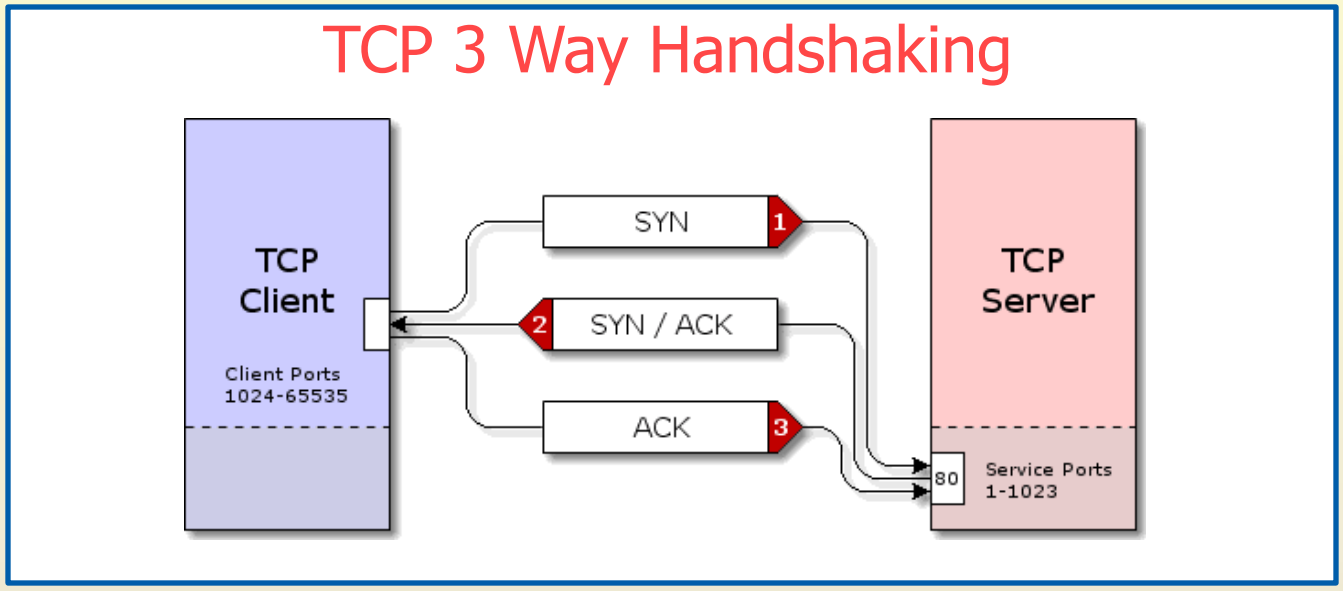
- نفوذ گر پس از تشخيص ماشين هاي فعال سعي خواهد كرد تا توپولوژي كل شبكه را ارزيابي كند . مراحل مقدماتي اين كار با عمليات Trace Route انجام مي شود تا تركيب مسيرياب ها و دروازه هايي كه ستون فقرات آن شبكه را تشكيل داده اند مشخص شوند. اين عمليات بر فيلد TTL از بسته ي IP متكي است.

- از ابزارهاي معروف براي توپولوژي شبكه Cheops مي باشد. اين نرم افزار كه تحت لينوكس اجرا مي شود عمل استخراج توپولوژي شبكه را به صورت خودكار و دقيق انجام مي دهد.

تعيين پورت هاي باز بر روي يک ماشين

- پس از شناسايي ماشين هاي فعال شبکه و توپولوژي آن نفوذگر مي خواهد بداند هر ماشين چه وظيفه اي بر عهده دارد و چه خدماتي ارائه مي کند و هر کدام از اين سرويس ها به چه نحو در اختيار کاربران قرار مي گيرد .
  - ✓ پورت هاي باز و فعال TCP يا UDP روي هر ماشين سرويس هايي را که آن ماشين ارائه مي دهد و پروسه هايي را که روي آن اجرا شده اند ، مشخص مي کنند.
- عمل پويش پورت توسط نرم افزارهايي که به نام Port Scanner مشهورند انجام مي شود.

برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين



برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين

- TCP Connect Scanning
  - ✓ در اين روش نفوذگر سعي مي کند يک ارتباط سه مرحله اي و کامل TCP با پورت مورد نظر کامپيوتر هدف برقرار کند. در صورتيکه اين ارتباط بر قرار شد نشان دهنده ي باز بودن پورت مورد نظر مي باشد.
  - ✓ اين روش زمان زيادي از نفوذگر مي گيرد. از طرف ديگر اکثر سرويس دهنده ها به محض ايجاد ارتباط TCP آدرس و مشخصات طرف ارتباط را ثبت مي نمايد .
- TCP SYN Scanning
  - ✓ در اين روش به جاي ايجاد يک ارتباط کامل سه مرحله اي تنها اقدام به ارسال بسته ي SYN مي کند. در صورتي که بسته ي SYN/ACK دريافت شد نشان دهنده ي باز بودن پورت مورد نظر مي باشد. در اين حالت نفوذگر در جواب بسته ي RST را ارسال نموده و بدين مرحله خاتمه مي دهد.
  - ✓ اگرجواب دريافت نشد نمي توان مطمئن بود که پورت مورد نظر بسته است چرا که ممکن است از ناحيه ي ديواره آتش بسته شده باشد.
  - ✓ سرعت عمليات در اين روش افزايش مي يابد. ضمنا در اين حالت اکثر سرويس دهنده ها از ثبت اطلاعات مربوطه خودداري مي نمايند .

برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين

- TCP FIN Scan
  - ✓ از بسته ي TCP FIN در حالت معمول براي خاتمه دادن به يک ارتباط TCP استفاده مي شود.
  - ✓ در صورتي که بدون ارتباط قبلي چنين بسته اي ارسال شود اگر پورت هدف باز باشد هيچ پاسخي به ارسال کننده نخواهد داد در غير اين صورت يک بسته ي TCP RST براي ارسال کننده مي فرستد.
- Null Scan
  - ✓ در اين مکانيزم برنامه ي پويشگر بدون آنکه ارتباط TCP با مقصد برقرار کرده باشد يک بسته ي TCP براي يک پورت خاص ارسال مي کند. ويژگي اين بسته آن است که هيچ يک از بيتهاي SYN ، FIN و ACK آن يک نيست.
  - ✓ اين بسته طبق تعريف پروتکل TCP هيچ معناي خاصي ندارد و اگر پورت مربوطه باز باشد بسته حذف مي شود و هيچ پاسخي برنخواهد گشت در حاليکه اگر پورت مربوطه بسته باشد در پاسخ بسته RST برمي گردد.

برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين

- Xmas Tree
  - در اين روش نفوذگر بسته اي را به پورت هدف ارسال مي کند که هر سه پرچم FIN، URG، PUSH آن با يک تنظيم شده است در صورتي که پورت هدف باز باشد اين بسته حذف مي شود. در غير اين صورت پاسخ TCP براي ارسال کننده فرستاده خواهد شد. RST

- سه مکانيزم پويش اخير که هر سه از نقض اصول پروتکل استفاده مي کنند به جز در ماشين هاي با سيستم عامل ويندوز در ساير سيستم عامل ها به خوبي کار مي کنند.
  - در ويندوز هر گاه بسته اي غير متعارف دريافت شود چه پورت باز باشد و چه بسته در جواب RST باز خواهد گشت.

برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين

- TCP SYN ACK Scanning
  - ✓ نفوذگر به سمت پورت هدف بسته هاي TCP SYN ACK ارسال مي کند. از آنجايي که در مراحل handshaking سه مرحله اي ارسال بسته ي SYN/ACK جزء مرحله ي دوم محسوب مي شود بعضي از ديواره ي آتش آن را عبور داده و بدين ترتيب بسته به درون شبکه نفوذ مي کند.
  - ✓ اگر پورت هدف باز باشد بسته ي TCP RST را در جواب باز مي گرداند در غير اين صورت بسته اي در جواب ارسال نمي گردد.
  - ✓ ديواره آتش Stateful اين روش پويش پورت را تشخيص داده و مانع اجراي آن خواهد شد. معمولا اگر بسته اي در جواب بازگردانده نشود نمي توان به صراحت از بسته يا باز بودن پورت اطمينان حاصل نمود چرا که ممکن است توسط ديواره آتش Statefull حذف شده باشد.
- پويش پورت هاي UDP
  - ✓ جهت پويش پورت هاي باز UDP مي توان دنباله اي از بسته هاي UDP را به پورت هاي هدف ارسال نمود. اگر در پاسخ بسته ICMP port unreachable دريافت شد مي توان اطمينان حاصل کرد که پورت مورد نظر بسته است در غير اين صورت نمي توان به صورت قطعي اظهار نظر داشت.
  - ✓ معمولا بهترين روش جهت پويش پورت ها ي UDP آن است که با توجه به نوع سرويس دهنده بسته هاي تقاضا به پورت هدف ارسال شود.

برخي روش هاي تعيين پورت هاي باز بر روي يک ماشين

- **تنظيم زيرکانه شماره ي پورت مبدا براي پويش موفق**

- فيلد source port از هر بسته ي ارسال شده به سمت هدف پارامتر تعيين کننده اي براي فيلتر ها و ديواره آتش است. بعضي شماره پورت ها اگر در فيلد source port از يک بسته ي TCP تنظيم شود قادر به عبور از ديوارآتش خواهد بود. مثلا پورت ۸۰و۲۵ ، بسته اي که با اين شماره ي پورت به سمت ماشين هدف ارسال شود شانس زيادي براي عبور از فيلترها و ديوارهاي آتش دارد چرا که به نظر مي رسد اين بسته از طرف يک سرويس دهنده ي وب ارسال شده و ناشي از تقاضاي قبلي آن ماشين بوده است ، در اينجا فيلتر به ناچار بسته را عبور خواهد داد.

تشخيص سيستم عامل ميزبان هاي هدف

- يكي از روش هاي تشخيص سيستم عامل هدف جواب هايي است كه سيستم هاي عامل مختلف در مواجهه با بسته هاي دريافتي نامتعارف TCP/IP به ارسال كننده مي فرستند.به اين روش اصطلاحا TCP Stack Fingerprinting گويند.

- موارد مشخص شده در مستندات RFC مربوط به TCP/IP جزئيات ارتباطات و اتفاقات مجاز را مشخص نموده ولي هيچ يک از RFC ها تعيين نكرده اند كه وقتي اتفاق نامعمولي مثل ارسال يک بسته ي SYN/ACK به يک پورت بسته رخ مي دهد سيستم بايد چه پاسخي دهد.
  - ✓ نفوذگر با استفاده از ابزارهاي مختلف بسته هاي گوناگوني با تنظيم پرچم هاي سرآيند آنها به سمت مقصد ارسال مي كند. بدين ترتيب بر اساس جوابي كه در هر مرحله سيستم به بسته هاي دريافتي مي دهد مي توا ن نوع آن را تشخيص داد.
  - ✓ ابزارهاي معروفي نظير NMAP در تشخيص سيستم عامل هدف استفاده مي 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

Vulnerability چیست ؟

- Vulnerability یا به صورت مختصر Vul را حفره ، سوراخ امنيتي و يا آسيب پذيري مي‌گوييم.
- سايت‌هايي هستند كه كارشان به‌طور عمده گزارش جديدترين Vul هاي كشف شده است مثل securitytracker.com يا securityfocus.com و...
- كشف Vul معمولا فقط در حد يک گزارش مي‌ماند تا اينكه روشي براي exploit كردن آن Vul درست شود. پس Vul جنبه تئوري قضيه است و exploit قسمت عملي آن!

پويش نقاط آسيب پذير

- معمولا نفوذگر از نرم افزارهايي براي پويش نقاط آسيب پذير استفاده مي كند كه يک پايگاه داده از نقاط ضعف بنيادي سيستم هاي عامل و نرم افزارهاي معروف در اختيار دارند و چون در مرحله ي قبلي نوع سيستم عامل مشخص گرديده است ، ابتدا با استفاده از اين پايگاه داده به دنبال اشكالات و نقاط ضعف بنيادي سيستم مي گردد.

- ابزارهاي پويش نقاط آسيب پذير ، به دنبال كشف موارد زير روي ماشين هدف مي گردند:
  - ✓ ضعف در پيكربندي پيش فرض يک سرويس دهنده
  - ✓ ضعف در پيكربندي سرويس دهنده
  - ✓ نقاط آسيب پذير شناخته شده

اجزاء اساسي ابزارهاي پويش آسيب پذيري

پايگاه اطلاعاتي از نقاط ضعف و آسيب پذيري سيستم ها

- در اين پايگاه اطلاعاتي فهرستي از نقاط ضعف سيستم هاي مختلف ذخيره شده است و نحوه ي آزمايش اين نقاط ضعف نيز تعيين گرديده است.

واسط كاربر

- اين قسمت از نرم افزار ،براي دريافت فرامين كاربر از طريق يک واسط گرافيكي است. از طريق اين واسط ، نفوذگر شبكه هدف و نوع آزمايشي را كه بايد انجام شود مشخص مي نمايد.

موتور پويش

- موتور پويش بر اساس بانک اطلاعاتي نقاط ضعف و همچنين تنظيماتي كه نفوذگر انجام داده است ، بسته هاي خاص و مشخصي را توليد و به سمت ماشين هدف ارسال مي نمايد تا بتواند تعيين كند كه آيا نقطه ي ضعف مورد آزمايش واقعا وجود دارد يا خير ؟

اجزاء اساسي ابزارهاي پويش آسيب پذيري

- پايگاه اطلاعاتي از نقاط ضعف سيستم كه در پويش هاي اخير كشف شده است
  - ✓ اين قسمت در حقيقت ذخيره كننده ي نتايج هر مرحله از پويش سيستم و نقاط ضعف كشف شده مي باشد. نتايج حاصل ازاين مرحله مي تواند مجددا در خدمت موتور پويش براي بررسي هاي جديد قرار بگيرد.
- بخش گزارشگيري و ثبت نتايج پويش
  - ✓ اين قسمت از نرم افزار گزارش هاي نهايي از فهرست بررسي هاي انجام شده و نتيجه ي پويش ماشين هدف را ارائه مي دهد.