



دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

مقدمه ای بر حملات در شبکه

نستوه طاهری جوان

nastoooh@aut.ac.ir



مراحل حملات

✓ اکثر حملات هدفمند در شبکه دارای پنج مرحله هستند:

1. شناسایی مقدماتی شبکه هدف

2. جستجو به دنبال رخنه ای برای نفوذ

3. نفوذ و حمله

4. حفظ سیطره بر شبکه

5. رد گم کردن و پوشش مسیر

مرجع

Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Edward Skoudis, 2nd ed.



مراحل حملات

✓ مرحله اول: شناسایی مقدماتی

عموما به کمک روش هایی مانند زیر انجام می شود:

1. مهندسی اجتماعی
 - مثل تخلیه اطلاعاتی و و
2. دسترسی مستقیم و فیزیکی
 - ورود به سازمان هدف
3. آشغالگردی
 - جستجو به دنبال کاغذ، سی دی، هارد سوخته
4. جستجو در وب
 - وب سایت سازمان قربانی، رقبا و شرکا... سایت های Who is و و
5. و غیره



مراحل حملات

✓ مرحله دوم: جستجو به دنبال رخنه ای برای نفوذ

عموما به کمک روش هایی مانند زیر انجام می شود:

1. War Dialing

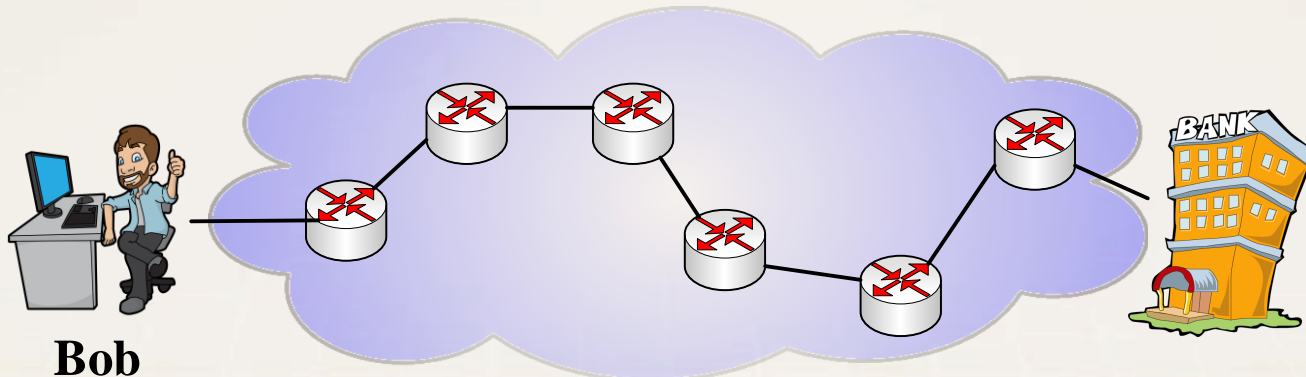
- جستجو برای مودم های فعال

2. نقشه برداری از شبکه از راه دور

- آیا از راه دور ممکن است؟ اهمیت تنظیمات فایروال

➤ استفاده از ping, TraceRoute, ارسال بسته های خاص TCP مانند بسته Syn یا بسته های نامتعارف...

➤ پیشنهاد: برای نقشه برداری از شبکه با نرم افزارهایی مانند Cheops-ng سر و کله بزنید.





مراحل حملات

✓ مرحله دوم: جستجو به دنبال رخنه ای برای نفوذ

عموما به کمک روش هایی مانند زیر انجام می شود:

3. Port Scanning

- هدف: کشف پورتهای باز (سرویس دهنده ها) بر روی یک ماشین.
- ارسال بسته های خاص TCP بر روی پورتها و انتظار برای پاسخ ها
 - یادآوری یک: طبق پروتکل TCP، دریافت یک بسته بر روی پورت بسته: نادیده گرفتن بسته...
 - یادآوری دو: ارسال بسته نامتعارف (غیر منتظره) بر روی یک پورت باز: برگشت بسته RST...
 - یادآوری سه: در سیستم عامل های مختلف ممکن است این قانون به گونه دیگری پیاده شده باشد.
 - روش های مختلفی برای پویش پورت ها وجود دارد، بر اساس ارسال بسته های متفاوت...
- اهمیت نقش فایروال... مثلا تفاوت ارسال SYN یا ارسال SYN-Ack
- مساله لو رفتن آدرس IP نفوذگر، به دلیل ارسال بسته های متوالی؟
- پیشنهاد: حتما با نرم افزارهایی مانند Nmap سر و کله بزنید.



مراحل حملات

✓ مرحله دوم: جستجو به دنبال رخنه ای برای نفوذ

عموما به کمک روش هایی مانند زیر انجام می شود:

4. FireWalk بر علیه FireWall

- نکته: هنگام ارسال بسته های خاص برای اسکن پورتهای، در صورت عدم بازگشت جواب، نفوذگر نمیداند فایروال اجازه عبور بسته را نداده است یا پاسخی در کار نبوده است؟
- هدف: کشف پورت های باز بر روی فایروال...
- فرض: نفوذگر آدرس IP دیواره آتش را دارد.
- گام اول: همانند TraceRoute بسته های IP با TTL های یک، دو، سه و ... ارسال می کنیم تا فاصله تا فایروال را کشف کنیم.
- گام دوم: یک بسته IP با TTL مساوی $n+1$ و با شماره پورت مورد نظر به سمت ماشین هدف ارسال می کنیم. یعنی دقیقا آدرس روتر پشت فایروال... حال منتظر بسته ICMP Time Exceeded میمانیم.



مراحل حملات

✓ مرحله دوم: جستجو به دنبال رخنه ای برای نفوذ

عموما به کمک روش هایی مانند زیر انجام می شود:

5. پویش نقاط آسیب پذیر برنامه ها و سرویس ها

- جایگاه: پس از کشف یک پورت باز... یا در صورت ارائه سرویس عمومی توسط یک پورت باز...
- روش: برقراری ارتباط های متفاوت با سرویس دهنده...
- هدف: کشف نقاط ضعف مانند پیکربندی ضعیف، کلمات عبور ساده، نقاط ضعف مشهور و ...
- نرم افزارهای مختلف و متنوعی برای این امور وجود دارد.
- پیشنهاد: حتما با برنامه هایی مانند SAINT, SARA, SATAN, Nessus سر و کله بزنید.



مراحل حملات

✓ مرحله سوم: نفوذ

حملات بر اساس اهدافشان، تنوع بسیار زیادی دارند مانند:

- حملات افشای اطلاعات و استراق سمع ها
- قطع ارتباط و اخلال در سرویس
- دستکاری غیر مجاز در داده ها
- سو استفاده از منابع شبکه با اهداف خاص (مثل ماینینگ!)
- استفاده غیر مجاز از سرویس ها
- جعل هویت
- و و و



مراحل حملات

✓ مرحله سوم: نفوذ

حمله یک، حمله بر علیه کلمات عبور

○ راه اول: مبتنی بر سعی و خطا

- کلمات عبور پیش فرض

- حدس های آگاهانه

- Brute Force

- نکته: مواظب راه کار محدود کردن تعداد سعی و خطا، و ارتباط آن با DOS باشید!

○ راه دوم: روش های علمی تر!

- نکته مهم یک: اصل کلمات ورود (یا هش آنها) باید در یک محل ذخیره شود!

- کاربرد عمومی: محیط لوکال مانند ویندوز

- پیشنهاد: حتما در مورد تغییر فایل های SAM در ویندوز تحقیق کنید.

- نکته مهم دو: کلمات ورود (یا رمز شده آنها) بر روی شبکه در حال رفت و آمد هستند!

- کاربرد عمومی: در شبکه ها



مراحل حملات

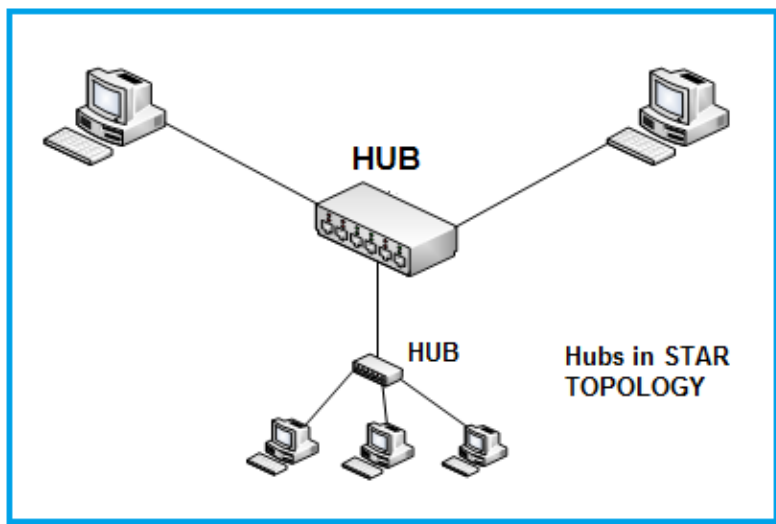
✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر هاب

- یادآوری: توپولوژی و نحوه عملکرد اترنت مبتنی بر هاب
- استفاده از مود promiscuous در کارت شبکه.

- پیشنهاد: حتما با ابزار WireShark سر و کله بزنید.





مراحل حملات

✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر سوئیچ

- یادآوری: تفاوت سوئیچ با هاب و نحوه عملکرد سوئیچ در اترنت.
- یادآوری: نحوه تشکیل و استفاده از جدول سوئیچینگ.

interface #	MAC Add.
1	xxx
2	yyy
3	zzz
1	aaa
1	bbb
...	...

- بیان شماتیک جدول سوئیچینگ:



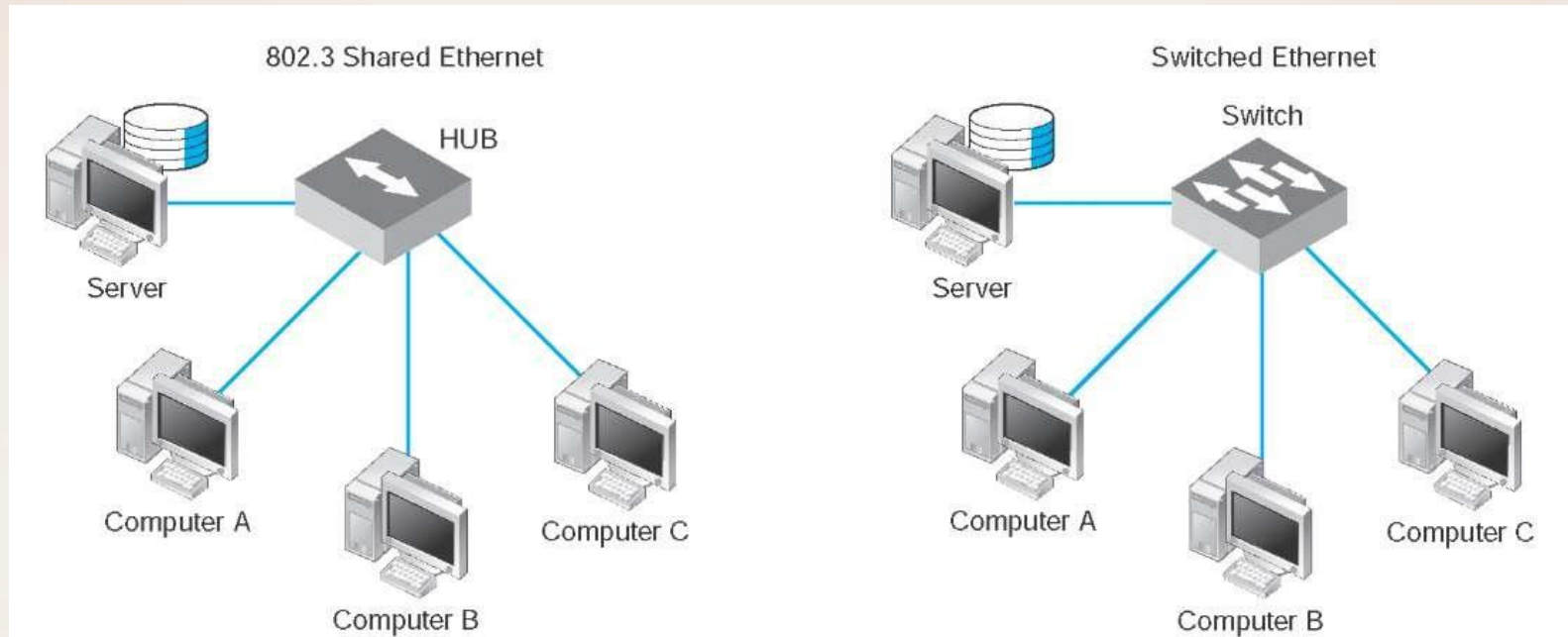
مراحل حملات

✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر سوئیچ

جمع بندی تفاوت هاب و سوئیچ





مراحل حملات

✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر سوئیچ

- روش اول: ارسال فریم های جعلی، با آدرس های مبدا متفاوت
 - نتیجه: تلاش سوئیچ برای یادگیری آدرس های جدید
 - نتیجه: پر شدن جدول سوئیچینگ
 - نتیجه: از پا درآمدن سوئیچ
 - تحلیل: بهترین عملکرد سوئیچ در این شرایط از دید شما چیست؟؟؟
- پیشنهاد: حتما با ابزارهای Dsniff یا Cain سر و کله بزنید.



مراحل حملات

✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر سوئیچ

• روش دوم: ARP spoofing

➤ یادآوری: جزئیات کامل پروتکل ARP

» شامل: بسته های ARP، جدول ARP و سایر جزئیات...

➤ مثال از ARP spoofing: هدف Gateway پیش فرض شبکه!!! ☹️

➤ خلاصه روال کار: ارسال بسته پاسخ ARP برای ماشین قربانی

» استمرار حمله نیازمند به فوروارد کردن کلیه بسته های بعدی را دارد.

➤ عملاً این حمله بر علیه سوئیچ نیست، بلکه در شبکه های مبتنی بر سوئیچ کاربرد دارد.



مراحل حملات

✓ مرحله سوم: نفوذ

حمله دو، استراق سمع در سطح شبکه داخلی

○ شبکه های اترنت مبتنی بر سوئیچ

• روش سوم: DNS spoofing

➤ یادآوری: جزئیات کامل پروتکل DNS در شبکه

» شامل: پرس و جوها، سرور محلی و ...

➤ روال کار، قدری مشابه ARP Spoofing

➤ تامل: ترکیب این حمله (ها) با مفهوم فیشینگ!!!



مراحل حملات

✓ مرحله سوم: نفوذ

حمله سه، حمله به وب، Session Hijacking

- یادآوری: مفهوم State-less بودن یا نبودن... (از ابتدا تا امروز)
- یادآوری: مرور مفهوم سشن در وب
 - استفاده از کوکی ها
 - استفاده از Session ID
 - » روش های تبادل Session ID
 - » تبادل از طریق URL
 - » تبادل از طریق کوکی! دائم یا موقت؟ در دیسک یا در حافظه؟
 - » تبادل از طریق کدهای مخفی HTML
 - روش نهایی و مطمئن: استفاده از پراکسی برای کشف یا تغییر ID خود...
 - » پیشنهاد: حتما حتما با ابزارهایی مانند Achilles سر و کله بزنید.
 - مساله مهم: حدس یک ID معتبر (کورکوران یا هدفمند؟)

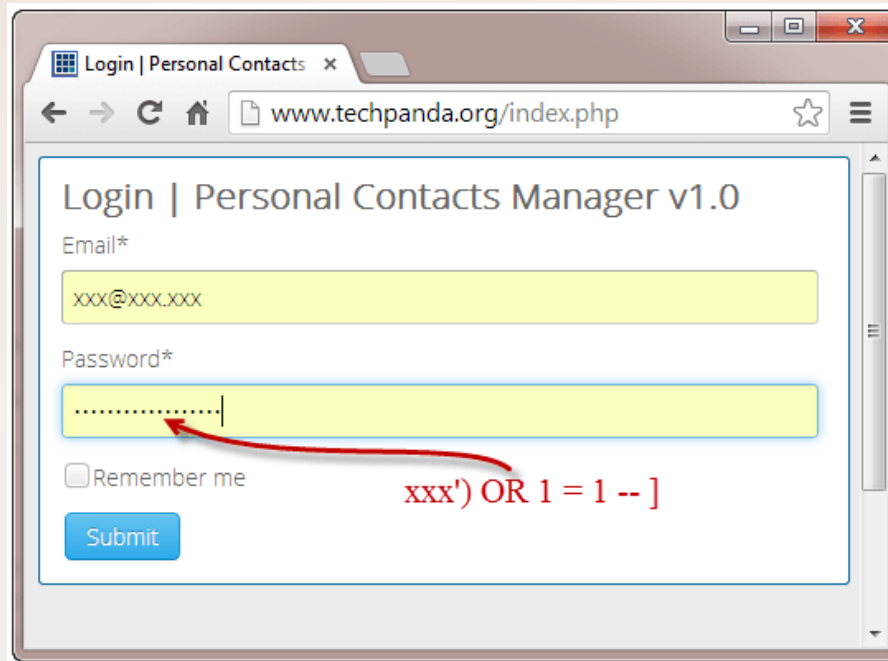


مراحل حملات

✓ مرحله سوم: نفوذ

حمله چهارم، حمله به وب، SQL Injection

- روش: نفوذگر با استفاده از دانش SQL اش، فیلدها را به گونه ای پر می کند که به هدف خود برسد.



`SELECT * FROM users WHERE email = 'xx@xx.xx' AND password = md5('1234');`



مراحل حملات

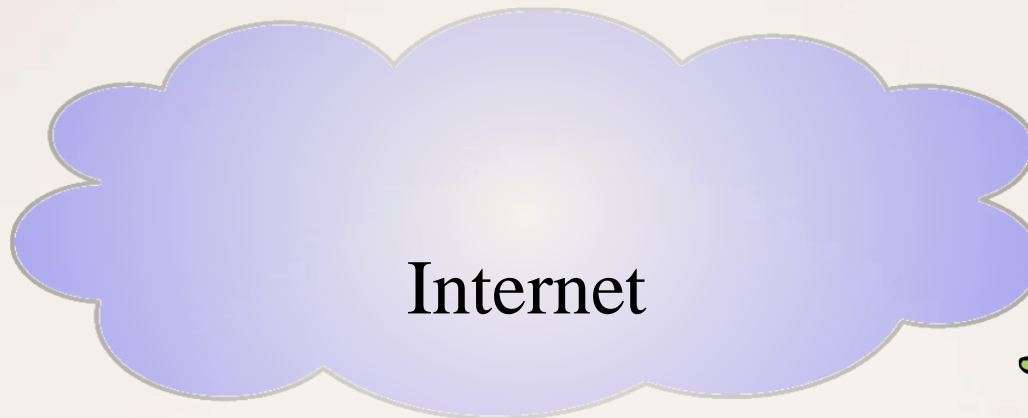
✓ مرحله سوم: نفوذ

حمله پینج، DOS

- یادآوری: هدف اصلی و مفهوم حملات از نوع DOS



Trudy





مراحل حملات

✓ مرحله سوم: نفوذ

حمله پنج، DOS

• نوع اول: SYN flood

- یادآوری: دست تکانی سه مرحله ای در TCP
 - » نگهداری اطلاعات SYN توسط سرور در حد چند دقیقه
 - ارسال بسته های جعلی SYN به صورت سیل آسا به سمت سرور

• انواع دیگری از حملات DOS قدیمی: Smurf و Fraggle و Land و و و



مراحل حملات

✓ مرحله سوم: نفوذ

حمله پنج، DOS

D.D.O.S •

- نکته مهم: جنگ منابع!
- راه حل: استفاده از ماشین های زامبی!
- مزیت برای نفوذگر:
 - » احتمال موفقیت بالا
 - » کاهش هزینه
 - » پنهان ماندن هویت
- دست تکانی سه مرحله ای در TCP
 - » نگهداری اطلاعات SYN توسط سرور در حد چند دقیقه
 - ارسال بسته های جعلی SYN به صورت سیل آسا به سمت سرور



مراحل حملات

✓ مرحله سوم: نفوذ

ادامه دارد...



منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.



پایان