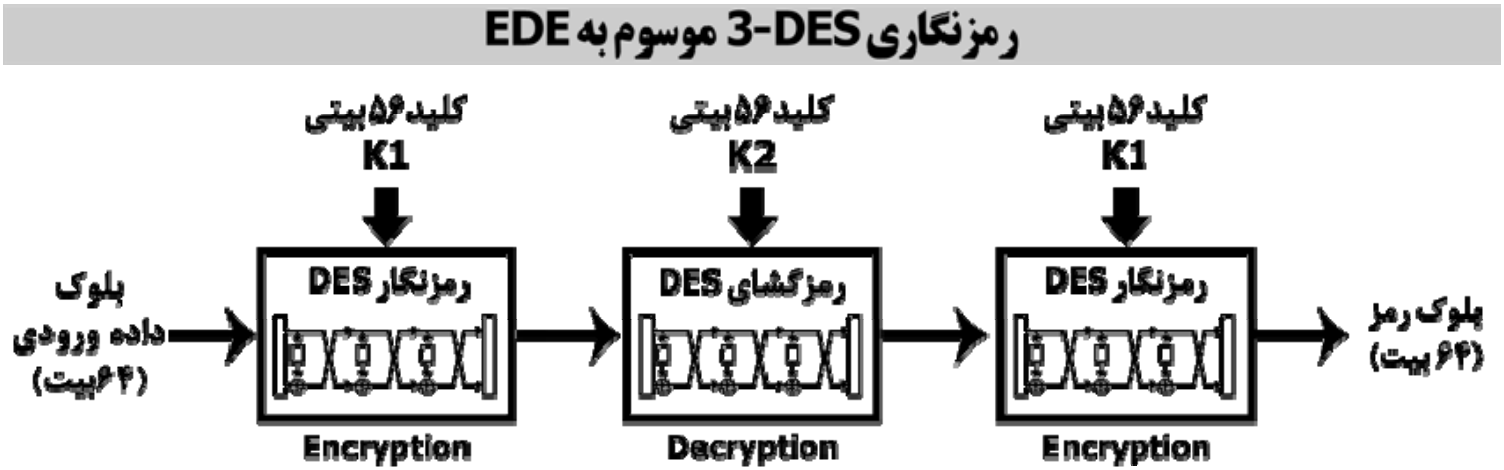
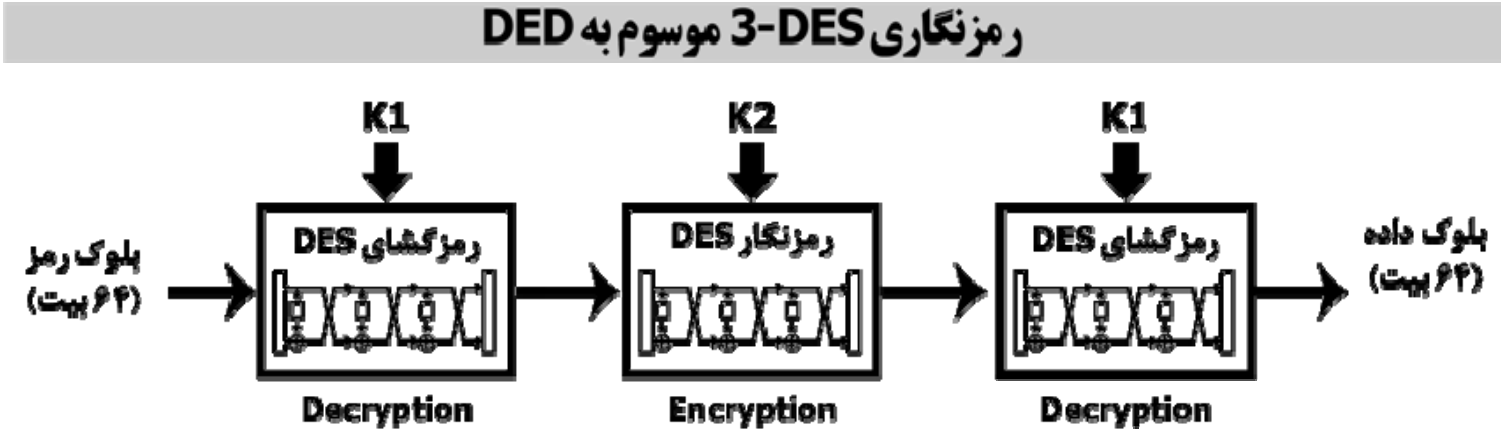
الگوریتم 3-DES

- IBM برای افزایش طول کلید DES به 112 b ، روش 3-DES (Triple DES) را ابداع کرد.
- در 3-DES ، داده ها به کمک دو کلید ۵۶ بیتی، سه بار رمزنگاری می شوند.
- در 3-DES در مرحله دوم رمزنگاری، از رمزگشای DES و کلید K_2 استفاده شده است که عملاً تفاوتی با رمزنگاری ندارد و دلیل آن اینست که با انتخاب $K_2=K_1$ این مدار برای DES نیز جواب می دهد.

الگوریتم 3-DES





سخت افزار رمزنگار 3-DES تولید IBM

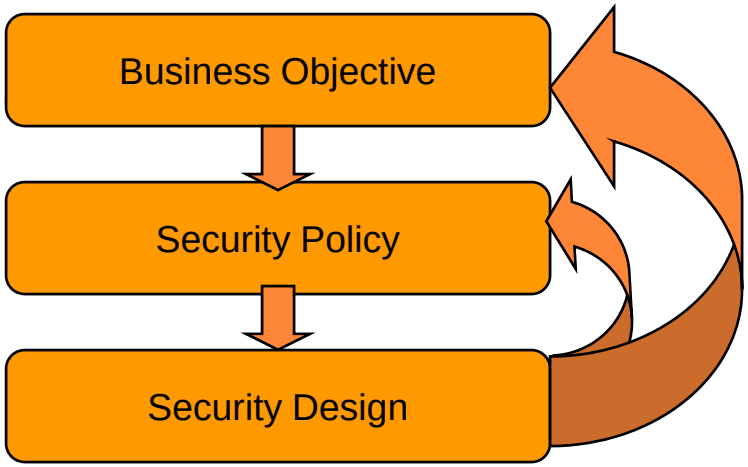
امنیت شبکه

امنیت شبکه یک سیستم است

- تعریف سیستم امنیت شبکه: مجموعه ای از ابزارها و فناوری های شبکه، به همراه روشهای مؤثری که در همکاری با یکدیگر امنیت اطلاعات را تأمین می کنند.
- ارزش اصلی سیستم امنیتی وقتی مشخص می شود که بتواند در برابر حملات ناشناخته مقاومت کند.

نیازهای کاری باید در اولویت قرار گیرند

- برای اعمال هر تغییر جدید در سیستم امنیتی باید سه عامل زیر را در نظر بگیرید.



طراحی شبکه امن، مستقل از طراحی شبکه نیست

- نباید امنیت را به شبکه اضافه کنید، بلکه باید بر اساس طراحی امنیتی از همان ابتدا، شبکه را امن طراحی نمایید تا کارایی و قابلیتهای آن افزایش یابد.

همه چیز هدف است

- با توجه به وابستگی اجزای شبکه به یکدیگر یک مهاجم می تواند با حمله به یکی از اجزای شبکه، با استفاده از وابستگی ها، به هدف خود برسد، بنابراین در طرح امنیتی شبکه، باید از تمامی اجزای شبکه، به اندازه کافی محافظت شود.
- مهاجم برای نیل به اهداف خود می تواند از هر چیزی به عنوان سلاح استفاده کند، حتی از سیستمهای موجود در شبکه، مانند سرورها.

سعی کنید کارها از نظر عملیاتی ساده باشند

طراحی شبکه های امن باید تا حد ممکن ساده باشد، به گونه ای که تیم عملیاتی شبکه در نگهداری آن با مشکل مواجه نشوند.

برخی معیارهای اندازه گیری سادگی عبارتند از:

- برای نگهداری شبکه به چند متخصص نیاز دارید؟
- در شرایط فشار و حمله، امکان اشتباه چقدر است؟
- برای بررسی حمله انجام شده، پس از وقوع، چه تعداد فایل Log باید بررسی شوند؟
- برای یافتن شواهد قانونی، جهت ارائه به دادگاه،چقدر زمان لازم است؟

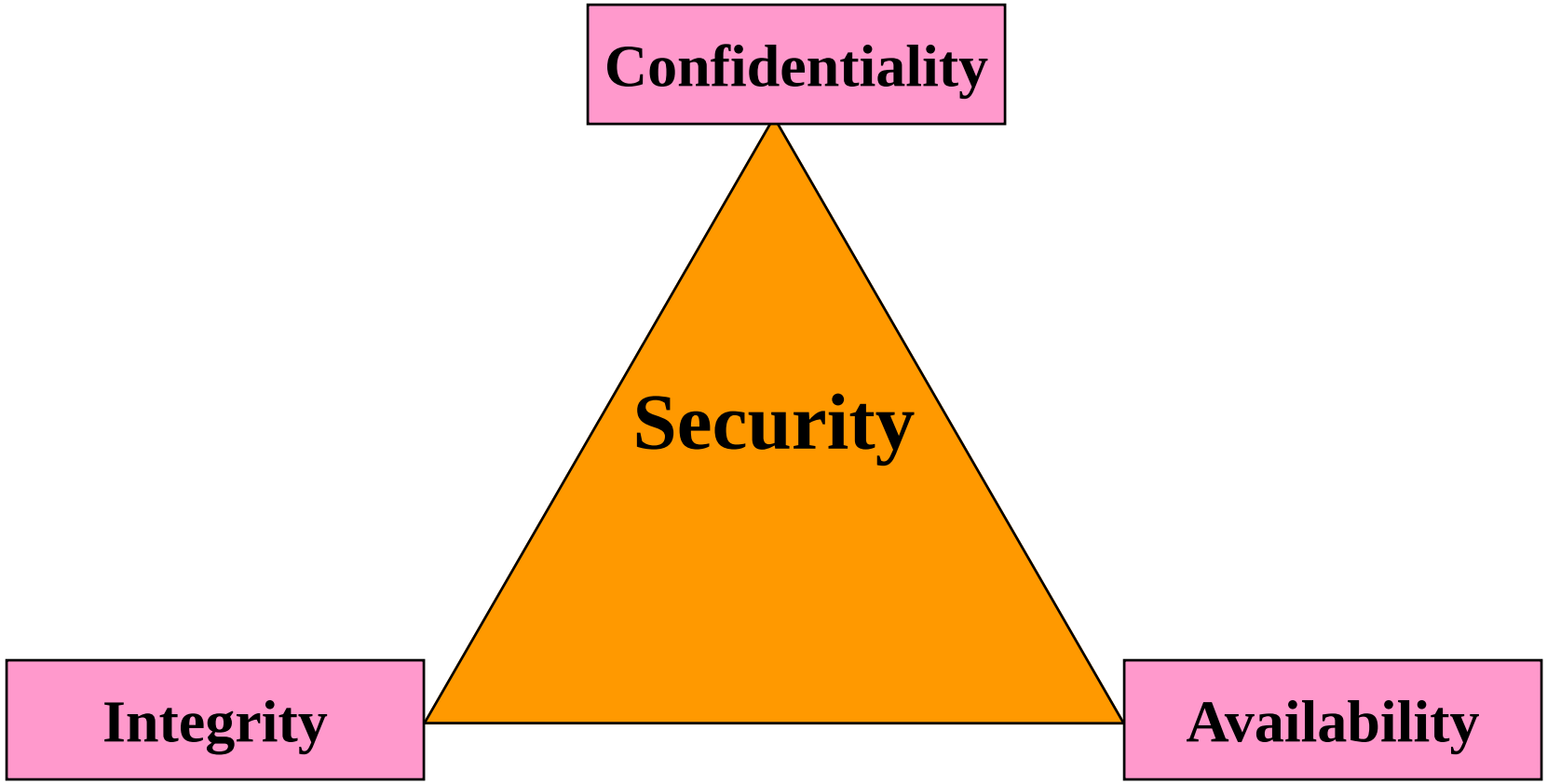
امنیت از طریق پنهان کاری به دست نمی آید

- امنیت یک شبکه باید مبتنی بر عملکرد درست اجزا، جهت کنترل دسترسی ها، باشد نه مخفی کردن اطلاعات مربوط به اجزاء و ورژن نرم افزارها.
- گرچه در بعضی موارد لازم است اطلاعات مربوط به تکنولوژی ها و پیکربندی ها را مخفی نگه دارید، اما امنیت شبکه نباید به آن متکی باشد.

محرمانگی و امنیت با هم تفاوت دارند

- محرمانگی، حفاظت از اطلاعات در مقابل دسترسی افراد غیر مجاز است.
- امنیت، حفاظت از سیستمها، منابع و اطلاعات در مقابل دسترسی غیر مجاز و سوء استفاده است.
- در واقع محرمانگی، زیر مجموعه ای از امنیت است.

امنیت متکی بر سه عنصر CIA است.



امنیت شبکه قابل خریداری نیست

- امنیت شبکه صرفاً با خرید محصولات امنیتی قابل حصول نیست، بلکه لازم است از متخصصین و راهکارهای مناسب مبتنی بر نیازهایتان استفاده نمایید.

سیاست امنیتی چیست؟

- سیاست امنیتی، بیانی رسمی از قوانینی است که باید توسط افرادی که به فناوری و دارایی اطلاعاتی سازمان شما دسترسی دارند، رعایت شود.
- در واقع، سیاستهای امنیتی مانند نقشه ای است که چگونگی طراحی امنیتی و عملیاتی کردن آنرا به شما نشان می دهد و نیز مرجعی است برای بررسی شبکه امن پیاده سازی شده، جهت اطمینان از اجرای استراتژی امنیتی خود.
- نیازهای تجاری و تحلیل ریسک، مهمترین عوامل تأثیرگذار در سیاست امنیتی هستند.

ملاحظات اعمال سیاست امنیتی

برای اعمال و اجرای سیاستهای امنیتی طراحی شده، چهار راهکار وجود دارد:

1. اعمال به وسیله تکنولوژی های بلادرنگ: استفاده از یک تکنولوژی امنیتی برای کنترل دسترسی ها
2. بررسی تطابق به کمک تکنولوژی های پس زمینه: مشکل در این حالت بلافاصله تشخیص داده نمی شود، بلکه امکان بررسی پیروی کاربران از سیاستهای امنیتی وجود دارد.
3. بررسی تطابق غیر فنی: در این روش بررسی کاربران و سیستم توسط مدیران، و نه تیم فنی، انجام می شود.
4. بررسی تطابق قراردادی: در این روش، الزامات امنیتی در قرارداد کارمندان گنجانده می شود تا عدم پیروی منجر به توبیخ شود.

ایجاد سیستم امنیتی

ایجاد یک سیستم امنیتی در سه گام انجام می شود:

1. بررسی راه اندازهای (Driver) سیاست امنیتی
2. تولید یک سیاست امنیتی
3. طراحی سیستم امنیتی

- بهتر است سیاستهای امنیتی، خلاصه و عاری از جزئیات فنی باشد.

گام اول: بررسی راه اندازهای سیاست امنیتی

- دو راه انداز سیاستهای امنیتی عبارتند از : نیازهای تجاری و تحلیل ریسک
- دو دسته از نیازهای تجاری می توانند بر سیاست امنیتی تأثیر بگذارند: اهداف تجاری و تحلیل هزینه/ منفعت
- برای تشخیص نقاط ضعف سیستم امنیتی خود می توانید از ابزارهای نفوذگری استفاده کنید.

گام دوم: تولید یک سیاست امنیتی

مهمترین بخشهایی که باید برای آنها سیاست امنیتی داشته باشید عبارتند از:

1. سیاستهایی که کاربرد درست را مطرح می کنند.
2. سیاستهایی که ارتباط با شبکه های راه دور را مد نظر قرار می دهند.
3. سیاستهایی که میزان اهمیت اطلاعات بخشهای مختلف سازمان را تبیین می کنند.
4. سیاستهایی که از حریم خصوصی کاربران و مشتریان شبکه دفاع می کنند.
5. سیاستهایی که حداقل امنیت ابزارها، پیش از اتصال به شبکه را تعیین می کنند.

گام سوم: طراحی سیستم امنیتی

- آخرین گام، پیاده سازی سیستم امنیتی، بر اساس سیاستهای امنیتی، به صورت عملی است.

- نمونه یک سیاست امنیتی

چرخه عمر اقدامات امنیتی

اقدامات امنیتی، فرآیندهای زیر را شامل می شود:

- نظارت بر سیستم و نگهداری از آن: برای مثال انجام آخرین Update های نرم افزارها
- بررسی تطابق: در دوره های مشخص باید تطابق سیستم امنیتی با سیاستهای امنیتی بررسی شود.
- واکنش به رخدادها: انعطاف پذیری سیستم و حتی سیاستهای امنیتی با تغییرات، مشکلات و نیازهای جدید سازمان

فرآیند حمله و انواع مهاجم

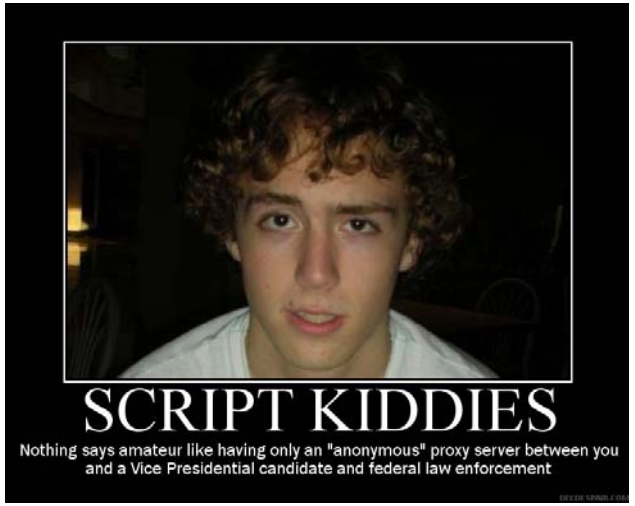
- فرآیند حمله با یک مهاجم، بر علیه یک هدف مشخص، با استفاده از یک آسیب پذیری انجام می شود.

انواع مهاجمین از نظر دانش فنی عبارتند از:

- تازه کار (Script Kiddy)
- قفل شکن (Cracker)
- نخبه (Elite)

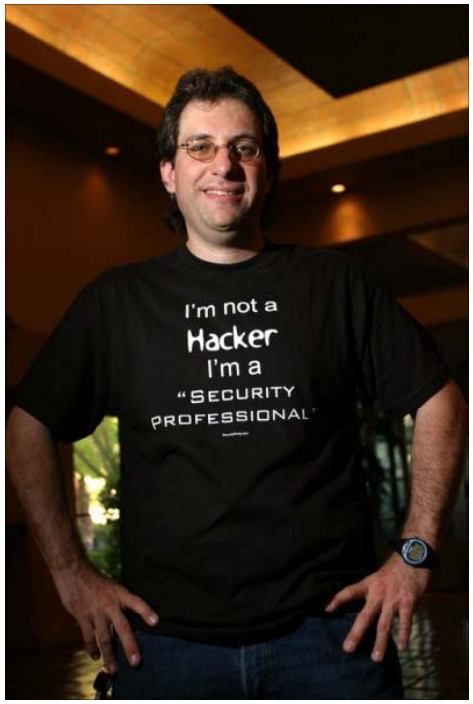
تازه کار (Script Kiddy)

- اعضای این گروه، جوانانی هستند که معمولاً از ابزارهای خودکار ،که برای این کارها ساخته شده استفاده می کنند.



قفل شکن (CRACKER)

- این افراد قادرند حملات جدیدی را پی ریزی و اجرا کنند.
- به این گروه، کلاه مشکی (Black Hat) نیز گفته می شود.
- واژه هکر (Hacker) یک واژه مثبت است و برای این گروه مناسب نیست.



کوین دیوید می‌تنیک متولد ۱۶ آگوست ۱۹۶۳ یک مشاور امنیتی رایانه‌ای و نویسنده‌است. وی در اواخر قرن بیستم یک هکر رایانه‌ای بود که در زمان دستگیری اش توسط وزارت دادگستری آمریکا به عنوان مهم‌ترین و تحت تعقیب‌ترین یاغی رایانه‌ای تاریخ آمریکا معروف شد. در اواخر دهه ۱۹۹۰ می‌تنیک به جرم استفاده غیرقانونی و سرقت اطلاعات و حقوق شخصی از شبکه‌های رایانه‌ای تحت تعقیب بود.می‌تنیک در سال۲۰۰۲ در کتابش با عنوان» **هنر فریفتن** «اظهار کرد که دستیابی وی به کلمات عبور به‌وسیله مهندسی اجتماعی بوده‌است.نکته قابل توجه آنکه می‌تنیک از نرم‌افزارهای هک و پویشگر و هیچ دستگاه دیجیتال دیگری برای کسب اطلاعات استفاده نکرده بود.

درحال حاضر می‌تنیک یک شرکت مشاوره امنیت رایانه‌ای دارد.

نخبه (ELITE)

- این گروه خطرناکند و منابع مالی کافی دارند.
- جاسوسان، گروههای نظامی و تروریستها جزء این گروهند.

انواع آسیب پذیری

نقاط ضعف و آسیب پذیری شبکه ها ۵ دسته اند:

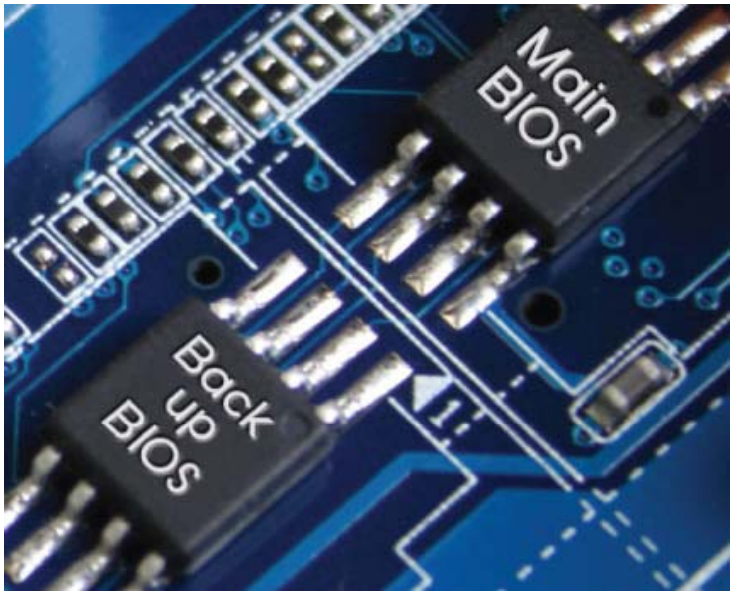
1. نرم افزاری
2. سخت افزاری
3. پیکربندی
4. سیاست
5. کاربرد

آسیب پذیریهای نرم افزاری

- در بررسی های انجام شده مشخص شده در هر ۱۰۰۰ خط کد، به طور متوسط، ۵ تا ۱۵ خطا وجود دارد. (Windows XP حدود ۵۰ میلیون خط کد دارد) اگر تنها درصد کمی از این خطاها نیز امنیتی باشند خواهید دید که هزاران حفره امنیتی در نرم افزار های امروزی وجود دارد.

آسیب پذیریهای سخت افزاری

- این نوع آسیب پذیریها کمتر شایع هستند. مثلاً آسیب پذیری Bios، CPU و ... خطرناکتر از آسیبهای نرم افزاری هستند چون امکان تعمیر آنها با Patch وجود ندارد.



آسیب پذیریهای پیکربندی

- اکثر اپراتورهای شبکه، اطلاعات کافی در مورد فناوری های شبکه، به خصوص در سیستمهای پیچیده ندارند. بنابراین احتمال اشتباه در پیکربندی وجود دارد.

آسیب پذیریهای سیاست

- با توجه به وابستگی امنیت سیستم به سیاستهای امنیتی، ضعف در تعریف یا پیاده سازی سیاستهای امنیتی موجب این نوع آسیب پذیری می شود.
- به همین دلیل امنیت سیستم باید در طول زمان با تغییر سیستم و سیاستها بهبود یابد.

آسیب پذیریهای کاربرد

- کاربران ممکن است در یک سیستم امنیتی دخل و تصرف کنند و سیاستهای امنیتی را نقض کنند.

نتایج حمله

- افشای اطلاعات Disclosure of information

انتشار اطلاعات بین افراد غیرمجاز شامل دزدی گذرواژه، خواندن بخشهای غیر مجاز از هارددیسک، آموختن اطلاعات محرمانه قربانی

- تخریب اطلاعات Corruption of information

تغییر غیر مجاز اطلاعات ذخیره شده یا در حال انتقال مانند حملات "مرد میانی" یا ویروسهایی که داده ها را خراب می کنند.

- منع خدمت Denial of service

کاهش یا مسدود سازی عمدی منابع شبکه مانند حملات "سیل ریزی"

نتایج حمله

- دزدی خدمت Theft of service

دسترسی غیر مجاز به خدمات کامپیوتر یا شبکه، بدون تنزل خدمات به سایر کاربران، مانند دزدی گذرواژه و ورود به شبکه، به صورت مجاز، دسترسی به Wireless LAN و دزدی نرم افزار

- دسترسی بیشتر Increased access

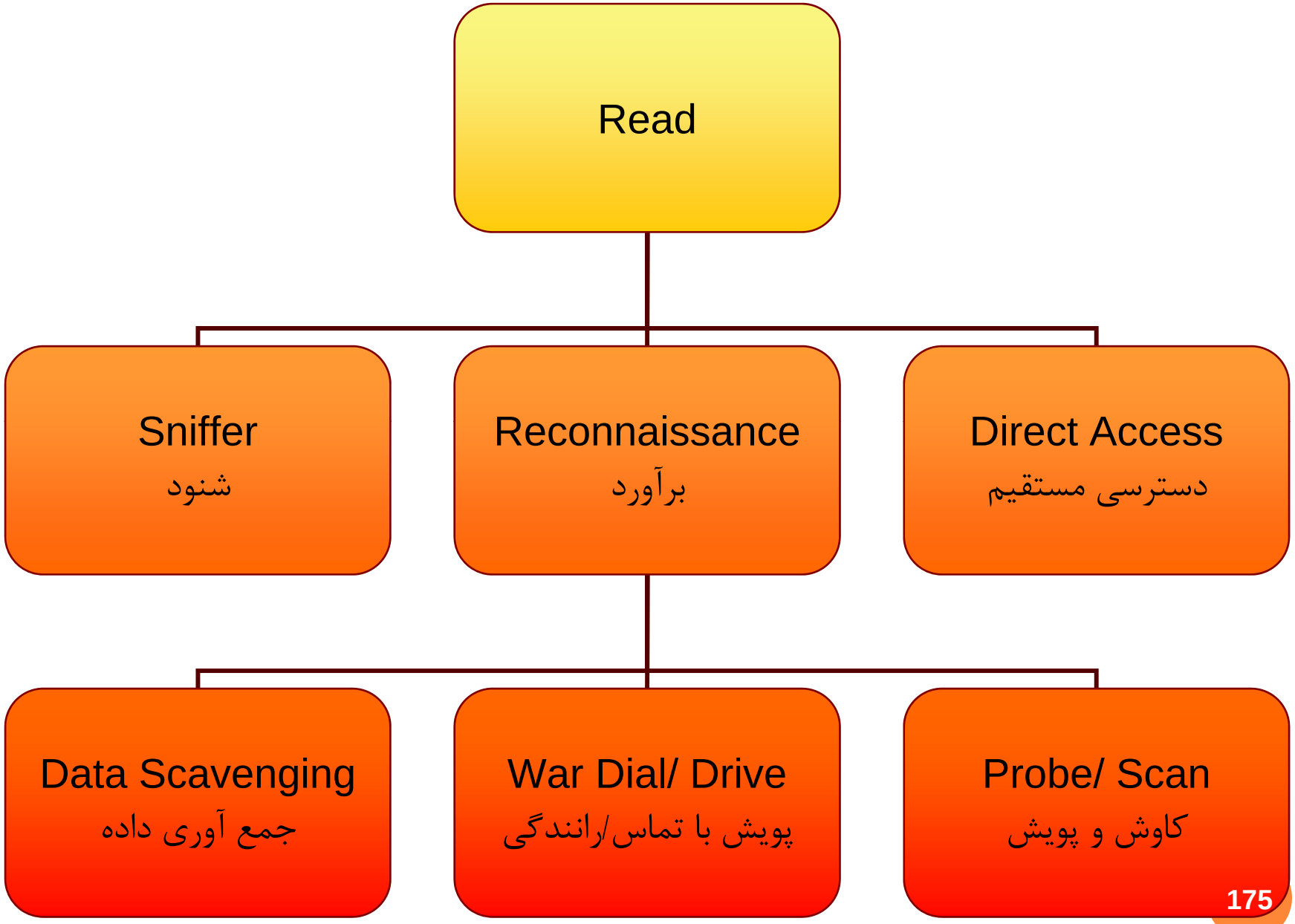
افزایش غیرمجاز حقوق دسترسی به یک سرور یا شبکه، که اغلب پایه ای برای سایر حملات است و خود نتیجه نهایی محسوب نمی شود.

دسته بندی حملات

1. خواندن (Read) – دسترسی غیر مجاز به اطلاعات
2. دستکاری (Manipulate) – تغییر اطلاعات
3. جعل (Spoof) – ارائه خدمات یا اطلاعات غلط
4. سیل ریزی (Flood) – سرریز منابع یک کامپیوتر
5. هدایت (Redirect) – تغییر جریان اطلاعات
6. ترکیبی (Composite) – استفاده از چند روش فوق

حمله خواندن

- حمله خواندن دربرگیرنده خانواده ای از حملات است که هدف آنها کسب اطلاعات از قربانی است. این خانواده از حملات شامل به دست آوردن آدرسهای IP سازمان، پویش پورت و پویش آسیب پذیری های این آدرسها و دسترسی به سیستمهای آسیب پذیرو خواندن داده های آن است.


Read
Sniffer
شنود
Reconnaissance
برآورد
Direct Access
دسترسی مستقیم
Data Scavenging
جمع آوری داده
War Dial/ Drive
پویش با تماس/رانندگی
Probe/ Scan
کاوش و پویش

برآورد

- هدف اصلی حملات برآورد، به دست آوردن اطلاعات در مورد قربانی است.

جمع آوری داده

جمع آوری داده، همیشه گام اول در حملات شبکه است. در این حمله، مهاجم با استفاده از ابزارهای مبتنی بر شبکه و موتورهای جستجو، تا جایی که بتواند، در مورد سازمان هدف اطلاعات کسب می کند. این حملات به دلیل حجم ترافیک کم، عمومی بودن موتورهای جستجو و استفاده از سرورهایی غیر از سرورهای قربانی، غیر قابل کشف است.

نتیجه این نوع حمله، اطلاعات زیر را به ما می دهد:

- آدرس IP سرورهای قربانی(Email, DNS, Web)
- بازه های IP منتسب به قربانی
- ISP قربانی
- ابزارهای این حمله عبارتند از: Whois, Nslookup, Tracert, Ping, Search Engine,

پویش با تماس و پویش با رانندگی

- این حملات به مهاجمین اجازه می دهد بدون ورود از در اصلی، وارد شبکه قربانی شوند. در حمله پویش با تماس، مهاجم با شماره تلفنهای قربانی تماس می گیرد تا مودمهای فعال را پیدا کند، سپس مهاجم سعی می کند به این مودمها متصل شده و Login نماید. در صورت موفقیت آمیز بودن این حمله، مهاجم قادر خواهد بود بخش مهمی از مکانیزمهای امنیتی را دور بزند، چون مهاجم برای شبکه همانند یک کارمند قانونی سازمان به نظر می رسد.
- پویش با رانندگی مشابه پویش با تماس است، با این تفاوت که مهاجم با یک ماشین در اطراف سازمان قربانی به رانندگی پرداخته و از یک آنتن قوی برای اتصال به شبکه بیسیم قربانی استفاده می کند. هدف مهاجم آن است که به آنتنهای بیسیم شبکه قربانی (Access point) که از امنیت ضعیفی برخوردارند، متصل شده و از این طریق به شبکه او نفوذ کند.

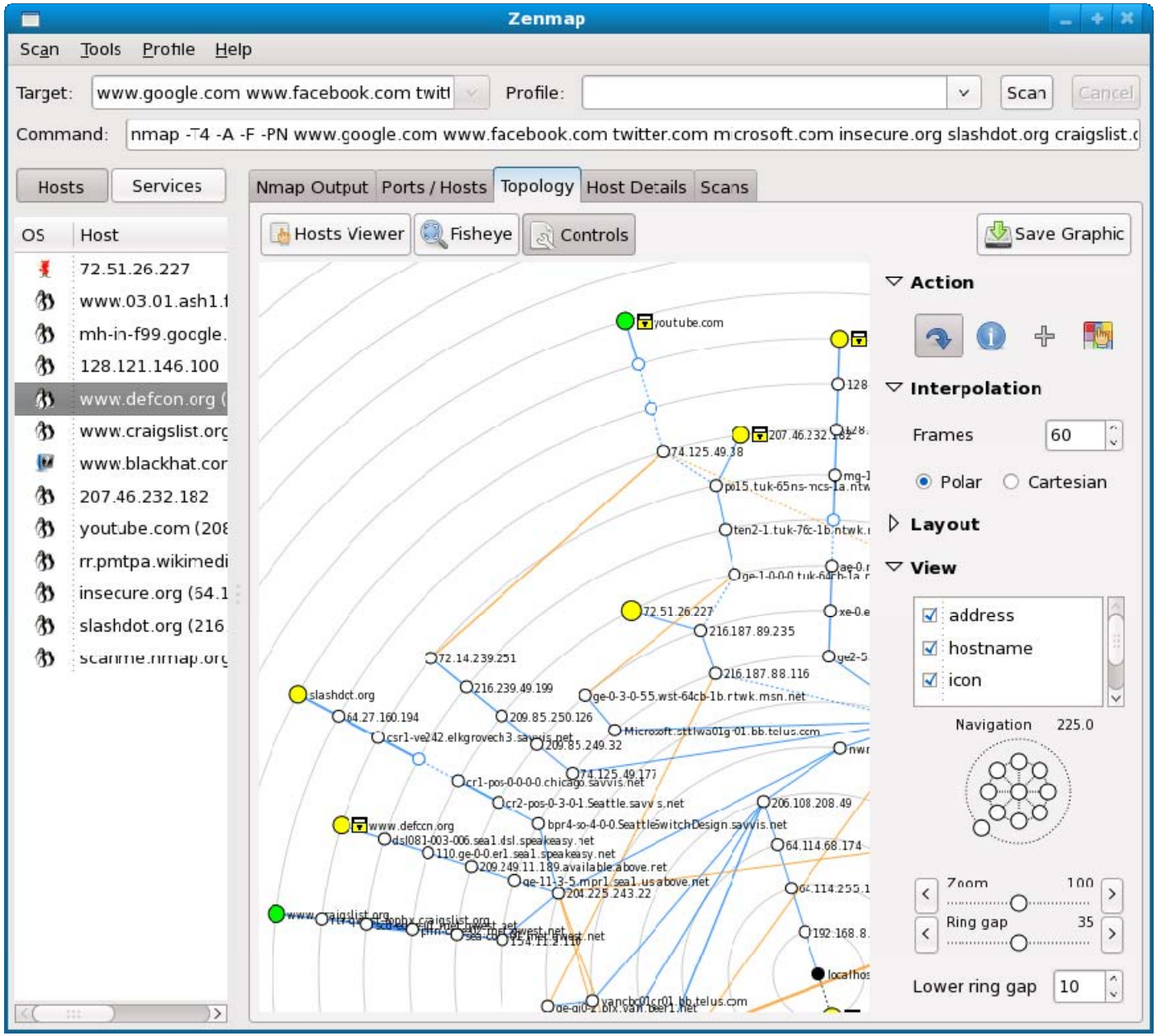

USR5462 46%
Ahead 27%
SANDOZ 53%
WGWL 12%
FZ_Matten 22%
d4rkwl4n 33%
flozonet
risen
lasvegas
kiffkaff 33%
OttosNetz 27%
risen
5463 4420 33%
LILY'S 43%

کاوش و پویش

این حمله معمولاً در دو فاز پویش پورت و در مرحله بعد، پویش آسیب پذیری و با استفاده از اطلاعات حمله، "جمع آوری داده" انجام می شود.

برای این حمله از ابزارهایی نظیر Nmap استفاده می شود که می تواند اطلاعات زیر را به دست آورد:

- آدرسهای IP قابل دسترسی توسط عموم در شبکه قربانی
- حدسی از سیستم عاملهای، سیستمهای قابل دسترسی
- سرویسهای در دسترس هر یک از IP های کشف شده
- تشخیص محافظت از شبکه قربانی توسط حفاظ و تشخیص نوع آن

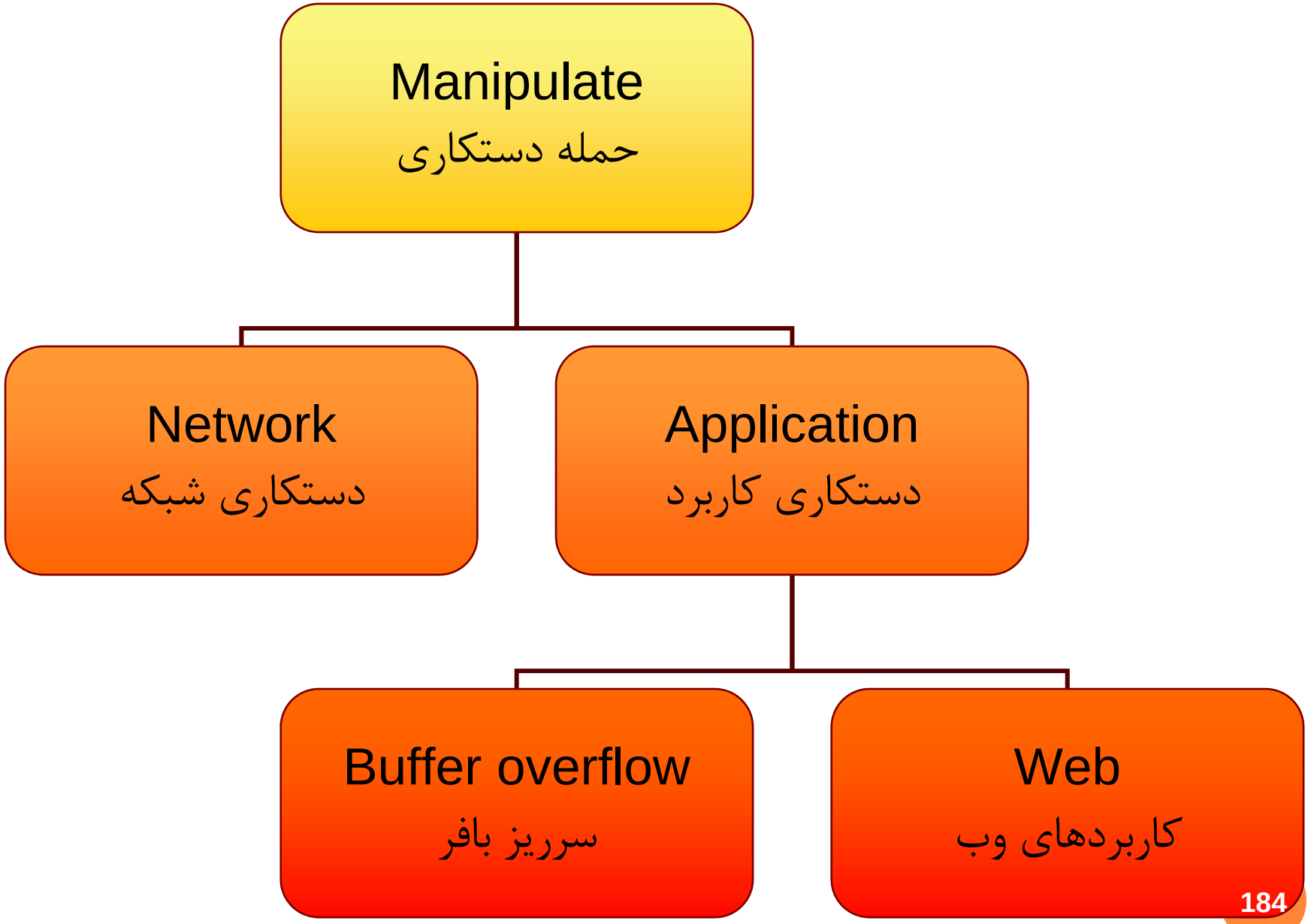

Zenmap
Scan Tools Profile Help
Target: www.google.com www.facebook.com twitt
Profile:
Scan
Cancel
Command: nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com insecure.org slashdot.org craigslist.c
Hosts
Services
OS
Host
72.51.26.227
www.03.01.ash1.t
mh-in-f99.google.
128.121.146.100
www.defcon.org (
www.craigslist.org
www.blackhat.cor
207.46.232.182
youtube.com (208
rr.pmtpa.wikimedi
insecure.org (54.1
slashdot.org (216
scanme.nmap.org
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Save Graphic
youtube.com
74.125.49.38
72.51.26.227
216.187.89.235
72.14.239.251
216.187.88.116
slashdot.org
216.239.49.199
ge-0-3-0-55.wst-64cb-1b.rtwk.msn.net
64.27.160.194
209.85.250.126
209.85.249.32
74.125.49.177
cr1-pos-0-0-0-0.chicago.savvis.net
cr2-pos-0-3-0-1.Seattle.savvis.net
206.108.208.49
www.defcon.org
bpr4-so-4-0-0.SeattleSwitchDesign.savvis.net
64.114.68.174
209.249.11.189.available.above.net
204.225.243.22
192.168.8.
localhos
Action
Interpolation
Frames
60
Polar
Cartesian
Layout
View
address
hostname
icon
Navigation
225.0
Zoom
100
Ring gap
35
Lower ring gap
10

شنود

- مهاجم در این نوع حمله، بسته ها را از روی رسانه در حال انتقال، در حال عبور دریافت می کند. برای اینکه حمله شنود موفقیت آمیز باشد، پروتکلهای مورد استفاده باید داده ها را به شکل رمز نشده منتقل کنند. اطلاعات حاصل از این حمله عبارتند از:
- اطلاعات احراز هویت (گذرواژه)
- الگوهای استفاده از شبکه قربانی
- اطلاعات مدیریت شبکه
- تراکنشهای محرمانه

دسترسی مستقیم

- در این نوع حمله، مهاجم سعی می کند از حفاظها گذشته و به منابع شبکه مستقیماً دسترسی داشته باشد.


Manipulate
حمله دستکاری
Network
دستکاری شبکه
Application
دستکاری کاربرد
Buffer overflow
سرریز بافر
Web
کاربردهای وب

دستکاری شبکه

- معمولترین حمله دستکاری شبکه، تکه تکه سـازی (Fragmentation) بسته های IP است.
- در این حمله، مهاجم عمداً بسته های ترافیک را تکه تکه می کند تا شاید بتواند کنترلهای امنیتی را دور بزند.
- دو نوع حمله دستکاری وجود دارد: دستکاری بسته های حمله، برای مخفی کردن حمله و دستکاری بسته های ترافیک اصلی، برای آسیب رسانی به آنها.

دستکاری کاربرد

- منظور از دستکاری کاربرد، آن دسته از حملاتی است که در لایه هفتم صورت می گیرند و هدف از آنها سوء استفاده از یک نقص امنیتی در طراحی یا پیاده سازی کاربردهاست.

سرریز بافر

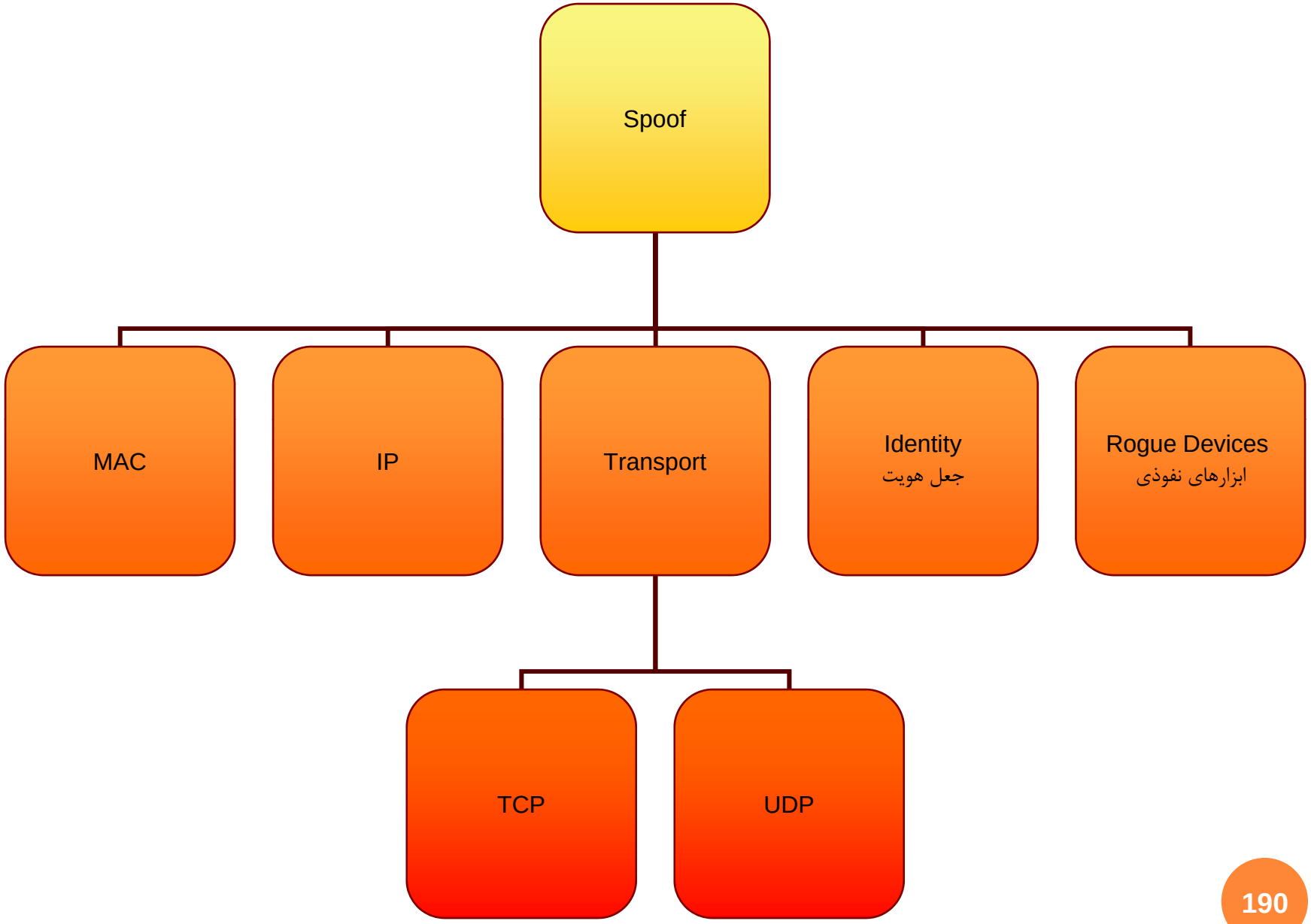
- سرریز بافر معمولترین شکل آسیب پذیری نرم افزاری است. این آسیب پذیری هنگامی رخ می دهد که برنامه نویس شرایط مرزی آدرسهای حافظه مورد استفاده برنامه را به درستی بررسی نکند. این نوع حمله از خطرناکترین حملات است و ضمن اینکه خسارت جدی وارد می کند، مکانیزمی برای کشف آن وجود ندارد.

کاربردهای وب

- حملات به کاربردهای وب متنوعند. اسکریپت های بین سایتی و CGI ناامن دو نمونه از آنهاست. در اسکریپتهای بین سایتی، اگر کاربر روی URL حاوی اطلاعات مضر کلیک کند، کد مخربی اجرا می شود که هدف آن اغلب دزدی اطلاعات است. از اسکریپتهای CGI، برای پردازش فرمهای وب یا انواع URL استفاده می شود، اما اگر به صورت ناامن نوشته شوند و ورودی نادرست را بپذیرند، به مهاجم اجازه می دهند که کدی را روی وب سرور، با سطح دسترسی خود وب سرور، اجرا کند.

حمله جعل

- حملات جعل وقتی رخ می دهند که مهاجم بتواند کاربر یا ابزاری را متقاعد کند که اطلاعات از منشاء مشخصی آمده است، حال آنکه اطلاعات از آن منشاء نیامده باشد. پی ریزی حملات جعل در هر بخشی از شبکه، که احراز هویت وجود نداشته باشد، یا ضعیف باشد، ممکن خواهد بود.


Spoof
MAC
IP
Transport
Identity
جعل هویت
Rogue Devices
ابزارهای نفوذی
TCP
UDP

جعل MAC

- جعل MAC حمله ساده ای است که در آن مهاجم آدرس MAC سیستم خود را به آدرس MAC یکی از سیستمهای مورد اعتماد تغییر می دهد.
- در محیطهای اترنت امروزی که سوییچ شده هستند، جدول CAM (Content Addressing Memory) سوییچ، اطلاعات مربوط به آدرسهای MAC و انتساب آدرسهای MAC به پورتهای سوییچ را نگهداری می کند.
- هرگاه مهاجم آدرس MAC ماشین دیگری را جعل کند، سوییچ فکر می کند که آن ماشین از مکانی به مکان دیگری جابجا شده، و جدول CAM خود را به روز می کند.

جعل MAC

- این به روز رسانی به محض آنکه سیستم مهاجم، فریمی را روی سیم ارسال کند، اتفاق می افتد. از این پس هر ترافیکی که به مقصد این آدرس MAC (و آدرس IP مربوطه) ارسال شود به دست مهاجم می رسد، مگر آنکه سیستم اصلی مجدداً فریمی را ارسال کند. این حمله ، به خصوص در مورد سیستمهایی که بیشتر از ارسال، دریافت می کنند خوب کار می کند.
- برای جلوگیری از این حمله، باید از رکوردهای CAM ایستا استفاده کرد، تا آدرسهای MAC، همواره به پورتهای مشخصی منتسب شوند.

CAM Table

Station	Port1	Port2	Port3	Port4
00-00-3D-1F-11-01			X	
00-00-3D-1F-11-02				X
00-00-3D-1F-11-03	X			

Received Frame

Destination	Source	Data	CRC
00-00-3D-1F-11-05	00-00-3D-1F-11-01		

جعل IP

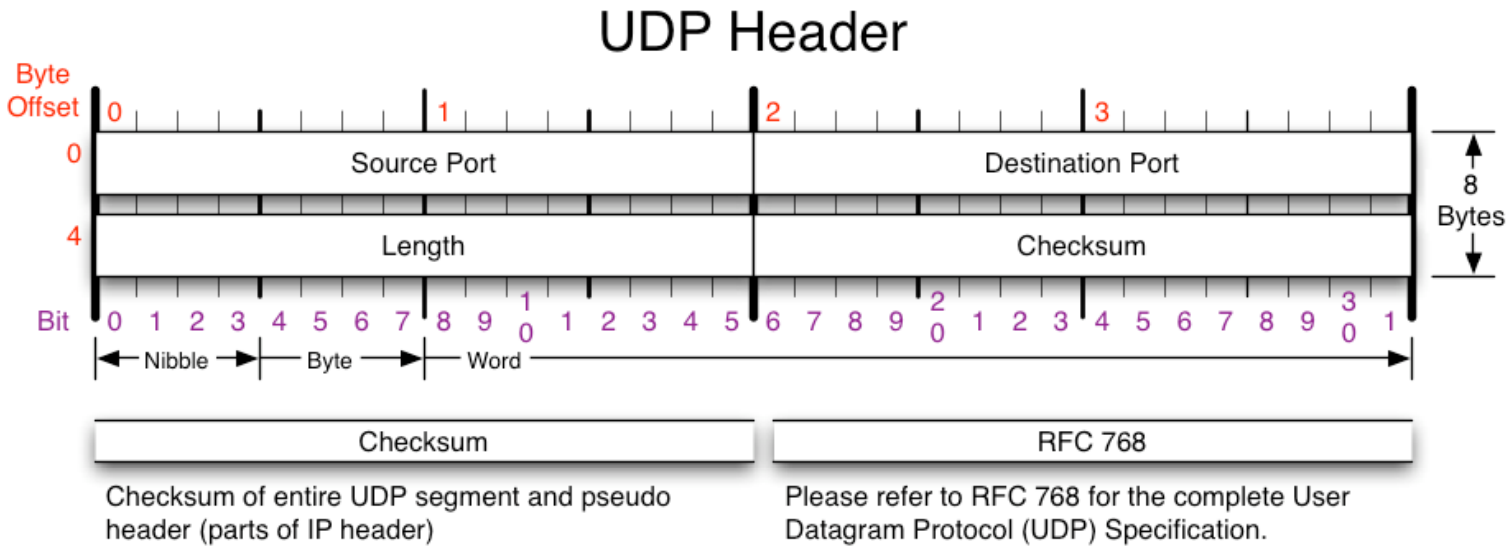
- در این نوع حمله، مهاجم به درایور سازنده بسته های شبکه سیستم، با اختیارات Root، دسترسی پیدا کرده، سپس بسته ای را با Header دلخواه ارسال می کند.
- برای مقابله با این حملات، می توان از رمزنگاری در لایه شبکه استفاده کرد.

جعل در لایه انتقال

- منظور از جعل در لایه انتقال، اجرای موفقیت آمیز جعل ارتباطات در لایه انتقال است.
- حملات اصلی در این خانواده عبارتند از : جعل UDP و جعل TCP

جعل UDP

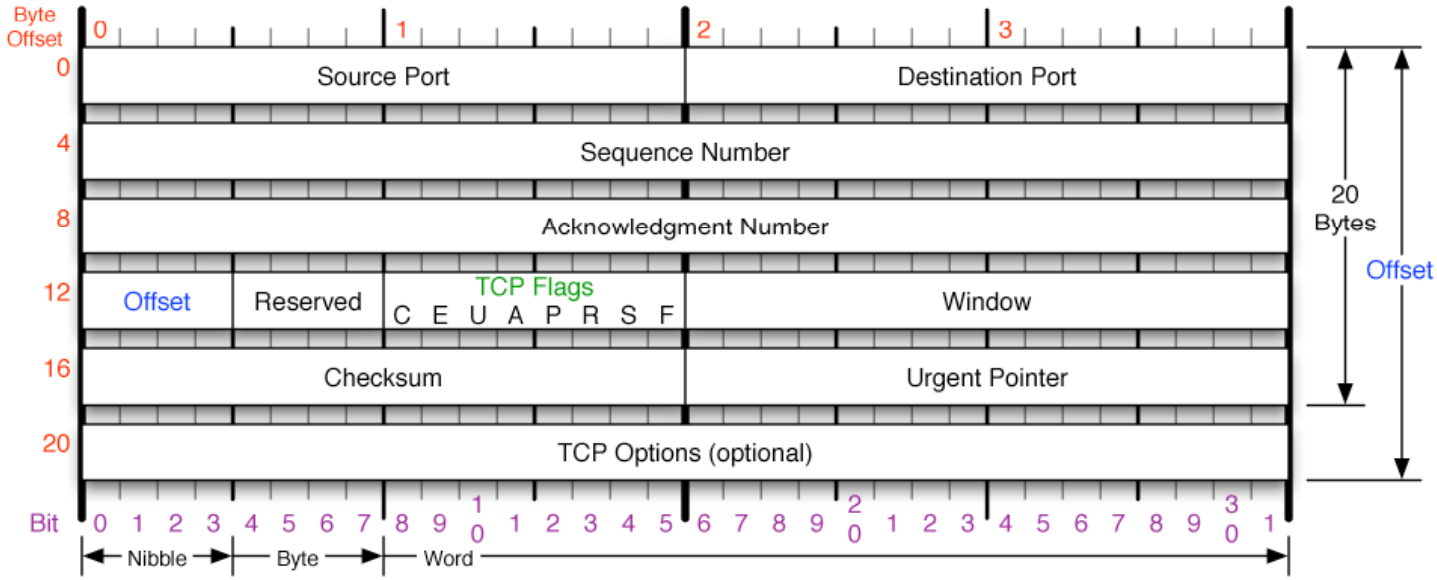
- UDP Header از IP ساده تر است و جعل آن نیز همینطور. با توجه به اینکه UDP پروتکلی نامتصل است بنابراین پیشگیری از جعل UDP تنها در لایه کاربرد امکان پذیر است.



جعل TCP

به دلیل پیچیدگی IP Header ، جعل آن نیز مشکل تر است. مزیت TCP در ماهیت اتصال گرای آن است. TCP از یک توالی شمار (Sequence Number) ۳۲ بیتی، که بر حسب اتصال ممکن است فرق کند، استفاده می کند. تعیین توالی شمار یک اتصال دلخواه بسیار مشکل است (مگر با دسترسی مستقیم به جریان داده ها و شنود اطلاعات). مهاجم برای درج ترافیک خود، در جریان ترافیک، باید توالی شماری را که مورد استفاده سرور است حدس بزند و به طور همزمان، مانع دسترسی کلاینت مشروع به سرور شود. حملات جعل TCP اگر از محلی در مسیر بین کلاینت واقعی و سرور پی ریزی شوند، بسیار خطرناک خواهند بود.

TCP Header



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Reciever Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

جعل هویت

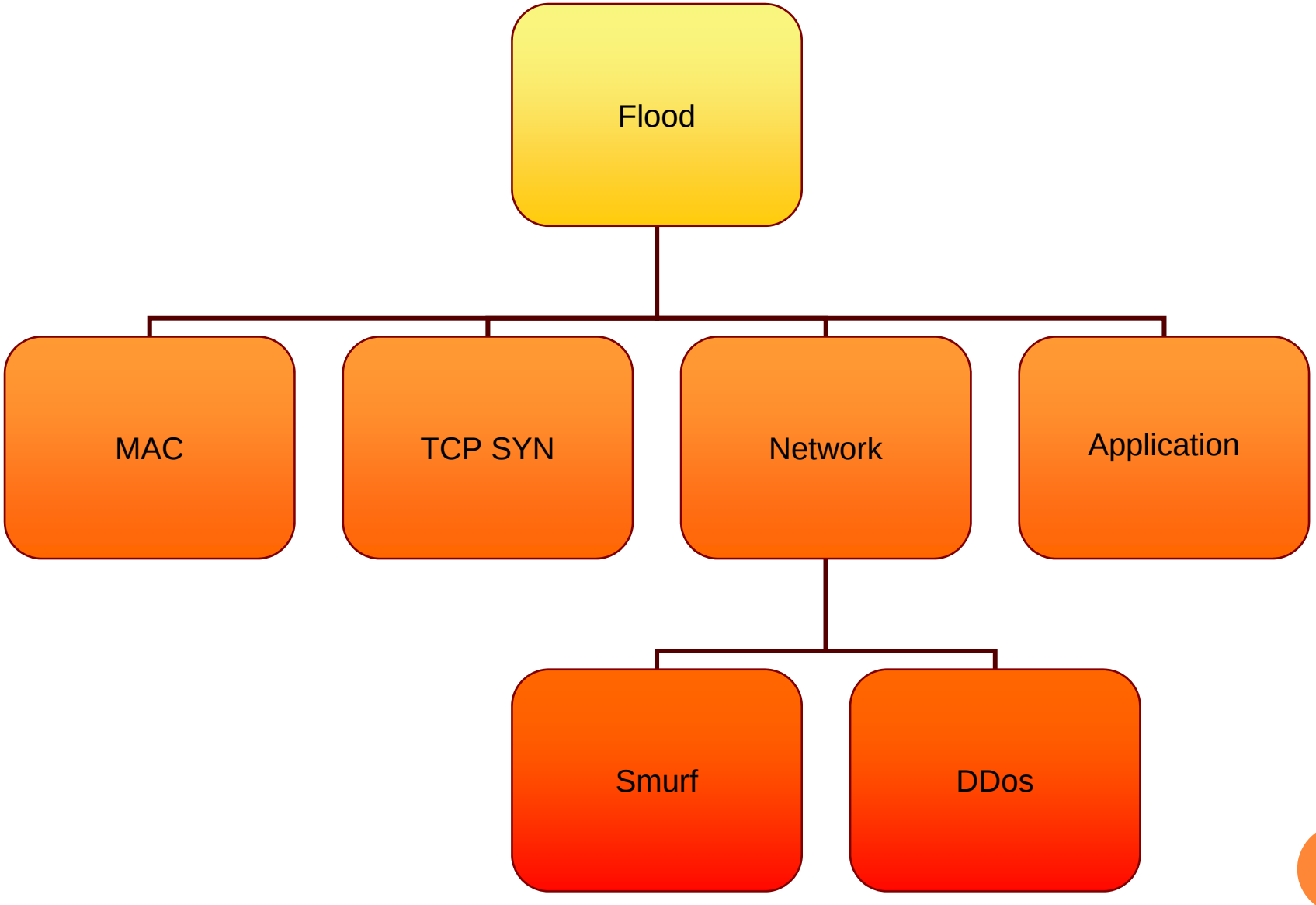
- انواع جعل هویت عبارت است از : شکستن گذرواژه ها، ورود به سیستمها با امتحان کردن تمامی حالات، دزدی گواهی های دیجیتال و تقلید.
- حملات جعل قبلی بیشتر مربوط به هویت شبکه (IP, MAC) بودند، اما مهاجمین بیشتر علاقه دارند به اطلاعات، در لایه کاربرد، که اغلب توسط اطلاعات مربوط به هویت کاربر محافظت شده اند، دست پیدا کند.
- برای جلوگیری از این نوع حملات، از تکنیکهای مختلف رمزنگاری و همچنین الزام کاربران به انتخاب گذرواژه های قوی استفاده می شود.

ابزارهای نفوذی

- در این نوع حمله، مهاجم ابزاری را وارد شبکه می کند و سعی می کند به سایر ابزارها یا کاربران شبکه بقبولاند که این ابزار، ابزار معتبری است.
- این ابزار مثلاً می تواند یک سرور DHCP، یک PC یا ... باشد که از طریق آن امکان اجرای حمله راه دور امکان پذیر است.

حمله سیل

- حملات سیل هنگامی رخ می دهند که مهاجم حجم زیادی از داده ها را به سوی یکی از منابع شبکه (مانند مسیریاب، سوئیچ، سرور، میزبان، کاربرد و ...) ارسال کند.


Flood
MAC
TCP SYN
Network
Application
Smurf
DDos

سیل MAC

- در این نوع حمله، مهاجم بسته های زیادی را با آدرس MAC مبدأ و مقصد جعلی وارد شبکه اترنت می کند. جدول CAM ، که حاوی تناظر آدرسهای MAC شبکه به پورتهای سوییچ است، حجمی محدود دارد. اگر این جدول پر شود، فریمهایی که مقصد آدرس MAC بدون مدخل CAM ارسال شده اند، در تمام پورتهای متعلق به همان VLAN پخش می شوند تا از تحویل فریم به میزبان درست مطمئن شویم. چنین حمله ای به مهاجم اجازه می دهد که این فریمها را شنود کند. درست مثل اینکه مهاجم به جای حضور در یک محیط سوئیچ شده، در یک محیط اشتراکی حضور داشته باشد.

سیل در لایه شبکه

- هدف این حملات، مصرف پهنای باند لینکهای شبکه، به خصوص لینک اینترنت سازمان، که کند و پراهمیت است، می باشد.

SMURF

در ایـن حملـه از بسـته هـای Ping Broadcast (Ping در پروتکـل ICMP وجود دارد) استفاده می کند.

پروتکل IP ویژگیی بـه نـام پخـش جهـت دار (Directed Broadcast) دارد، در این حالت امکان ارسـال بسـته هـای Broadcast از یـک شـبکه برای شبکه دیگری وجود دارد.

مثلاً یک ایستگاه کاری در شبکه 192.0.2.0/24 ممکن است بسته ای را بـه آدرس 192.0.3.255 ارسال کند.

اگر مسیریاب به گونه ای پیکربندی شده باشد که بسته های پخشی جهت دار را عبور دهد، شبکه 192.0.3.0/24 این بسـته را دریافـت کـرده و آن را بـه تمامی ایستگاههای کـاری شـبکه 192.0.3.0/24 ارسـال مـی کنـد. هـر ایستگاه کاری که به گونه ای پیکربندی شده باشد که به بسته هـای پخشـی جواب دهد، چنین خواهد کرد.

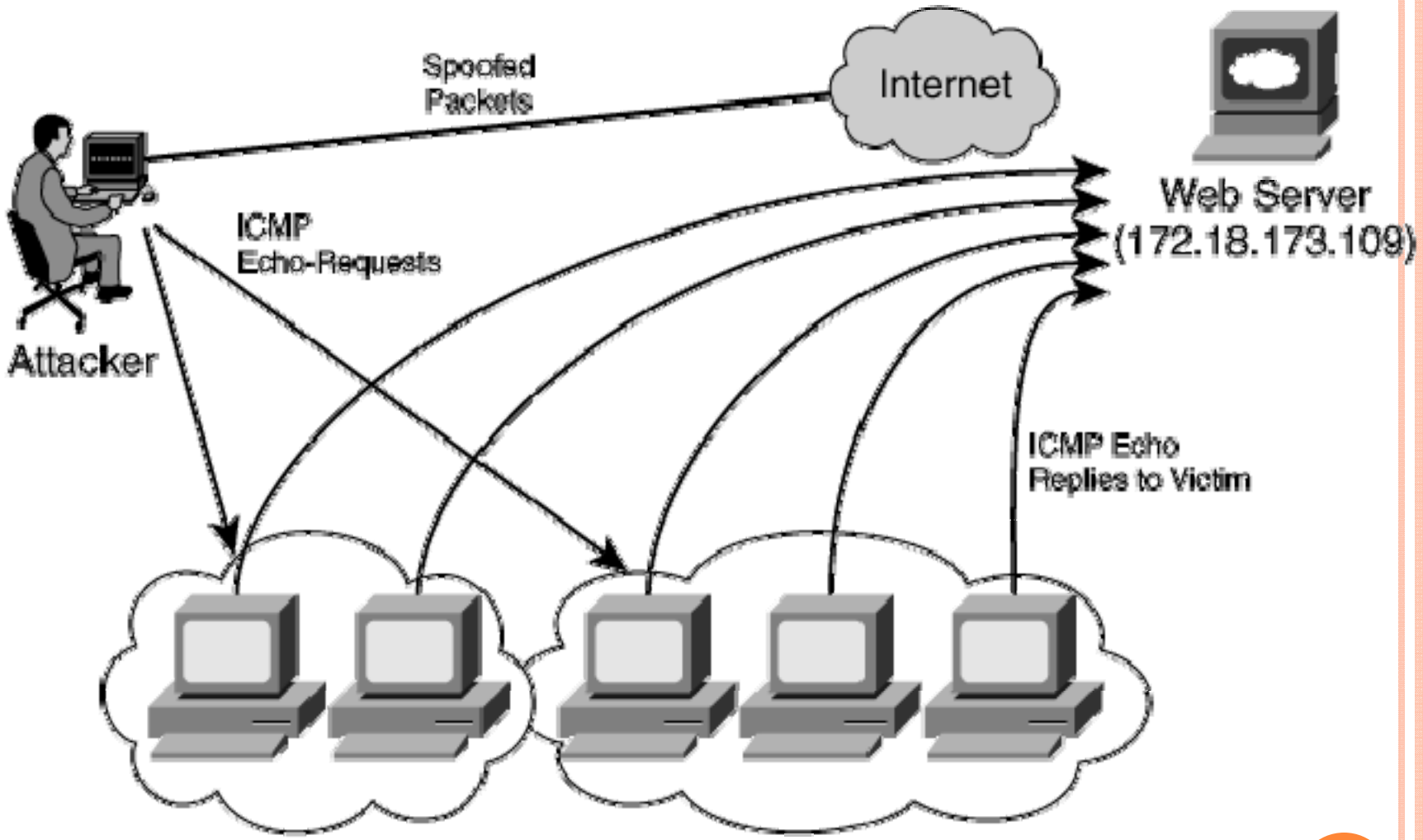
SMURF

- حمله Smurf از این ویژگی استفاده کرده، تا بسته های کوچک Ping با ایجاد پدیده تشدید (Amplification) ، در اثر پاسخ به Ping های مجازی، به حمله ای بزرگ تبدیل شود.
- برای انجام حمله Smurf، مهاجم از طریق یکی از مسیریابها، بسته های ICMP Echo Request را به آدرس پخش شبکه قربانی ارسال می کند. آدرس مبدأ بسته های ICMP (Ping) جعلی است، این آدرس، آدرس یکی از ابزارهای شبکه قربانی است (معمولاً یکی از مسیریابهای واسط)
- حمله Smurf یکی از حملات تشدید است، چون هنگامیکه بسته Ping جعلی به شبکه قربانی می رسد، هر یک از میزبانهای آن شبکه، با یک بسته Ping منحصربفرد به قربانی پاسخ می دهد.

SMURF

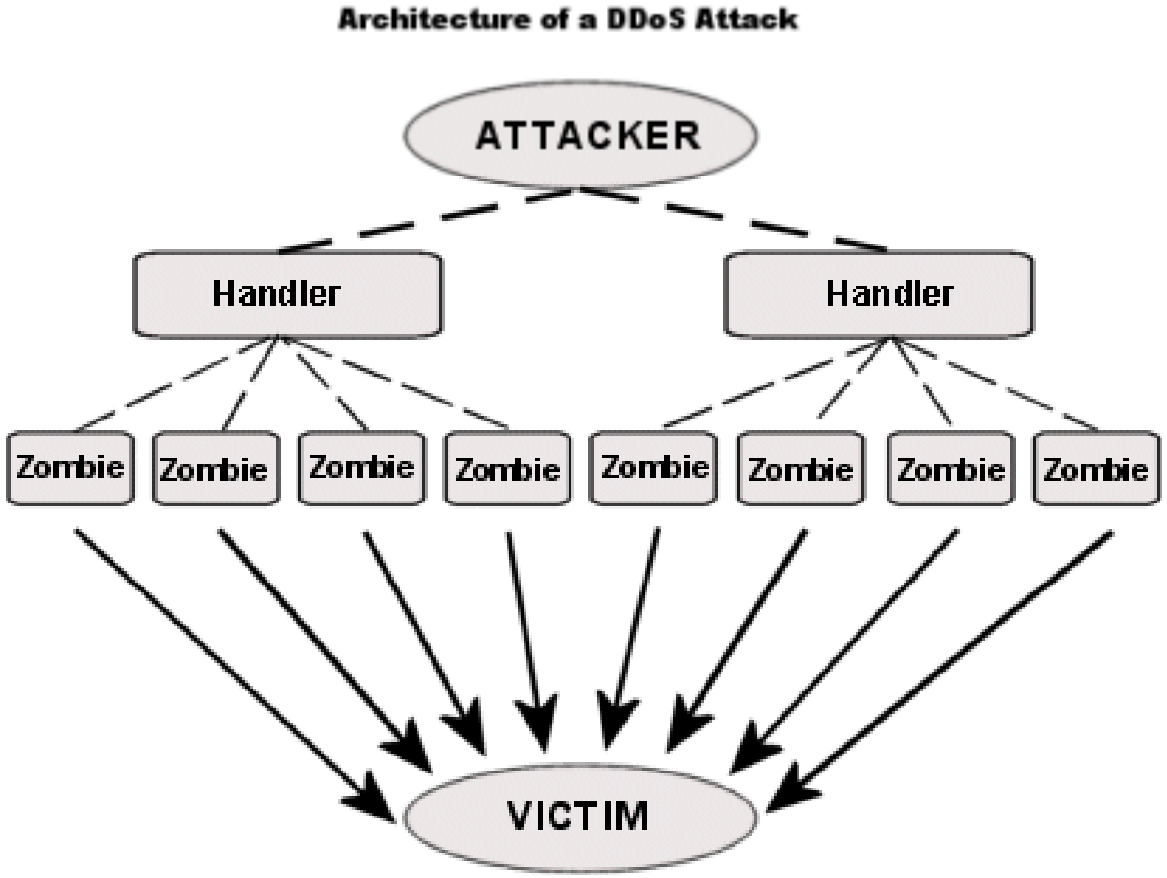
فرض کنید مهاجم قادر باشد بسته های Ping جعلی را با نرخ 768 kbps به شبکه جهشی که ۱۰۰ میزبان دارد ارسال کند. چنین حمله ای سبب می شود که جریانی از بسته ها با نرخ 76.8 Mbps به شبکه قربانی برسد. هر قدر شبکه جهش بزرگتر باشد، تشدید قوی تر خواهد بود.

توجه داشته باشید که پیکربندی مسیریاب با دستور -No ip directed broadcast مانع از آن می شود که شبکه شما مبدأ حمله Smurf باشد، اما از قربانی شدن آن پیشگیری نمی کند. اگر قربانی چنین حمله ای شوید، حجم زیادی از ترافیک ICMP Echo Reply را خواهید دید که باید بوسیله تکنولوژی هایی مانند CAR فیلتر شود.


Spoofed
Packets
Internet
Web Server
(172.18.173.109)
ICMP
Echo-Requests
Attacker
ICMP Echo
Replies to Victim

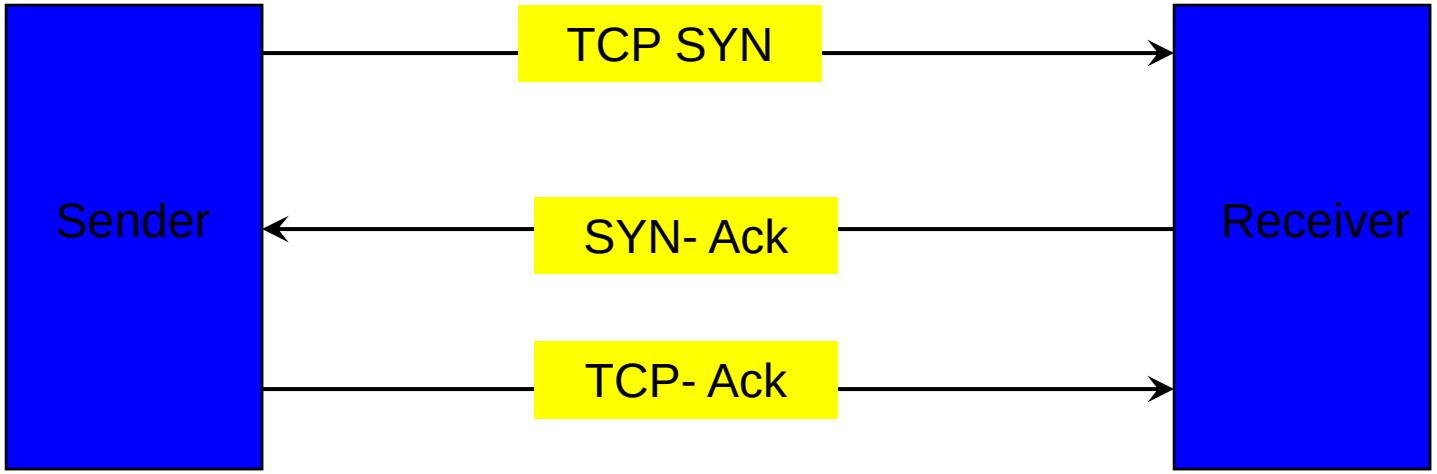
DDOS

در این نوع حمله، مهاجم نرم افـزار مـدیر DDOS (Handler) را بـر روی تعدادی سیستم در اینترنت نصب می کند، سپس این نـرم افزارهـا بـه طـرق مختلفی، مانند اسـتفاده از E-mail هـای حـاوی Trojan و یـا بـا سـوء استفاده از حفره هـای امنیتـی سیسـتم عامـل یـا نـرم افزارهـای کـاربردی، سیستمهای دیگری را به عنوان مأمور (Agent) آلوده می کنند. هـر زمـان کـه مهـاجم بـه Handler هـا فرمـان دهـد، ترافیـک سـنگینی از ناحیـه Agent های آن، روانه IP وب سایت قربانی می شود، بـه نحـوی کـه کـل پهنای باند آن را اشغال کرده و توان پاسخگویی به درخواستهای مشـروع را از دست می دهد.


Architecture of a DDoS Attack
ATTACKER
Handler
Handler
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
Zombie
VICTIM

سیل TCP SYN

لازم است بدانید در پروتکل امن TCP ابتدا فرستنده بسته TCP SYN را برای گیرنده می فرستد. سپس گیرنده پاسخ تأیید (Acknowledge)، SYN-Ack را برای فرستنده می فرستد. آنگاه فرستنده، دریافت تأیید را تأیید (TCP Ack) می کند.



سیل TCP SYN

حملات سیل TCP SYN که جزء اولین حملات سیل به شمار می روند، حجم زیادی از بسته های TCP SYN را برای گیرنده ارسال می کنند اما هیچگاه تأیید SYN-Ack (TCP-Ack) را انجام نمی دهند. در این حالت گیرنده برای مدتی اتصال را باز نگه می دارد تا TCP-Ack را دریافت کند، ضمناً تا چهار بار تأیید SYN-Ack را برای فرستنده می فرستد تا پاسخی دریافت کند در غیراینصورت اتصال بسته می شود.

این حمله موجب پر شدن صف تقاضاهای اتصال سرور گیرنده شده و آنرا از کار می اندازد.

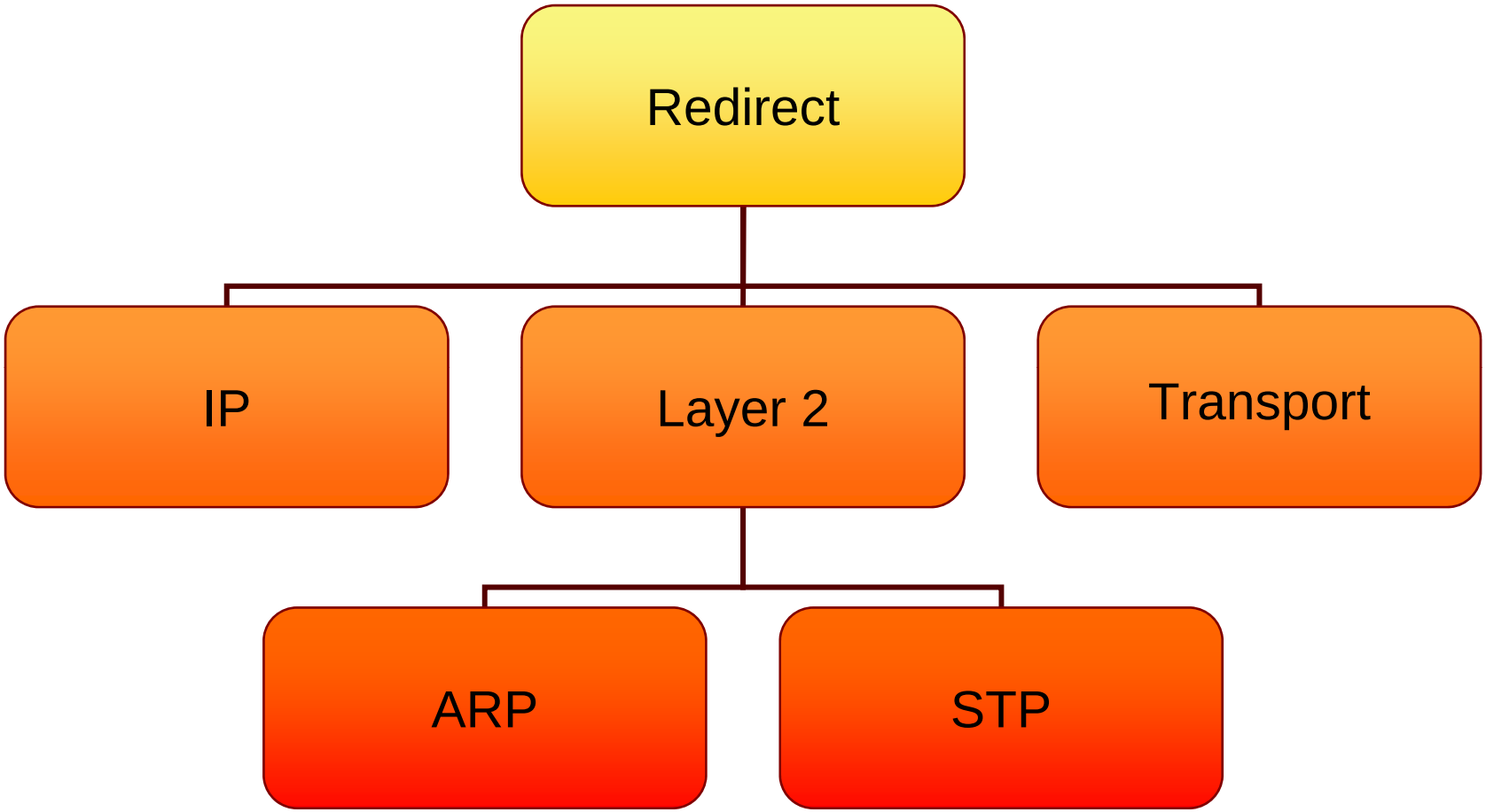
سیل در لایه کاربرد

این حملات موجب مصرف منابع برنامه کاربردی یا سیستم می شوند.

مثلاً ارسال هرزنامه (Spam) ، اجرای برنامه های پردازش بر (Cpu intensive) روی سرور و تولید سیلی از تقاضاهای احراز هویت، بدون خاتمه فرآیند (اتصال برقرار شده و گذرواژه پرسیده می شود، اما پاسخی از ناحیه درخواست شده، داده نمی شود)

حمله هدایت

در این نوع از حملات، مهاجم سعی دارد جریان اطلاعات یک شبکه را تغییر دهد. این کار در تمامی لایه ها امکان پذیر است، اما در L2، IP و لایه انتقال، به امنیت شبکه مربوط است.


Redirect
IP
Layer 2
Transport
ARP
STP

هدایت در L2

حملات هدایت از طریق ARP یا STP قابل اجرا هستند.

هدایت / جعل ARP

این حمله، همان جعل ARP است که در واقع، هدایت را با جعل ARP انجام می دهد.

قبلاً با نام جعل MAC آنرا بررسی کردیم.

هدایت STP

- STP (Spanning Tree Protocol)

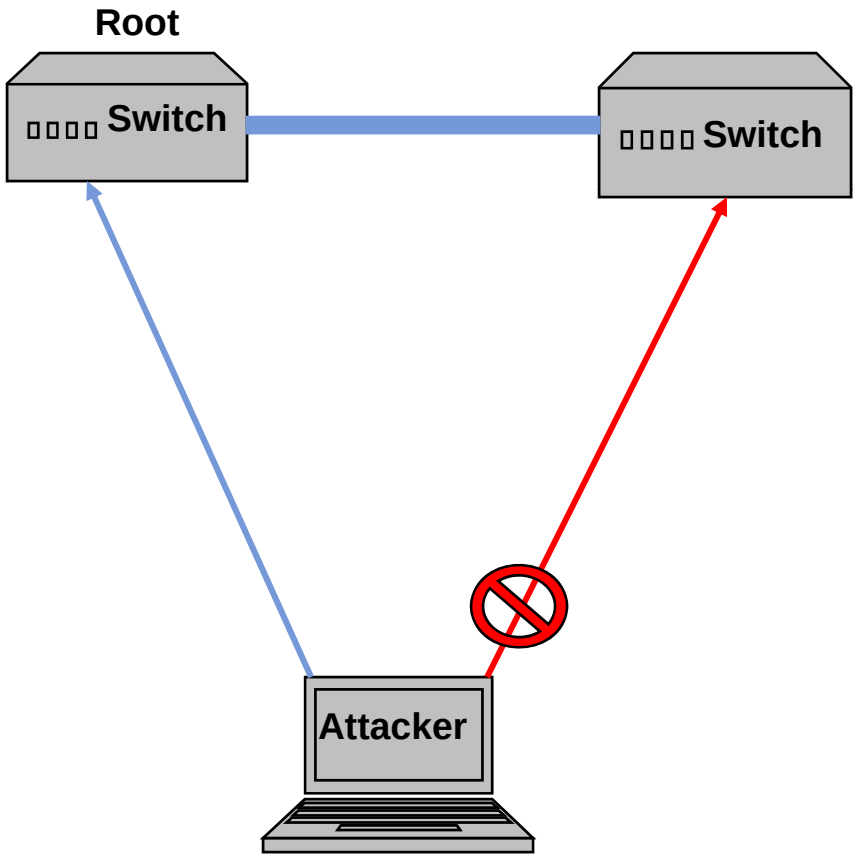
پروتکل درخت فراگیر (STP) ، روشی برای جلوگیری از ایجاد دور (Loop) در لایه ۲ می باشد. در صورتیکه از STP استفاده نشود ممکن است از طریق یکسری لینک تکراری L2 دور تشکیل شده و کارایی شبکه را به شدت کاهش دهد.

در این نوع حملات، مهاجم با جعل هویت ایستگاه کاری خود، با سوییچی با ماکزیمم اولویت، وضعیت به هم بندی شبکه در STP را تغییر داده و تمام ترافیک شبکه را از خود عبور می دهد.

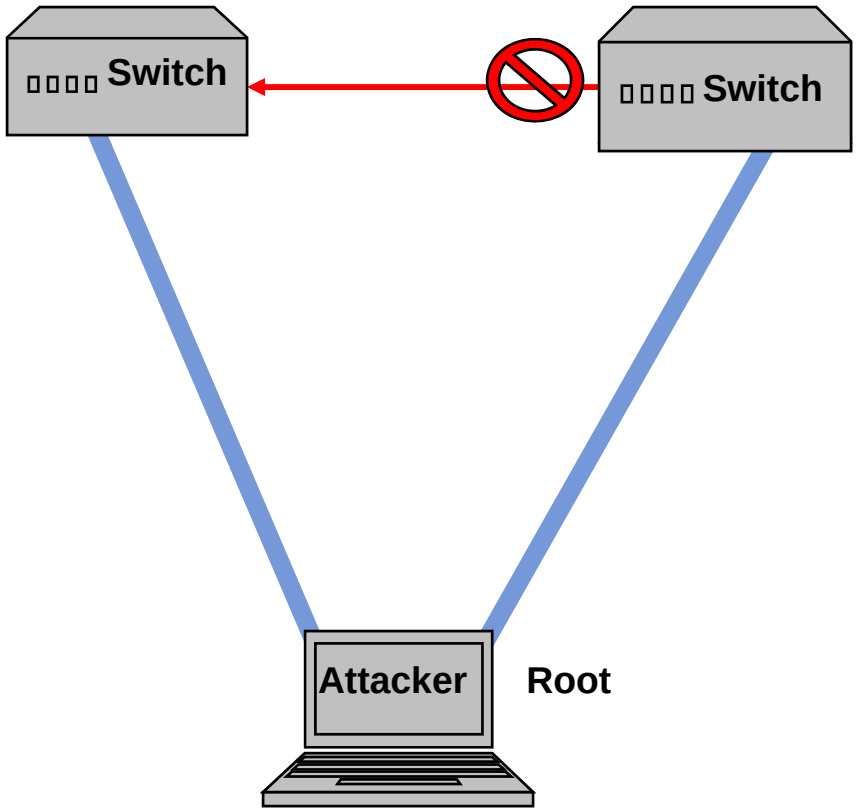
مهاجم از طریق بسته های پیکربندی سوییچ، ایستگاه کاری خود را یک سوییچ با بالاترین اولویت معرفی می کند، بنابراین همه ترافیک از سیستم مهاجم عبور می کند.

هدایت STP

در شکل اولیه روبرو، STP مانع از ایجاد لینک سمت راست، که باعث دور است، می شود.



هدایت STP



مهاجم، ایستگاه کاری خـود را بـه عنـوان سوییچی با بـا لاتـرین اولویـت معرفـی کرده، و STP ارتباط دو سوییچ واقعی را قطع کرده، کل جریـان را از ایسـتگاه کاری مهاجم عبور می دهد.

ضمن اینکه ارتباط به شدت کند می شود، ضمناً امکـان هـر نـوع حملـه ای بـرای مهاجم فراهم می شود.

هدایت IP

حمله هدایت IP می تواند جریان اطلاعات را به دو طریق تغییر دهد:

1. وارد کردن یک مسیریاب نفوذی، که اطلاعات غلط را در شبکه تبلیغ می کند.
2. تغییر پیکربندی مسیریابهای موجود

معمولترین استفاده از این حمله، هدایت ترافیک به محل مورد نظر مهاجم است، به نحوی که مهاجم پیش از ارسال بتواند اطلاعات را خوانده، یا تغییر دهد.

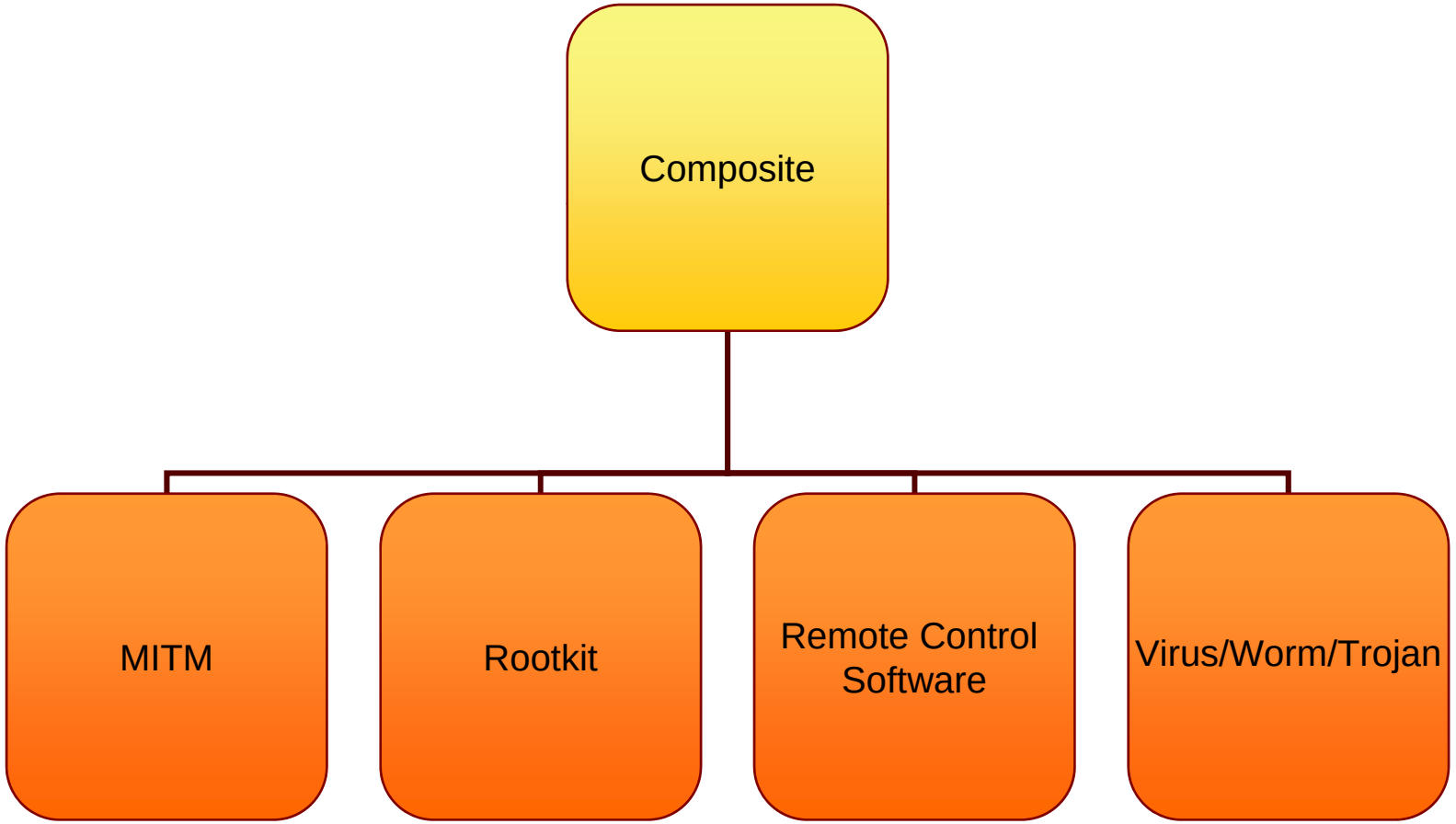
هدایت در لایه انتقال

این حمله، هدایت پورت نیز نامیده می شود. یکی از ابزارهای متداول این حمله، Netcat می باشد.

مهاجم ابتدا یک سرور عمومی در شبکه مقصد را تسخیر کرده، سرور Netcat را روی آن نصب می کند. (این سرور قادر است، درخواستها به آن سیستم و پورت مشخصی از آنرا، به سیستم و پورت دیگری هدایت کند.)

سپس مهاجم درخواستی را روی سرور تسخیر شده Netcat بر روی پورت مشخصی می فرستد. آنگاه سرور Netcat درخواست را به پورت مشخص سیستم دیگری می فرستد. در نتیجه با این عمل مهاجم با واسطه سرور تسخیر شده، به سیستم مقصد دست پیدا می کند.

حملات ترکیبی



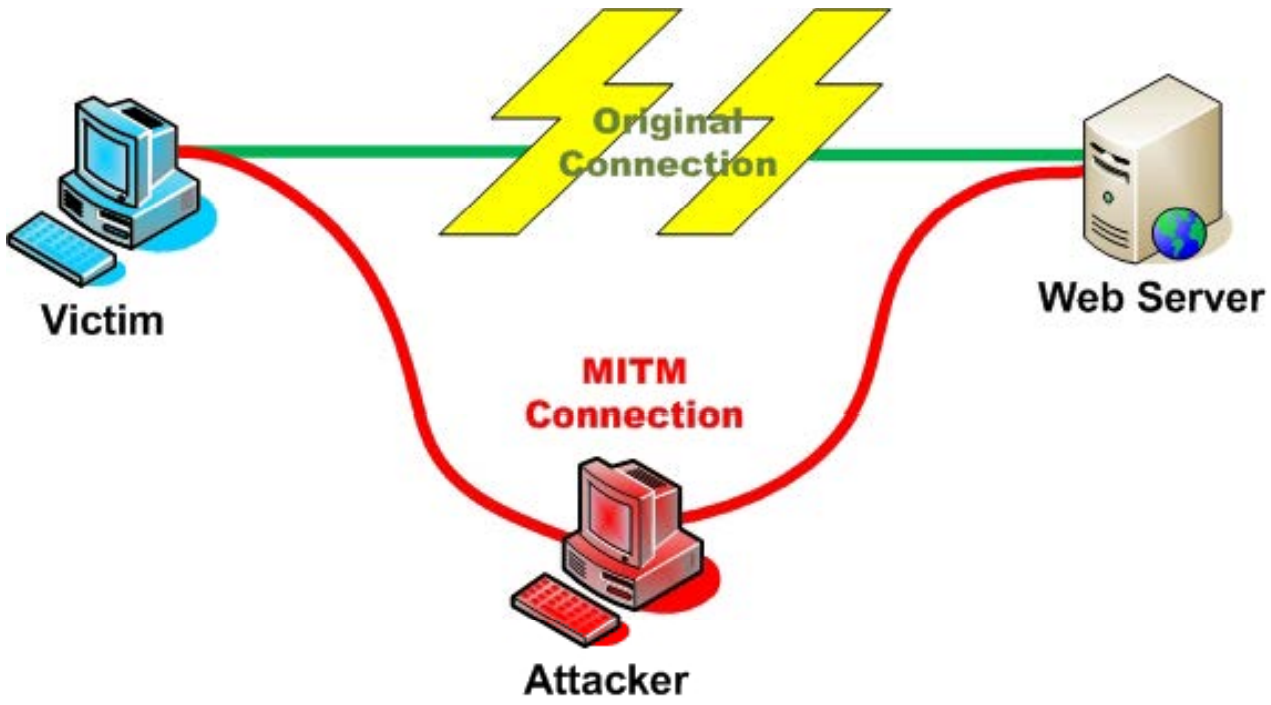
مرد میانی (MITM)

- Man In The Middle

منظور از حمله "مرد میانی" ، حمله ای است که در آن، مهاجم کنترل فعالی بر بالاترین لایه ارتباطی بین دو قربانی دارد. این لایه اغلب لایه هفتم است.

مثال سنتی از حمله MITM، مکالمه یک مشتری بانک است. مشتری تصور می کند که دارد با بانک صحبت می کند، و بانک تصور می کند که دارد با مشتری صحبت می کند. اما در حقیقت مکالمات هر دو از سیستم مهاجم می گذرد و او اطلاعاتی نظیر شماره حساب، رقمهای نقل و انتقال مالی و نظایر آن را تغییر می دهد.

بهترین روش مقابله با حملات MITM، استفاده از رمزنگاری است.


Original
Connection
Victim
Web Server
MITM
Connection
Attacker

VIRUSES ویروسها

ویروس ها یک برنامه یا کد(اسکریپت) بسیار کوچکی است که بر روی برنامه های بزرگتر سوار می شوند. یعنی در بین کد های اصلی یا فایل های اصلی یک برنامه دیگر که معمولا پر کاربرد می باشد قرار می گیرند و به محض نصب برنامه اصلی، خود را وارد کامپیوتر شخص قربانی می کنند و هنگام اجرای برنامه به طور خود کار اجرا شده و شروع به تخریب (کارهایی که نویسنده ویروس از آن خواسته) می کنند.

مشخصه اساسی ویروسهای کامپیوتری

تمام ویروسها دارای سه مشخصه اساسی زیر می باشند:

۱) روشی برای تکثیر و پخش خود در دیگر کامپیوترها.

۲) انجام دادن عملیاتی خاص در کامپیوتر (مثلا در تاریخی مشخص).

۳) از کار افتادن برنامه پس از انجام عملیاتی خاص از قبیل نمایش یک پیغام کاملا بی ضرر مانند " "Free Frodo تا از بین بردن تمام محتویات هارد.

ویروسها بر حسب نحوه ورود به کامپیوتر به دو گروه مقدماتی تقسیم می شوند. گروه اول برنامه هایی هستند که دارای پسوندهای .. SYS, EXEو COMبوده و می توانند از طریق E-Mailوارد Notepadموجود در Windowsگردند. گروه دوم از طریق دیگر برنامه های فرعی وارد کامپیوتر شده و یکی از اهداف آنها آسیب رساندن به بوت سکتورها (Boot Sector) است.

ویروسی که در یک برنامه پنهان شده است با هر بار اجرای برنامه راه اندازی می شود بطور مثال اگر ویروس همراه برنامه Wordشما باشد با هر بار استفاده ،ویروس موجود در آن راه اندازی می شود.

در صورتیکه ویروس هایی که درون بوت سکتورها ذخیره شده باشند با هر بار روشن شدن کامپیوتر فعال می شوند.

یک ویروس ممکن است پس از فعال سازی درون حافظه RAMنفوذ کرده و به دیگر برنامه ها سرایت کند به طور مثال تعداد دفعات راه اندازی خود را محاسبه کرده و در صورتیکه این تعداد به رقم ۱۰۰ رسید تمام اطلاعات کامپیوتر را پاک کند یا ممکن است حافظه RAMرا از طریق تکثیر خود پر کرده و سرعت عملیاتی کامپیوتر را تا حد بالایی پایین بیاورد.

ویروسها، کرمها و اسب های تروا

ویروس، کد مخربی است که نرم افزارهای موجود روی سیستم را آلوده کرده، تغییر داده یا از بین می برد.

انجام چنین کاری اغلب به انجام عملی از سوی کاربر نیاز دارد.

کرم (Worm)، ابزار مستقلی است که سیستمهای آسیب پذیر را آلوده می کند. سیستمهای آلوده هم به نوبه خود، سایر سیستمهای آسیب پذیر را آلوده می کنند. اغلب کرمها به طور خودکار در شبکه پخش می شوند، هر چند گاهی شروع حمله به انجام عملی از سوی کاربر نیاز دارد.

اسب تروا (Trojan horse)، برنامه ای است که برای کاربر ابزار مفیدی به نظر می رسد، حال آنکه در حقیقت حاوی کد مخربی است. موضوع متفاوت در مورد تروا‌ها این است که کاربر،به دست خود آنها را وارد سیستمش می کند.

ROOTKIT

ابزارهای اختفاء

ابزارهای اختفاء، به مهاجم اجازه می دهند تا حضور خود را در سیستمهای تسخیر شده مخفی نگاه دارد.

نرم افزار کنترل از راه دور

امروزه اکثر سیستمهای عامل، جهت سهولت کار، ابزارهای کنترل از راه دور را دارند.

مهاجم می تواند با الحاق نرم افزار به یک Email ، یا از طریق تروا‌ها، نرم افزار مربوطه را فعال و کنترل سیستم را به دست گیرد. در اینصورت امکان پایه ریزی هر حمله دیگری ممکن می شود.

مشکلات شبکه بندی امن

به دلایل زیر هیچگاه نمی توانیم امنیت ٪۱۰۰ را در یک شبکه ایجاد کنیم:

1. مدیریت امنیت و تشخیص ترافیک خوب از بد با دقت ٪۱۰۰ ممکن نیست، ضمناً امکان گزارش گیری از تمام ابزارهای شبکه، به خصوص در یک شبکه بزرگ، کار بسیار مشکلی است.
2. نظارت بر هویت در لایه های مختلف شبکه، کار مشکلی است.
3. با افزایش اندازه شبکه، استفاده از بعضی تکنولوژی های امنیتی، سبب کاهش چشمگیر کارایی می شود.
4. در بعضی موارد، استاندارد های امنیتی شبکه وجود ندارد.

مشکلات شبکه بندی امن

5. کامپیوترها سیستمهای پیچیده ای هستند که هر بخش از آنها توسط سازنده ای ایجاد شده و ترکیب این سیستمهای پیچیده در شبکه، محیط بسیار پیچیده ای ایجاد می کند، که دشمن امنیت شبکه است.
6. اغلب سیستمها، در حالت اولیه ناامن فروخته می شوند و این وظیفه مدیر سیستم است که فرآیند وقت گیر و خطا خیز مقاوم سازی را طی کند.
7. خیلی اوقات، به دلیل کاربرد ناصحیح، حتی با اینکه فناوری وجود دارد، اما از آن استفاده نمی شود.

فناور های امنیتی

1. فناوری های هویت
2. امنیت میزبان و کاربرد
3. حفاظهای شبکه
4. فیلترینگ محتوا
5. NIDS
6. رمزنگاری

فناوری های هویت

هدف اصلی فناوری های هویت، تأیید هویت کاربر (یا کامپیوتر) در شبکه است.

1. گذرواژه های چند بار مصرف
2. RADIUS و TACAS+
3. OTP
4. PKI
5. کارتهای هوشمند
6. معیارهای زیستی

گذرواژه های چند بار مصرف

گذرواژه های چند بار مصرف تنها وقتی مفیدند که سیاستهای مناسبی برای انتخاب گذرواژه وجود داشته و کاربران این سیاستها را رعایت کنند.

بهتر است توسط ابزارهایی که قوت گذرواژه ها را امتحان می کنند، پیش از انتخاب، گذرواژه های کاربران تست شود.

ضمناً بهتر است روی سرور احراز هویت، تعداد دفعات ورود گذرواژه را محدود کنیم تا امکان جستجو از مهاجم گرفته شود.

RADIUS و TACAS+

هر دو مورد فوق، پروتکلهایی هستند که خدمات احراز هویت مرکزی، را در یک شبکه ممکن می سازند. مبنای کار هر دو پروتکل، بر وجود سروری مرکزی استوار است که شامل پایگا ه داده ای از نامهای کاربری، گذرواژه ها و حقوق دسترسی است. هرگاه ابزاری بخواهد کاربر را احراز هویت کند، اطلاعات کاربر به سرور مرکزی فرستاده شده و پاسخ سرور مشخص می کند که آیا کاربر اجازه دسترسی به آن را دارد یا خیر.

سرورهای RADIUS و TACAS+ ،اغلب سرورهای AAA نامیده می شوند.

Authentication	احراز هویت
Authorization	مجاز شناسی
Accounting	حسابرسی

- Authentication
  - مشخص می کند شما چه کسی هستید.
- Authorization
  - مشخص می کند که شما مجاز به انجام چه کارهایی هستید.
- Accounting
  - مشخص می کند که شما چه کرده اید. (ثبت وقایع)
- RADIUS
  - استانداردی است که توسط انواع ابزارها از سازندگان مختلف پشتیبانی می شود.
- TACAS+
  - توسط سیسکو طراحی شده و تنها روی ابزارهای سیسکو اجرا می شود.

ONE TIME PASSWORD OTP

اکثر OTP ها، بر مبنای احراز هویت با دو معیار، (Two factor authentication) عمل می کنند: معیار اول چیزی است که شما دارید (جواز/ نرم افزار شما)، و معیار دوم چیزی است که شما می دانید (PIN code) .

روش تولید و همگام سازی گذر واژه، بسته به سیستم OTP تفاوت می کند. در یکی از روشهای معمول، کارت جواز در دوره های زمانی مشخص (معمولاً هر ۶۰ ثانیه) کد عبور (Passcode) را صادر می کند. این کد که کاملاً تصادفی به نظر می رسد، بر مبنای الگوریتم ریاضی پیچیده ای، که هم روی سرور و هم روی کارت جواز اجرا می شود، تولید شده است.

OTP

OTP ها در موارد زیر بر گذرواژه ها برتری دارند:

- کاربران دیگر نمی توانند گذرواژه های ضعیف انتخاب کنند.
- کاربران کافی است PIN را به خاطر بسپارند و دیگر نیازی به به خاطر سپردن گذرواژه های قوی نیست.
- گذرواژه های شنود شده، به دلیل یکبار مصرف بودن، چندان به درد بخور نیستند.

دلایلی که هنوز OTP جای گذرواژه های عادی را نگرفته:

- کاربر باید کارت جواز را، برای احراز هویت، به همراه داشته باشد.
- OTP به سروری اضافی نیاز دارد که درخواستها را از سرور احراز هویت دریافت کند.
- وارد کردن گذرواژه با استفاده از OTP، بیشتر از وارد کردن گذرواژه های عادی طول می کشد.
- OTP در شبکه های بزرگ گران تمام می شود.

PUBLIC KEY INFRASTRUCTURE PKI

PKI مکانیزمی است برای توزیع گواهی های دیجیتال (که بیانگر هویت کاربران است) به کار می رود. گواهی های دیجیتال، کلیدهای عمومی هستند که توسط مراکز صدور گواهی (CA: Certificate Authority) امضاء شده اند. مراکز CA تأیید می کنند که یک گواهی دیجیتال به یک شخص یا سازمان خاص تعلق دارد.

روش PKI به دو دسته باز (Open) و بسته (Close) تقسیم می شوند.

در سیستم PKI باز، شما مجبورید به سازمانهای بیرونی اعتماد کنید، در حالیکه در سیستم PKI بسته، CA در داخل خود سازمان است و به همین دلیل امنیت آن بالاتر است.

کارتهای هوشمند

SMART CARDS

کارتهای هوشمند مجهز به حافظه و پردازنده هستند و از طریق یک واسط سریال (Serial Interface) با یک دستگاه کارت خوان ارتباط برقرار می کنند.

می توان از کارتهای هوشمند برای ذخیره اطلاعات هویت استفاده کرد. دستگاه کارت خوان به PC متصل شده و کاربران را احراز هویت می کند. کارتهای هوشمند محل امنی برای ذخیره کلید خصوصی به شمار می روند. اما این کارتها نیز می توانند در معرض حمله قرار گیرند. ضمناً هزینه پیاده سازی این روش در یک سازمان نیز بالاست.

BIOMETRICS

معیارهای زیستی

از معیارهای زیستی، مانند تشخیص صدا، اثر انگشت، تشخیص چهره و اسکن عنبیه چشم می توان به عنوان معیاری برای تشخیص هویت استفاده کرد. مزیت این روش اینست که کاربر نیازی به همراه داشتن و به خاطر سپردن چیزی را ندارد.

اشکالات این روش اینست که:

- فناوری جدید بوده و هنوز به بلوغ نرسیده است.
- اطلاعات زیستی قابل تغییر یا ابطال نیست بنابراین با به دست آوردن این اطلاعات عملیات جعل هویت به سادگی امکان پذیر است.

- اگر شما از اطلاعات زیستی در چند سیستم استفاده کنید، مهاجم می تواند با نفوذ به ناامن ترین سیستم ، اطلاعات شما را به دست آورده و به سیستم های دیگر نفوذ کند.

معمولاً با استفاده از PIN امنیت این روش را بالاتر می برند.

امنیت میزبان و برنامه کاربردی

امنیت میزبان و برنامه کاربردی از طریق فناوری هایی تأمین می شود که روی سیستمهای نهایی (End systems) اجرا شده و از طریق سیستم عامل، سیستم فایل و برنامه های کاربردی محافظت می کند.

این فناوری ها عبارتند از:

- بررسی یکپارچگی سیستم فایل
- حفاظهای میزبان
- HIDS
- ضد ویروسهای میزبان

بررسی یکپارچگی سیستم فایل
FILE SYSTEM INTEGRITY CHECKING

از طریق این فناوری امکان جلوگیری از حملات وجود ندارد، اما با اجرای یک تابع درهم ساز (Hash) روی فایلهای مهم سیستم و محاسبه چکیده محتوای آنها، در صورت تغییر این فایلها امکان کشف تغییر فراهم می شود.

حفاظهای میزبان
HOST BASED FIREWALLS

نصب حفاظ روی PC ها، بسته به پیکربندی آنها، می تواند تا حدی امنیت را به ارمغان بیاورد.

معمولاً حفاظها کاربر را از درخواست یک برنامه برای ارتباط با شبکه آگاه می کنند و از او کسب اجازه می نمایند.

HIDS
Host Intrusion Detection System

HIDS برای کشف یا پیشگیری از حملات به میزبانها طراحی شده است.

به دلیل هزینه بالا امکان نصب HIDS ها روی تمام میزبانها وجود ندارد بنابراین فقط روی سیستم های مهم نصب می شوند.

ضد ویروسهای میزبان

HOST ANTIVIRUS

ضد ویروسها یکی از مهمترین فناوری ها در امنیت کامپیوترها به شمار می روند. از این فناوری باید بر روی تمام میزبانها و تمام سرورهای شبکه استفاده کرد.

ضد ویروسها با استفاده از تطابق مشخصات ویروس با علائم موجود در پایگاه داده خود، عملیات تشخیص، پاکسازی فایل آلوده یا قرنطینه کردن آن را انجام می دهند. اما ویروسهای صفر روزه (Zero day) به دلیل جدید بودن ویروس و عدم وجود اطلاعات آن در پایگاه داده می توانند دردسر آفرین باشند. به هر حال ضد ویروسها به اندازه به روز رسانی آنها مفید و قابل اطمینان هستند.

فیلترینگ FILTERING

- **فیلتر اینترنتی** یا **فیلترینگ**، عبارت است از محدود کردن دسترسی کاربران اینترنت به وب سایتها و خدمات اینترنتی که از دیدگاه متولیان فرهنگی و سیاسی هر کشور برای مصرف عموم مناسب نیست، اعمال فیلتر به وسیله ارائه‌دهندگان خدمات اینترنتی انجام می‌شود ولی تعیین سطح، مصادیق و سیاست‌های فیلترینگ با حکومت‌هاست.
- کشورهای بلاروس، میانمار، چین، کوبا، مصر، ایران، کره شمالی، عربستان، سوریه، تونس، ترکمنستان، ازبکستان، و ویتنام از بزرگ‌ترین فیلتر کنندگان اینترنت در جهان هستند.

مبانی فیلترینگ در اینترنت

کامپیوتر یک صفحه وب را درخواست می‌کند.

این درخواست در ابتدا به ISP و از آنجا به شبکهٔ محلی فرستاده می‌شود.

قبل از این که درخواست از شبکه محلی به سروری که صفحه مورد نظر بر روی آن قرار گرفته‌است ارسال شود توسط سیستم فیلتر کننده بررسی می‌گردد.

سیستم فیلتر کننده کلیه درخواست‌ها را با لیستی که در بانک اطلاعاتی دارد مقایسه می‌کند که اصطلاحا به آن لیست سیاه می‌گویند. این لیست از سه جزء تشکیل شده‌است:

- آدرس دامین (Domain Address)
- آدرس IP (IP Address)
- کلمات کلیدی (Keywords)

اگر هیچ یک از کلمات و آدرس‌های موجود در لیست سیاه در درخواست شما وجود نداشته باشد، این درخواست تمیز (Clean) در نظر گرفته می‌شود. در غیر این صورت، درخواست آلوده (Dirty) تشخیص داده شده و بلوک می‌شود.

انواع فیلترینگ

- **فیلترینگ ازطریق DNS**
- سرویس DNSنام هر Domainرا به IPآدرس متناظرش ترجمه می‌کند.آدرس سروری که سرویس DNSرا ارائه می‌دهد، به طور اتوماتیک و در هنگام برقراری اتصال به اینترنت از طریق ISPدر اختیار کامپیوتر شما گذاشته می‌شود. اگر این سرور DNS، سانسور کننده باشد کلیه درخواست‌ها برای سایت‌های غیرمجاز را بی پاسخ می‌گذارد.
- **فیلترینگ به وسیلهٔ پروکسی**
- در این روش ISPدسترسی مستقیم به اینترنت را محدود کرده و شما را ملزم به استفاده از پروکسی می‌کند.باید در تنظیمات مرورگر، آدرس پروکسی سروری را که ISPداده را وارد کنید. کلیهٔ درخواست‌ها به پروکسی فرستاده می‌شود و در صورت مجاز بودن درخواست، پروکسی آن را از اینترنت گرفته و برایتان ارسال می‌کند.

- **فیلتر کردن به کمک مسیریاب ها**
- در قسمت انتهایی شبکه (Gateway)، مسیر یاب طوری تنظیم می‌شود که ترافیک خروجی شبکه را به سمت یک سیستم فیلتر کننده منحرف کند.کلیهٔ درخواست‌ها از این سیستم عبور داده می‌شوند و در صورت وجود سایت‌های غیر مجاز، جریان اطلاعات بلوک می‌شود.
- **فیلترینگ به کمک سانسورافزارها**
- این نرم‌افزارها بیشتر در منزل (برای کنترل والدین بر فرزندان)، مدارس و دانشگاهها استفاده می‌شوند. مانند : Net Nanny، Cyber sitter، Cyber portal

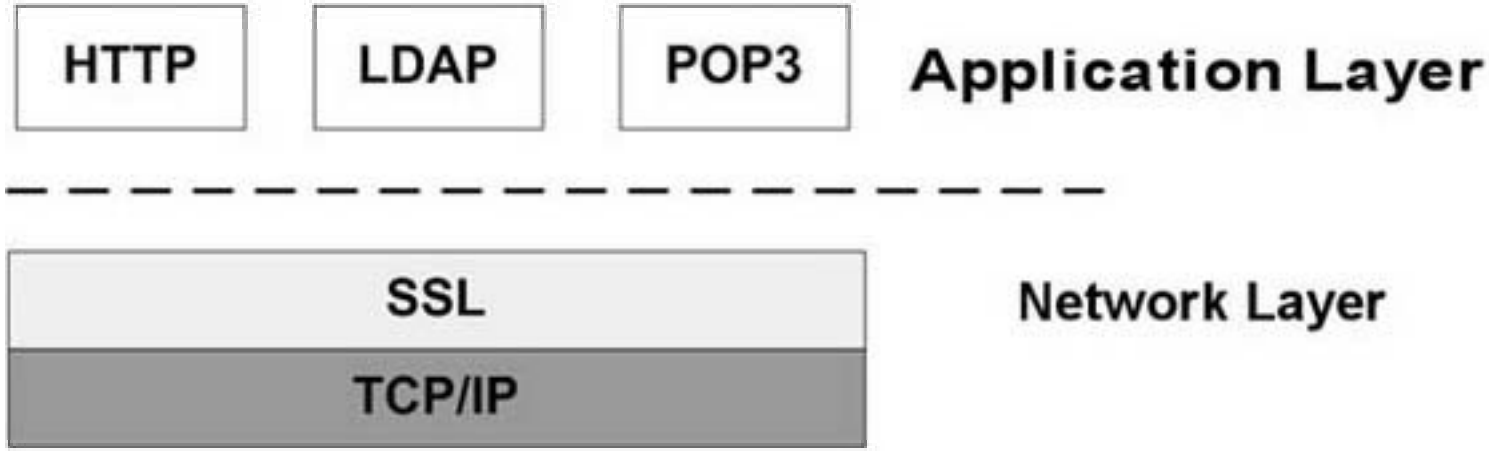
- **فیلترینگ به کمک مسدود کردن پورتها**
- پورتها مانند درهایی هستند که سرور از طریق آنها سرویسهایش را ارائه میدهد.اگر پورتی بلوک شود تمام سرویسهایی که از طریق آن پورت ارائه می‌گردد، غیر قابل دسترس می‌باشد. بیشتر پورتهای ۸۰، ۳۱۲۸، ۸۰۸۰ مسدود می‌شوند، زیرا پورت‌های متداول برای پروکسیها هستند.
- **لیست سیاه و لیست سفید**
- لیست سیاه : شامل آدرس مجموعه سایت‌هایی است که دسترسی به آن‌ها مجاز نمی‌باشد. گاهی هم از کلمات کلیدی استفاده می‌شود به طوری که اگر در سایت مورد درخواست این کلمات وجود داشته باشد، بلوک می‌شود.

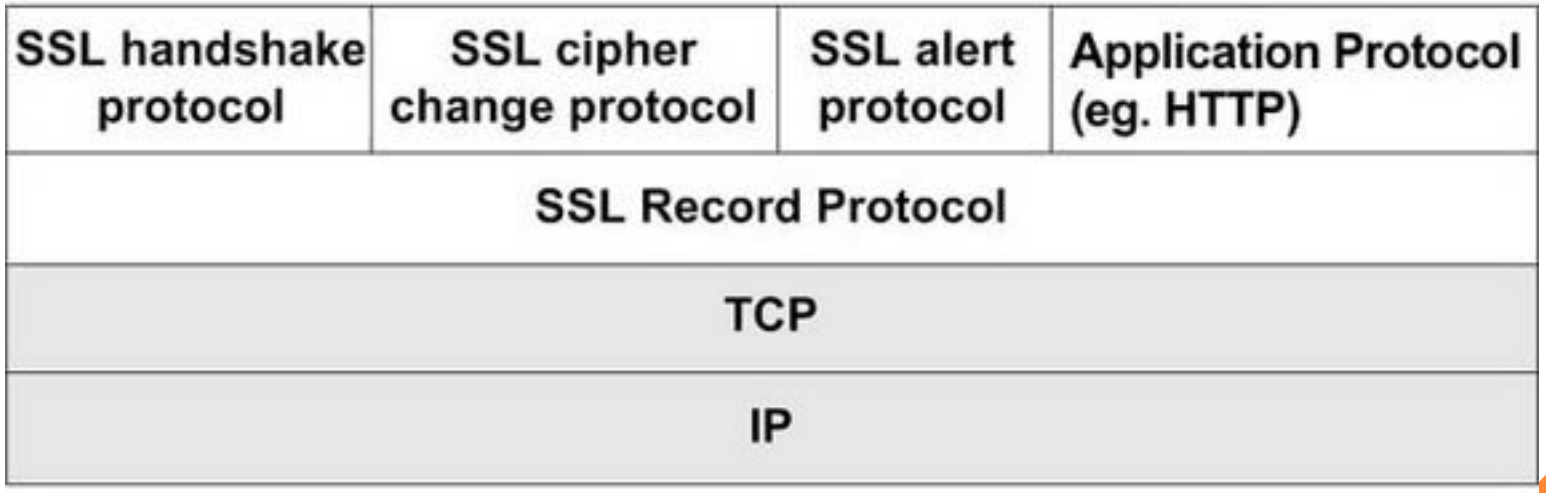
لیست سفید : شامل آدرس مجموعه سایت‌هایی است که دسترسی به آنها مجاز می‌باشد. در سازمان‌هایی استفاده می‌شود که می‌خواهند کارمندانشان فقط به تعداد معدودی سایت دسترسی داشته باشند.

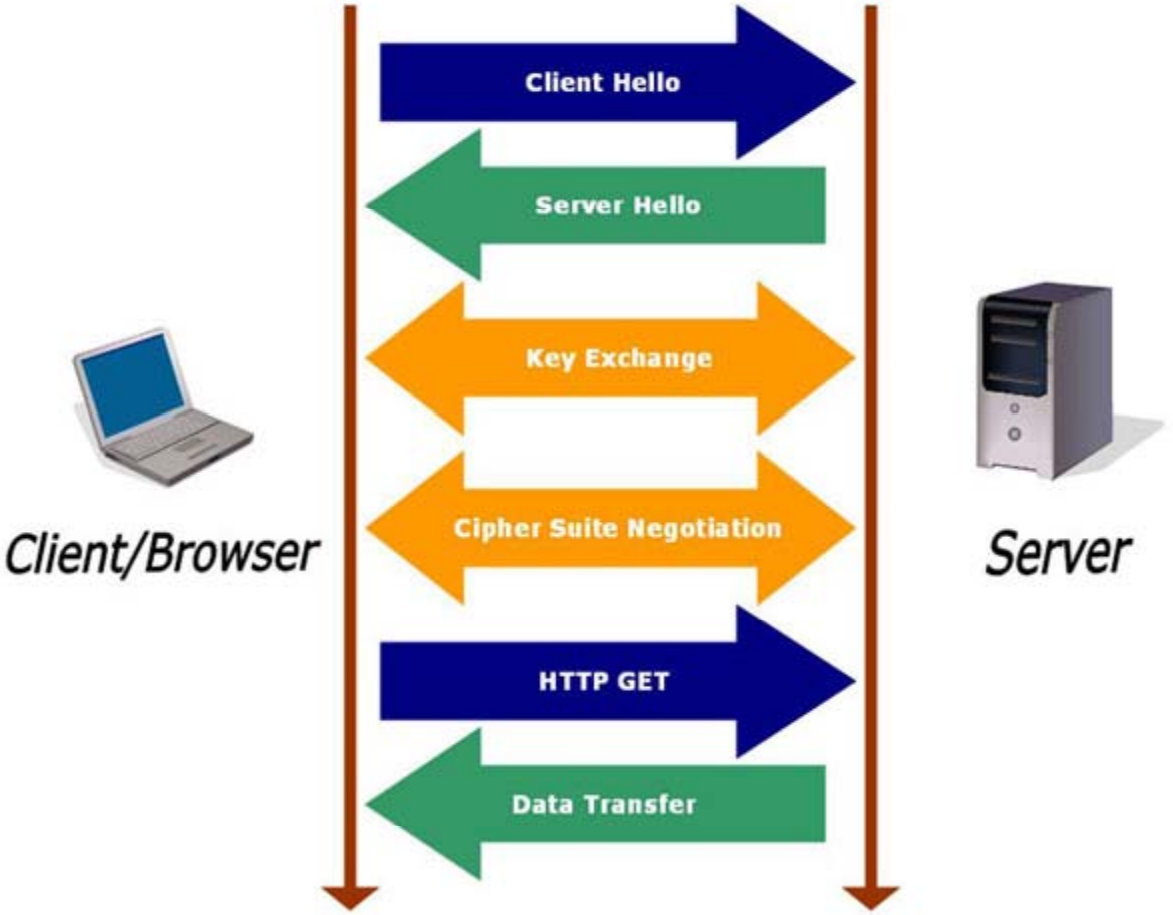
- **فیلترینگ معکوس**
- این نوع فیلترینگ در مقصد انجام می‌شود. سرور شرکت ارائه دهندهٔ خدمات، قبل از ارائهٔ هر گونه سرویسی، ابتدا IPمشتری را چک می‌کند و در صورتی که متعلق به یک کشور تحریم شده باشد، از ارائهٔ سرویس سرباز می‌زند.

SECURE SOCKET LAYER SSL

راه‌حلی جهت برقراری ارتباطات ایمن میان یک سرویس‌دهنده و یک سرویس‌گیرنده است که توسط شرکت Netscape ارایه شده است. در واقع SSL پروتکلی است که پایین‌تر از لایه کاربرد (لایه ۴ از مدل TCP/IP) و بالاتر از لایه انتقال (لایه سوم از مدل TCP/IP) قرار می‌گیرد.


HTTP
LDAP
POP3
Application Layer
SSL
TCP/IP
Network Layer


SSL handshake protocol
SSL cipher change protocol
SSL alert protocol
Application Protocol (eg. HTTP)
SSL Record Protocol
TCP
IP


Client Hello
Server Hello
Key Exchange
Cipher Suite Negotiation
HTTP GET
Data Transfer
Client/Browser
Server

مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده آن برای امن کردن پروتکل‌های غیرامن لایه کاربردی نظیر HTTP، IMAP،LDAP و... می‌باشد که براساس آن الگوریتم‌های رمزنگاری بر روی داده‌های خام (plain text) که قرار است از یک کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول کانال انتقال تضمین می‌کند.

به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس‌دهنده و سرویس‌گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند، البته غیر از این‌کار می‌بایست تضمین کند که اگر اطلاعات حین انتقال مورد سرقت قرار گرفت، برای رباینده قابل درک و استفاده نباشد که این‌کار را با کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می‌دهد.

ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL

برای داشتن ارتباطات امن مبتنی بر SSL عموماً به دو نوع گواهی دیجیتال SSL یکی برای سرویس‌دهنده و دیگری برای سرویس‌گیرنده و یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA نیاز می‌باشد. وظیفه CA این است که هویت طرفین ارتباط، نشانی‌ها، حساب‌های بانکی و تاریخ انقضای گواهینامه را بداند و براساس آن‌ها هویت‌ها را تعیین نماید.

مکانیزم‌های تشکیل‌دهنده SSL

- **تأیید هویت سرویس‌دهنده**

با استفاده از این ویژگی در SSL، یک کاربر از صحت هویت یک سرویس‌دهنده مطمئن می‌شود. نرم‌افزارهای مبتنی بر SSL سمت سرویس‌گیرنده (مثلاً یک مرورگر وب نظیر Internet Explerer از تکنیک‌های استاندارد رمزنگاری مبتنی بر کلید عمومی و مقایسه با کلیدهای عمومی یک سرویس‌دهنده (مثلاً یک برنامه سرویس‌دهنده وب نظیر IIS) می‌تواند از هویت او مطلع شود و پس از اطمینان کامل، کاربر می‌تواند نسبت به وارد نمودن اطلاعات خود مانند شماره کارت‌های اعتباری و یا گذرواژه‌ها اقدام نماید.

- **تأیید هویت سرویس‌گیرنده**

برعکس حالت قبلی در اینجا سرویس‌دهنده است که می‌بایست از صحت هویت سرویس‌گیرنده اطمینان یابد. طی این مکانیزم، نرم‌افزار مبتنی بر SSL سمت سرویس‌دهنده پس از مقایسه نام سرویس‌گیرنده با نام‌های مجاز موجود در لیست سرویس‌گیرنده‌های مجاز که در داخل سرویس‌دهنده تعریف می‌شود و در صورت وجود، اجازه استفاده از سرویس های مجاز را به او می‌دهد.

- **ارتباطات رمز شده**

کلیه اطلاعات مبادله شده میان سرویس‌دهنده و گیرنده می‌بایست توسط نرم‌افزارهای موجود در سمت سرویس‌دهنده و سرویس‌گیرنده رمزنگاری (Encrypt) شده و در طرف مقابل رمزگشایی (Decrypt) شوند تا حداکثر محرمانگی (Confidentiality) در این‌گونه سیستم‌ها لحاظ شود.

اجزای پروتکل SSL

پروتکل SSL دارای دو زیر پروتکل تحت عناوین زیر می‌باشد.

۱- SSL Rocord Protocol که نوع قالب‌بندی داده‌های ارسالی را تعیین می‌کند.

۲- SSL Handshake Protocol که براساس قالب تعیین شده در پروتکل قبلی، مقدمات ارسال داده‌ها میان سرویس‌دهنده‌ها و سرویس‌گیرنده‌های مبتنی بر SSL را تهیه می‌کند.

بخش‌بندی پروتکل SSL به دو زیر پروتکل دارای مزایای چندی است. از جمله:

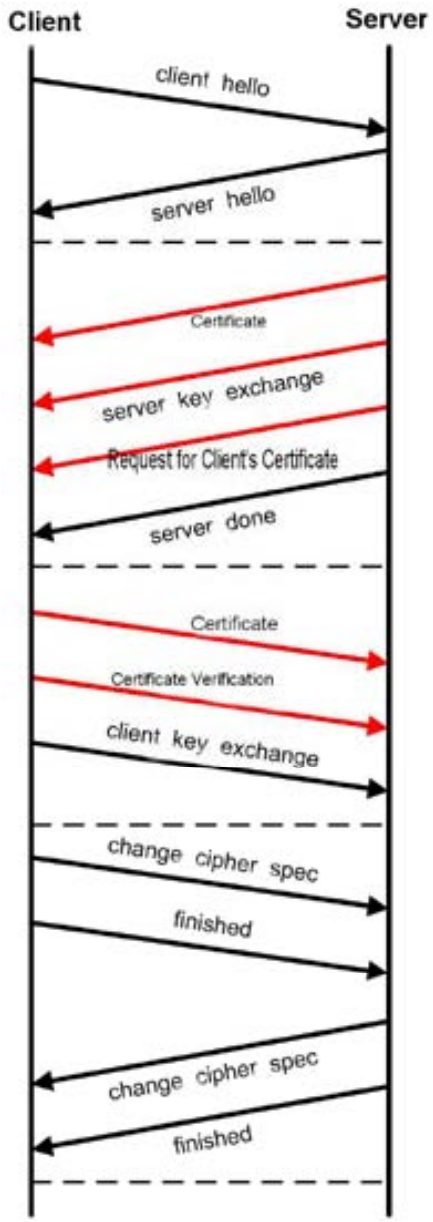
اول: در ابتدای کار و طی مراحل اولیه ارتباط (Handshake) هویت سرویس‌دهنده برای سرویس‌گیرنده مشخص می‌گردد.

دوم: در همان ابتدای شروع مبادلات، سرویس‌دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری تبادلی توافق می‌کنند.

سوم: در صورت لزوم، هویت سرویس گیرنده نیز برای سرویس‌دهنده احراز می‌گردد.

چهارم: در صورت استفاده از تکنیک‌های رمزنگاری مبتنی بر کلید عمومی، می‌توانند کلیدهای اشتراکی مخفی را ایجاد نمایند.

پنجم: ارتباطات بر مبنای SSL رمزنگاری می‌شوند.


Client
Server
client hello
server hello
Certificate
server key exchange
Request for Client's Certificate
server done
Certificate
Certificate Verification
client key exchange
change cipher spec
finished
change cipher spec
finished

الگوریتم‌های رمزنگاری پشتیبانی شده درSSL

در استانداردSSL ، از اغلب الگورتیم‌های عمومی رمزنگاری و مبادلات کلید (Key Exchcenge Algorithm) نظیر DES، DSA، KEA، RC2، MD5، RC4، RSA و RSA Key Exchauge، SHA-1، Skipjack و DES۳ پشتیبانی می‌شود و بسته به این‌که نرم‌افزارهای سمت سرویس‌دهنده و سرویس‌دهنده نیز از موارد مذکور پشتیبانی نمایید، ارتباطاتSSL می‌تواند براساس هر کدام این از الگوریتم‌ها صورت پذیرد. البته بسته به طول کلید مورد استفاده در الگوریتم و قدرت ذاتی الگوریتم می‌توان آن‌ها را در رده‌های مختلفی قرار دارد که توصیه می‌شود با توجه به سناریوهای موردنظر، از الگوریتم‌های قوی‌تر نظیر DES۳ با طول کلید ۱۶۸ بیت برای رمزنگاری داده‌ها و همچنین الگوریتم SHA-۱ برای مکانیزم‌های تأیید پیغام MD ۵ استفاده شود و یا این‌که اگر امنیت در این حد موردنیاز نبود، می‌توان در مواردی خاص از الگوریتم رمزنگاری RC ۴ با طول کلید ۴۰ بیت و الگوریتم تأیید پیغام MD ۵ استفاده نمود.

نحوه عملکرد داخلی پروتکلSSL

همان‌طور که می‌دانید SSL می‌تواند از ترکیب رمزنگاری متقارن و نامتقارن استفاده کند. رمزنگاری کلید متقارن سریع‌تر از رمزنگاری کلیدعمومی است و از طرف دیگر رمزنگاری کلید عمومی تکنیک‌های احراز هویت قوی‌تری را ارایه می‌کند. یک جلسه SSL (SSL Session) با یک تبادل پیغام ساده تحت عنوان SSL Handshake شروع می‌شود. این پیغام اولیه به سرویس‌دهنده این امکان را می‌دهد تا خودش را به سرویس‌دهنده دارای کلید عمومی معرفی نماید و سپس به سرویس‌گیرنده و سرویس‌دهنده این اجازه را می‌دهد که یک کلید متقارن را ایجاد نمایند که برای رمزنگاری‌ها و رمزگشایی سریع‌تر در جریان ادامه مبادلات مورد استفاده قرار می‌گیرد.

گام‌هایی که قبل از برگزاری این جلسه انجام می‌شوند براساس الگوریتم RSA Key Exchange عبارتند از:

۱- سرویس‌گیرنده، نسخه SSL مورد استفاده خود، تنظیمات اولیه درباره نحوه رمزگذاری و یک داده تصادفی را برای شروع درخواست یک ارتباط امن مبتنی بر SSL به سمت سرویس‌دهنده ارسال می‌کند.

۲- سرویس‌دهنده نیز در پاسخ نسخه SSL مورد استفاده خود، تنظیمات رمزگذاری و داده تصادفی تولید شده توسط خود را به سرویس‌گیرنده می‌فرستد و همچنین سرویس‌دهنده گواهینامه خود را نیز برای سرویس‌گیرنده ارسال می‌کند و اگر سرویس‌گیرنده از سرویس‌دهنده، درخواستی داشت که نیازمند احراز هویت سرویس‌گیرنده بود، آن را نیز از سرویس‌گیرنده درخواست می‌کند.

۳- سپس سرویس‌گیرنده با استفاده از اطلاعاتی که از سرویس‌دهنده مجاز در خود دارد، داده‌ها را بررسی می‌کند و اگر سرویس‌دهنده مذکور تأیید هویت شد، وارد مرحله بعدی می‌شود و در غیراین‌صورت با پیغام هشداری به کاربر، ادامه عملیات قطع می‌گردد.

۴- سرویس‌گیرنده یک مقدار به نام Premaster Secret را برای شروع جلسه ایجاد می‌کند و آن را با استفاده از کلید عمومی (که اطلاعات آن معمولاً در سرویس‌دهنده موجود است) رمزنگاری می‌کند و این مقدار رمز شده را به سرویس‌دهنده ارسال می‌کند.

۵- اگر سرویس‌دهنده به گواهینامه سرویس‌گیرنده نیاز داشت می‌بایست در این گام برای سرویس‌دهنده ارسال شود و اگر سرویس‌گیرنده نتواند هویت خود را به سرویس‌دهنده اثبات کند، ارتباط در همین‌جا قطع می‌شود.

۶- به محض این‌که هویت سرویس‌گیرنده برای سرویس‌دهنده احراز شد، سرویس‌دهنده با استفاده از کلید اختصاصی خودش مقدار Premaster Secret را رمزگشایی می‌کند و سپس اقدام به تهیه مقداری به نام Master Secret می‌نماید.

۷- هم سرویس‌دهنده و هم سرویس‌گیرنده با استفاده از مقدار master Secret کلید جلسه (Session Key) را تولید می‌کنند که در واقع کلید متقارن مورد استفاده در عمل رمزنگاری و رمزگشایی داده‌ها حین انتقال اطلاعات است و در این مرحله به نوعی جامعیت دادها بررسی می‌شود.

۸- سرویس‌گیرنده پیغامی را به سرویس‌دهنده می‌فرستد تا به او اطلاع دهد، داده بعدی که توسط سرویس‌گیرنده ارسال می‌شود به وسیله کلید جلسه رمزنگاری خواهد شد و در ادامه، پیغام رمز شده نیز ارسال می‌شود تا سرویس‌دهنده از پایان یافتن Handshake سمت سرویس‌گیرنده مطلع شود.

۹- سرویس‌دهنده پیغامی را به سرویس‌گیرنده ارسال می‌کند تا او را از پایان Handshake سمت سرویس‌دهنده آگاه نماید و همچنین این‌که داده بعدی که ارسال خواهد شد توسط کلید جلسه رمز می‌شود.

۱۰- در این مرحله SSL Handshake تمام می‌شود و از این به بعد جلسه SSL شروع می‌شود و هر دو عضو سرویس‌دهنده و گیرنده شروع به رمزنگاری و رمزگشایی و ارسال داده‌ها می‌کنند.

حملات تأثیرگذار برSSL

SSL نیز از حملات و نفوذهای مختلف در امان نیست. بعضی از حملات متداولی که براین پروتکل واقع می‌شود عبارتند از: Traffic Analysis یا تحلیل ترافیک، حملات Paste Cut بلووین، حملات Certification Injection و حملاَت از نوع Man in the middle.