امنیت تجارت الکترونیک

اطلاعات عمومی:
نفوذگران و حملات

تهیه و تنظیم:
دکتر آرش حبیبی لشکری

اولین نسخه: دی 1393
بروزرسانی: دی 1393

فهرست:

- نفوذگران
- دسته بندی نفوذگرها
- اهداف نفوذگرها
- انواع تهدیدها
  - Disclosure
  - Deception
  - Disruption
  - Usurpation
  - Repudiation
- گامهای یک حمله
  - Reconnaissance
  - Intrusion
  - Exploitation
  - Reinforcement
  - Consolidation
  - Pillage
- انواع حملات مرتبط با وب
- انواع حملات مرتبط با شبکه
- انواع حملات مرتبط با سیستم های عامل و برنامه های کاربردی

نفوذگرها و دسته بندی آنها

بعد از بدافزارها، یکی از مهمترین تهدیدات شایع در زمینه امنیت تجارت الکترونیک، مهاجمین هستند، که در اغلب موارد از آنها تحت عنوان هکرها یا کرکرها یاد می‌شود.

* آندرسون [ANDE80] سه کلاس برای مهاجمین معرفی مینماید:

* Masquerade: فردی که مجاز به استفاده از کامپیوتر نیست ولی به کنترلهای دسترسی سیستم رخنه می‌نماید تا از حساب کاربری یک کاربر قانونی و مجاز سوء استفاده نماید.

* Misfeasor: کاربر مجازی می‌باشد که به داده‌ها، برنامه‌ها، یا منابعی دسترسی دارد که چنین دسترسی برای او مجاز نمی‌باشد، یا کسی که برای این نوع دسترسی‌ها مجوز دارد اما از مجوزهای خود سوء استفاده می‌کند.

* Clandestine user: فردی که کنترل نظارت بر سیستم را تصرف می‌کند و از این کنترل برای فرار از حسابرسی و کنترل دسترسی یا متوقف کردن بازرسی‌ها استفاده می‌نماید.

یک Masquerader یا کاربر تغییر قیافه داده به احتمال زیاد یک فرد خارجی می‌باشد، یک misfeasor یا کاربر متجاوز در اغلب موارد یک فرد درون سیستمی است، و یک کاربر clandestiner یا کاربر مخفی و غیر مشروح می‌تواند فردی داخلی یا خارجی باشد.

اهداف نفوذگرها

محدوده حملات مهاجمین از بی خطر تا بسیار جدی و وخیم طبقه‌بندی می‌شود. در نوع بی‌خطر آن، مردم زیادی هستند که علاقه‌مندند تا بسادگی در اینترنت جستجو نموده و ببینند که در دنیای خارج چه چیزی رخ داده است. در نوع خطرناک و جدی تلاش می‌کنند تا داده‌های با مجوز دسترسی را بخوانند، و تغیرات غیر مجازی را در این داده‌ها بوجود بیاورند، یا سیستم را مختل کنند.

نمونهای از اهداف نفوذگران:

* از کار انداختن سرویس‌دهنده وب
* حدس زدن و شکستن رمزهای عبور
* کپی کردن یک پایگاه داده دارای شماره‌های مربوط به کارتهای اعتباری
* مشاهده داده‌های حساس، شامل رکوردهای لیست حقوق و اطلاعات پزشکی آن هم بدون مجوز دسترسی
* استفاده از خطای دسترسی بر روی یک سرویس‌دهنده FTP بی‌نام به منظور توزیع فایلهای جعلی
* معرفی خود به عنوان یک مدیر اجرایی و تماس با کاربر فنی سازمان برای تنظیم مجدد رمزعبور پست الکترونیکی مدیر اجرایی و بدست آوردن رمز عبور جدید
* استفاده از یک ایستگاه کاری که بدون مراقبت رها شده و ورود به ایستگاه کاری بدون مجوز دسترسی

انواع تهدیدها و گامهای نفوذ

تهدیدها را میتوان به پنج دسته کلی تقسیم نمود:

Disclosure یا افشاگری (دزدی اطلاعات، استراق سمع)

Deception یا فریبکاری (مرد در میانه، بازپخش پیام، دزدی شناسه)

Disruption یا قطع و ازکارانداختن (از کار انداختن سرویس)

Usurpation یا کنترل دسترسی داشتن (دسترسی غیر مجاز، تروجانها، زومبی ها)

Repudiation یا انکار کردن (پاکسازی)

کلیه تهدیدها و حملات عموما در شش گام انجام میشوند:

Reconnaissance: جمع آوری اطلاعات مرتبط با نقاط ضعف و عملکردههای قربانی

Intrusion: شروع عملیات حمله و با استفاده از اطلاعات جمع آوری شده

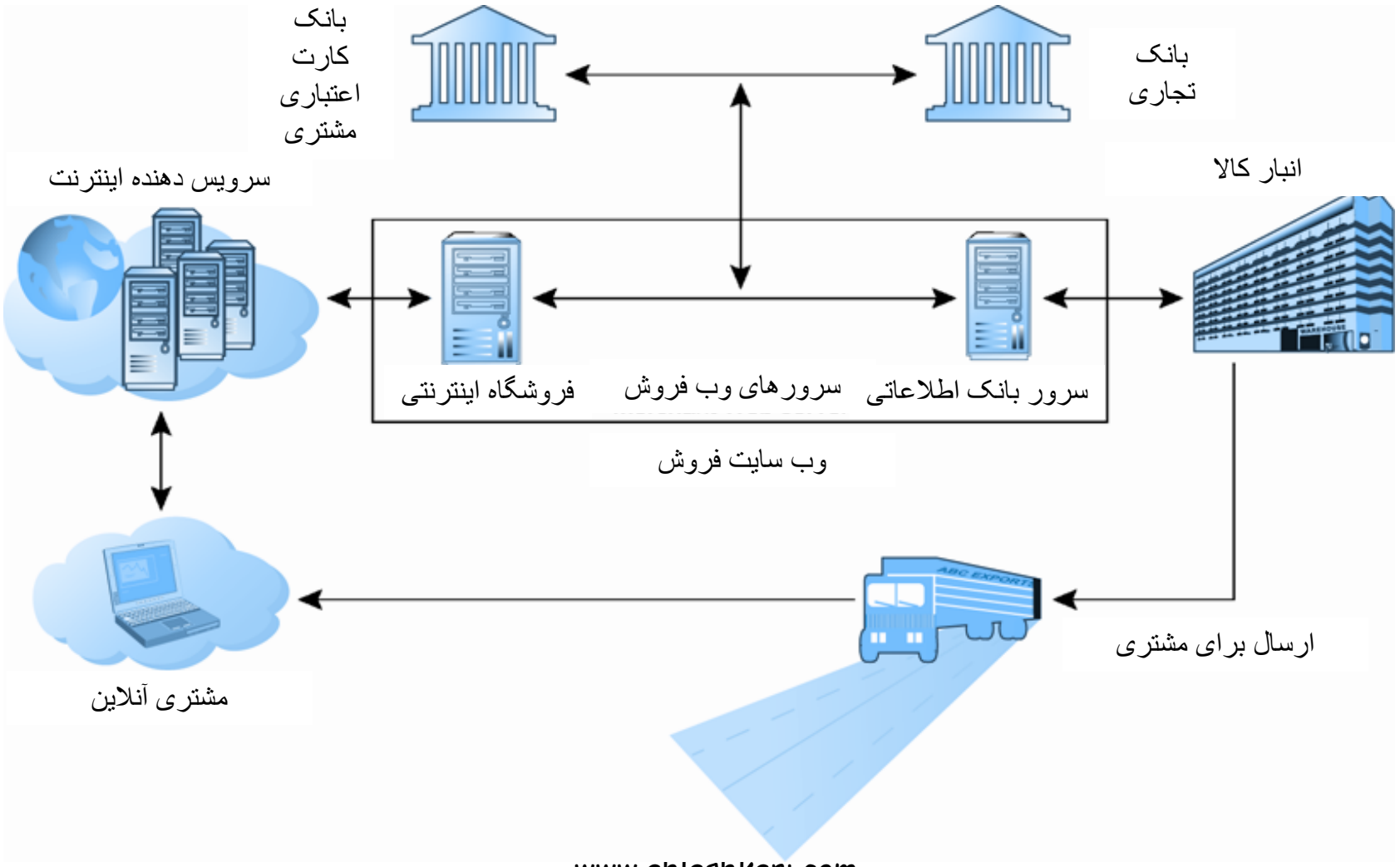
Exploitation: ازکار انداختن سرویس و نفوذ به سیستم مهاجم

Reinforcement: افزایش سطح دسترسی یا روشهای دسترسی مجدد برای آینده

Consolidation: اطمینان از برقراری ارتباط کامل با ماشین قربانی از طریق دربهای پشتی

Pillage: تشخیص و شناسایی اطلاعات مهم سیستم و انتقال آنها به خارج از سیستم (غارت کردن اطلاعات مفید) و یا استفاده از ماشین قربانی برای حملات به سایر ماشینها و شبکه

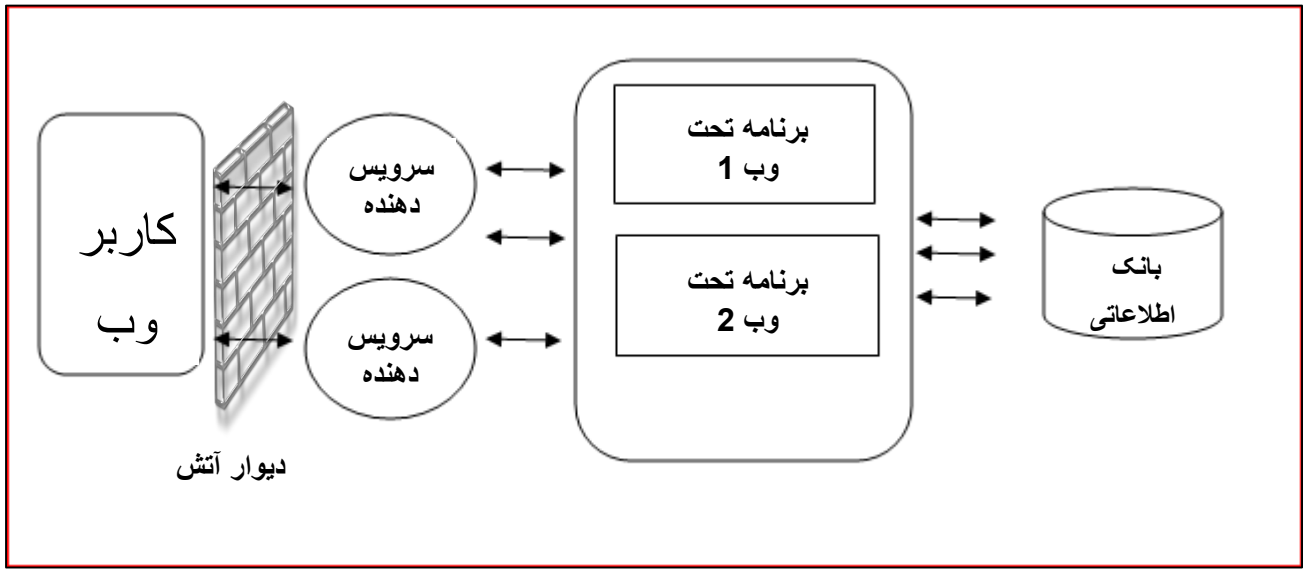
یک انتقال نمونه در تجارت الکترونیک



تهدیدهای وب

محیط: کاربر وب، دیوارآتش، سرویس دهنده وب، برنامه های روی سرویس دهنده، بانک اطلاعاتی

- تفسیر آدرس وب یا URL Interpretation
- تایید ورودی یا Input validation
- تزریق SQL یا SQL Injection
- ربودن جلسه یا Session Hijacking
- سرریز شدن بافر یا Buffer Overflow



تهدیدهای شبکه

محیط: شبکه داخلی کاربر – سرویس دهنده اینترنت – اینترنت – شبکه داخلی سرویس دهنده

- استراق سمع یا Eavesdropping
- دستکاری داده یا Data Modification
- مسمومیت (اسپوفینگ) آدرس شبکه یا IP Spoofing
- اسنیفینگ (خواندن، مونیتورینگ، کپی برداری) یا sniffing
- کشف کلید یا key compromising
- حملات برپایه رمزعبور یا Password-Based attack
- ازکار انداختن سرویس یا Denial-of-Service
- مرد – در– میانه یا Man-in-the-Middle
- مهندسی اجتماعی یا Social engineering

تهدیدهای مرتبط با برنامه ها و سیستم های عامل

محیط: برنامه سیستم عامل، برنامه های کاربردی کاربر

- سرریز شدن بافر برپایه پشته یا Stack-based buffer overflow
- دسترسی غیر مجاز یا Unauthorised access
- مسمومیت (اسپوفینگ) ورود یا login spoofing
- استفاده از بدافزارها برپایه نقاط ضعف سیستم عامل یا OS Vulnerability
- تروجانها – بمبهای منطقی – دربهای پشتی و ...
- کی لاگر یا Key logger / Keystroke
- جاسوس افزار یا Spyware
- آگهی افزار یا Adware

خلاصه: **نفوذگران، اهداف نفوذگران، دسته بندی نفوذگران، تهدیدهای وب، تهدیدهای شبکه، تهدیدهای سیستم عامل و برنامه های کاربردی**

جلسه بعدی: امنیت تراکنش پرداخت

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.