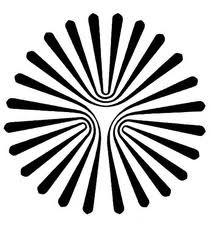
دانشگاه پیام نور



هک در شبکه‌های کامپیوتری / اینترنتی

پروژه دوره کارشناسی

مهندسی کامپیوتر گرایش نرم‌افزار

ارائه‌شده به:

گروه علمی فناوری اطلاعات و ارتباطات

دانشکده فنی مهندسی

دانشگاه پیام نورمرکز دماوند

استاد راهنما:

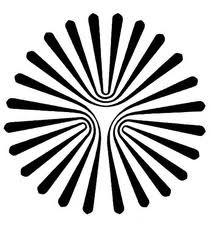
سرکار خانم محبوبه کمیاب

توسط:

سعید آذری

بهار 1395



دانشگاه پیام نور

هک در شبکه‌های کامپیوتری / اینترنتی

پروژه دوره کارشناسی

مهندسی کامپیوتر گرایش نرم‌افزار

ارائه‌شده به:

گروه علمی فناوری اطلاعات و ارتباطات

دانشکده فنی مهندسی

دانشگاه پیام نور مرکز دماوند

استاد راهنما:

سرکار خانم محبوبه کمیاب

توسط:

سعید آذری

بهار 1395

# چکیده

امروزه با افزایش کاربران کامپیوتر و دیجیتالی شدن حجم وسیعی از اطلاعات ازجمله عکس و فیلم، تراکنش‌های بانکی، ارتباطات، بایگانی‌های شرکت‌ها و سازمان‌ها و... اهداف زیادی را برای هکرها فراهم می‌کنند، ازاین‌رو شناخت روش‌های هک، حفره‌ها و امنیت در شبکه‌های کامپیوتری و اینترنت اهمیت بالایی دارد.

تأمین امنیت اطلاعات و کامپیوتر بخش مهمی از مهندسی کامپیوتر در دنیای امروز است و این امر با شناخت روش‌های هک، شناخت حفره‌های امنیتی و ابزارهای مورداستفاده هکرها امکان‌پذیر است. به دلیل تغییر روزافزون دستگاه‌های کامپیوتری، ارتقا آن‌ها و رفع حفره‌های امنیتی آن‌ها، هکرها نیز ابزارها و روش‌های خود را به‌روز می‌کنند، پس مهندسین کامپیوتر نیز باید دانش خود را در این زمینه به‌روز کنند تا بتوانند با آن‌ها مقابله کنند.

در این پروژه با انواع حملات هکرها، انواع باگ‌ها و روش‌های شناسایی هکرها پرداخته می شود.

مطالب این پروژه در شش فصل تنظیم‌شده است.

فصل اول به مقدمه‌ای بر هک، تعاریف پایه، تروجان ها و دیگر تعاریف پرداخته‌شده است که باعث فهم بهتر فصول بعد می‌شود.

در فصل دوم به تعریف امنیت، برخی از تهاجم‌ها و بررسی تخصصی بر روی آن‌ها، دیوار آتش و نحوه دور زدن آن و جلوگیری از شناسایی درگاه‌های باز پرداخته می شود. فصل سوم توپولوژی هک، عوامل تحریک هکر، ویروس‌ها، DDOS، کرم‌ها و صفحه‌کلید خوان‌ها را پوشش می‌دهد. فصل چهارم کدهای اسکریپتی را از قبیل جاوا اسکریپت را ازنظر امنیت و هک بررسی کرده و چگونگی هک شدن توسط آن‌ها بررسی می‌شود. فصل پنجم به نتیجه‌گیری و پیشنهاد‌ها امنیت اختصاص دارد.

کلمات کلیدی: هک – امنیت – روش‌های مقابله بانفوذ – نفوذ – سرقت اطلاعات – بدافزار

فهرست

[چکیده ج‌](#_Toc453834622)

[**1** فصل اول 1](#_Toc453834623)

[**1-1** **مقدمه** 2](#_Toc453834624)

[**1-2** **هک به چه معناست؟** 3](#_Toc453834625)

[**1-3** **اهداف هکر** 3](#_Toc453834626)

[**1-3-1** روش‌های نفوذ هکرها و نفوذگران به شناسه کاربری 7](#_Toc453834627)

[**1-4** **اصول ابتدایی برای گریز از کرک شدن** 8](#_Toc453834628)

[**1-5** **استفاده از صفحات جعلی** 9](#_Toc453834629)

[**1-6** **مهندسی اجتماعی چیست؟** 11](#_Toc453834630)

[**1-7** **تروجان ها** 13](#_Toc453834631)

[**1-8** **تکنیک‌های انتخاب کلمه عبور** 13](#_Toc453834632)

[**1-8-1** استاندارد ISO ۱۷۷۹۹ 17](#_Toc453834633)

[**1-9** **فیشینگ چیست؟** 19](#_Toc453834634)

[**1-9-1** مشخصات عمومی و مشترک بین پست الکترونیکی با هدف فیشینگ 20](#_Toc453834635)

[**1-9-2** قانون طلایی مواجهه با عملیات فیشینگ 22](#_Toc453834636)

[**1-10** **روش‌های معمول حمله به کامپیوترها** 24](#_Toc453834637)

[**1-10-1** برنامه‌های اسب تروآ 24](#_Toc453834638)

[**1-10-2** اسکریپت‌های Cross-Site 26](#_Toc453834639)

[**1-10-3** ایمیل‌های جعلی 27](#_Toc453834640)

[**1-10-4** پسوندهای مخفی فایل 28](#_Toc453834641)

[**1-10-5** شنود بسته‌های اطلاعات 28](#_Toc453834642)

[**1-10-6** حملات pharming 29](#_Toc453834643)

[**1-10-7** بررسی دنیای واقعی 32](#_Toc453834644)

[**1-10-8** دیوار آتش 32](#_Toc453834645)

[**1-11** **منظور از دیوار آتش چیست؟** 33](#_Toc453834646)

[**1-11-1** هدف از یک دیوار آتش 34](#_Toc453834647)

[**1-11-2** دیوار آتش ارائه کنترل دسترسی 35](#_Toc453834648)

[**1-11-3** مزایا و معایب دیوار آتش 36](#_Toc453834649)

[**1-11-4** چالش‌های درپشتی: تهدید مودم 36](#_Toc453834650)

[**2** فصل دوم 37](#_Toc453834651)

[**2-1** **مقدمه** 38](#_Toc453834652)

[**2-2** **امنیت به عنوان یک زیربنا** 38](#_Toc453834653)

[**2-3** **امنیت فراتر از یک کلمه رمز** 39](#_Toc453834654)

[**2-4** **اول خطرات سطح بالا و مهم‌تر را برطرف شود** 40](#_Toc453834655)

[**2-5** **امنیت به عنوان یک محدودیت** 41](#_Toc453834656)

[**2-6** **تهاجم DDOS چیست؟** 42](#_Toc453834657)

[**2-7** **تهاجمات مصرف منبع** 42](#_Toc453834658)

[**2-7-1** کالبدشکافی یک تهاجم سیل SYN 44](#_Toc453834659)

[**2-7-2** کالبد شکافی یک تهاجم DDOS 45](#_Toc453834660)

[**2-7-3** ابزارهای مهاجمین برای انجام خدمات DDOS 46](#_Toc453834661)

[**2-7-4** روش‌های اساسی حفاظت 46](#_Toc453834662)

[**2-7-5** تهیه شرح حال از خصوصیات و مشخصات ترافیک 47](#_Toc453834663)

[**2-7-6** تقسیم کردن شالوده NDS 47](#_Toc453834664)

[**2-7-7** متعادل ساختن بار 48](#_Toc453834665)

[**2-7-8** فیلتر سازی ورودی و خروجی 48](#_Toc453834666)

[**2-8** **محکم کردن پیکربندیهای دیوار آتش** 48](#_Toc453834667)

[**2-9** **ایجاد یک IDS** 49](#_Toc453834668)

[**2-9-1** اجرای یک مرور کننده آسیب پذیری 49](#_Toc453834669)

[**2-10** **ایجاد سرورهای پراکسی** 49](#_Toc453834670)

[**2-11** **پیکربندی کردن فداکارانه میزبانها** 50](#_Toc453834671)

[**2-12** **افزایش مدیریت میزبان و شبکه** 50](#_Toc453834672)

[**2-13** **گسترش بیشتر تکنولوژی‌های امنیت** 50](#_Toc453834673)

[**2-14** **گردآوری اطلاعات** 50](#_Toc453834674)

[**2-15** **راههای مختلف جهت مسیردهی** 51](#_Toc453834675)

[**2-16** **مقایسه قابلیت‌های امنیت سرور وب** 51](#_Toc453834676)

[**2-17** **تصدیق** 52](#_Toc453834677)

[**2-18** **کلمات عبور** 52](#_Toc453834678)

[**2-20** **به کارگیری برنامه‌های کاربردی CGI** 53](#_Toc453834679)

[**2-21** **IIS** 54](#_Toc453834680)

[**2-22** **پورت‌ها، سرویس‌ها و اجزاء بلا استفاده را غیر فعال کنید** 54](#_Toc453834681)

[**2-23** **اسکریپت‌ها و فایل‌های غیر لازم را پاک کنید** 55](#_Toc453834682)

[**2-24** **هک کردن کلمه عبور و ابزار تجزیه و تحلیل** 56](#_Toc453834683)

[**3** فصل سوم 58](#_Toc453834684)

[**3-1** **مقدمه** 59](#_Toc453834685)

[**3-2** **درک شرایط و سطوح** 60](#_Toc453834686)

[**3-3** **خلاصه‌ای بر تاریخچه هک کردن** 60](#_Toc453834687)

[**3-3-1** سیستم هک کردن تلفن 61](#_Toc453834688)

[**3-3-2** سیستم هک کردن کامپیوتر 62](#_Toc453834689)

[**3-4** **عوامل تحریک هکرها چیست؟** 63](#_Toc453834690)

[**3-4-1** مقابله در برابر هک کننده‌های بداندیش 64](#_Toc453834691)

[**3-4-2** کار کردن با حرفه‌ای‌های عرصه امنیت داده‌ها 64](#_Toc453834692)

[**3-4-3** کم کردن مشکلات با به خدمت گرفتن سیستم امنیتی 65](#_Toc453834693)

[**3-5** **شناخت انواع حملات در دستگاه‌های موجود** 65](#_Toc453834694)

[**3-6** **Dos/ DDos** 66](#_Toc453834695)

[**3-7** **ویروس‌های هک کننده** 68](#_Toc453834696)

[**3-8** **روش‌های صدمه و دفاع در برابر حمله** 70](#_Toc453834697)

[**3-9** **اسب تروآ** 70](#_Toc453834698)

[**3-10** **کرم‌ها** 72](#_Toc453834699)

[**3-11** **برنامه‌های ولگرد** 73](#_Toc453834700)

[**3-12** **دزدیدن** 74](#_Toc453834701)

[**3-12-1** دزدان کارت اعتباری 75](#_Toc453834702)

[**3-12-2** دزدی هویت 76](#_Toc453834703)

[**3-12-3** دزدان و راه زنان اطلاعات 77](#_Toc453834704)

[**3-13** **درک شیوه سیستم پیشگیری کننده امنیتی برنامه‌های کاربردی و تهدیدات آن** 77](#_Toc453834705)

[**3-13-1** اخلال‌های پنهان 78](#_Toc453834706)

[**3-13-2** پارامترهای جعلی و پنهان 78](#_Toc453834707)

[**3-13-3** برش ابتدایی 78](#_Toc453834708)

[**3-13-4** پر شدن و سرریز شدن بافر 79](#_Toc453834709)

[**3-13-5** شیرینی زهرآلود 79](#_Toc453834710)

[**3-14** **جلوگیری از هک شدن با روش فکر کردن مثل یک هکر** 80](#_Toc453834711)

[**3-14-1** تیم توسعه دهنده 81](#_Toc453834712)

[**3-14-2** تیم کنترل کیفیت (QA) 82](#_Toc453834713)

[**3-14-3** تیم امنیت اطلاعات 82](#_Toc453834714)

[**4** فصل چهارم 84](#_Toc453834715)

[**4-1** **مقدمه** 85](#_Toc453834716)

[**4-2** **تشخیص ضربه حملات کد تلفن همراه** 85](#_Toc453834717)

[**4-3** **حملات Mail client** 85](#_Toc453834718)

[**4-4** **ماکروها یا اسکریپتهای خرابکار** 87](#_Toc453834719)

[**4-4-1** زبانهای ماکرو (VBA) 88](#_Toc453834720)

[**4-4-2** مشکلات امنیتی با VBA 88](#_Toc453834721)

[**4-5** **ویروس ملیسا** 88](#_Toc453834722)

[**4-6** **حمایت در برابری ویروسهای VBA** 89](#_Toc453834723)

[**4-7** **جاوا اسکریپت** 89](#_Toc453834724)

[**4-7-1** امنیت جاوا اسکریپت 90](#_Toc453834725)

[**4-8** **جاوا اسکریپت و مشکلاتی که پدید می‌آورد** 90](#_Toc453834726)

[**4-9** **مشکلات امنیتی** 92](#_Toc453834727)

[**4-10** **حملات Web-Based E-mail** 92](#_Toc453834728)

[**4-11** **مهندسی اجتماعی Social Engineering** 93](#_Toc453834729)

[**4-12** **پایین آوردن خطرات امنیتی Java script** 93](#_Toc453834730)

[**4-13** **VBScript** 93](#_Toc453834731)

[**4-13-1** امنیت در VBScript 94](#_Toc453834732)

[**4-13-2** مشکلات امنیت در VBScript 94](#_Toc453834733)

[**4-13-3** پیشگیری امنیتی VBScript 95](#_Toc453834734)

[**4-14** **برنامه‌های کاربردی جاوا** 96](#_Toc453834735)

[**4-14-1** مشکلات امنیتی با جاوا 96](#_Toc453834736)

[**4-15** **نگاهی به کنترلهای اکتیو ایکس** 97](#_Toc453834737)

[**4-15-1** مشکلات امنیتی با اکتیو ایکس 97](#_Toc453834738)

[**4-15-2** اشتباه در انتقال و جایگیری کاراکترها 98](#_Toc453834739)

[**4-15-3** غیر فعال کردن کنترلهای اکتیو ایکس 98](#_Toc453834740)

[**4-16** **متعلقات ایمیل** 98](#_Toc453834741)

[**4-16-1** حمایت از سیستم شما در مقابل با حملات کد تلفن همراه 99](#_Toc453834742)

[**4-17** **برنامه‌های امنیتی** 99](#_Toc453834743)

[**4-17-1** کشف کننده‌های حفره‌ها 99](#_Toc453834744)

[**4-17-2** نرم‌افزار فایروال 100](#_Toc453834745)

[**5** فصل پنجم 101](#_Toc453834746)

[**5-1** **مقدمه** 102](#_Toc453834747)

[**5-2** **جلوگیری از مشکلات ناشی از جاوا، جاوا اسکرپت و اکتیو ایکس** 102](#_Toc453834748)

[**5-3** **برنامه نویسی اسکریپت‌های ایمن** 105](#_Toc453834749)

[**5-5** **سیاست امنیت چیست؟** 107](#_Toc453834750)

[**5-6** **ارزش در برابر ریسک** 108](#_Toc453834751)

[**5-6-1** سیاست امنیت شامل چه عناصری است 109](#_Toc453834752)

[**5-6-2** هجوم‌های دسترسی به فایل 113](#_Toc453834753)

[**5-6-3** تهاجمات اطلاعات غلط 114](#_Toc453834754)

[**5-6-4** هجوم‌های دسترسی به فایل / بانک اطلاعاتی ویژه 115](#_Toc453834755)

[**فهرست منابع** 118](#_Toc453834756)

[**Abstract** 119](#_Toc453834757)

# فصل اول

نگاهی به هکرها و شیوه عملکردشان

## **مقدمه**

فنّاوری اینترنت تنها به منزل و محل کار ما هدایت نشده است و در بیشتر جنبه‌های زندگی ما وجود دارد، بشکه‌های بی‌سیم و دست‌یابی به دستگاه‌ها، حضور اینترنت را در همه‌جا فعال کرده است. بسیاری از این دستگاه‌ها به‌طور مأیوسانه‌ای امنیت ضعیف و سستی دارند که باعث می‌شود کاندیدای ایدئال برای یک هکر باشند. این موضوع وقتی اسفبارتر است که دستگاه‌های دارای امنیت ضعیف، دستگاه‌هایی را که دارای امنیت جامعی هستند را با سوار کردن تهاجمات روی آن‌ها به مخاطره می‌اندازند. حتی برنامه‌ها و دستگاه‌هایی که دارای امنیت صوتی هستند از هجوم یا خطر مصون نیستند. افزایش تقاضای نرم‌افزار و کاهش سریع در چرخه‌های توسعه بدین معنی است که نسخه جدید نرم‌افزارهای نصب‌شده روی ماشین‌ها یک گام جلوتر است. جرم‌ها و سوءاستفاده‌های فنی در کشمکش با دنیای اینترنت هست. کشورهای بیگانه اغلب گرفتار جرم‌های اینترنتی می‌شوند و پی گیری گروه‌های مجرم وقت‌گیر و پرزحمت است. انجام هک تا حدودی بر مبنای کسب علم و دانش استوار است یک اشتیاق برای ارضای یک حس ذاتی کنجکاوی فنی. با این دید، به بسیاری از هکرها در مورد فعالیت‌هایشان حق داده می‌شود. بدین معنی که آن‌ها رخنه‌ها و کاستی‌های امنیت را آشکار می‌سازند. بعضی اشخاصی که به‌عنوان هکر شناخته می‌شوند در حقیقت موافق با بسیاری از عادات هک کردن اصیل نیستند و ترجیح می‌دهند که اهداف خود را به دلایلی غیر از کسب دانش و جهت آرزو برای افزایش آگاهی امنیت، مورد هدف قرار دهند.

بعضی هکرها، برنامه‌ها، دستگاه‌ها را به‌منظور بالا بردن آگاهی امنیت مورد هدف قرار می‌دهند این نوع فعالیت هنوز هم می‌تواند به‌عنوان یک هجوم برچسب بخورد چراکه فعالیت آن‌ها می‌تواند نتایج ناخواسته و غیرمنتظره‌ای را در برداشته باشد. بدین علت است که برخی اصطلاح هک کردن اخلاقی را یک تناقض می‌دانند.

## **هک به چه معناست؟**

شاید تابه‌حال برای شما اتفاق افتاده باشد که موردحمله هکرها قرار بگیرید. شاید بارها حساب‌های اینترنتتان در عرض یک روز خالی‌شده باشد بدون آنکه خودتان استفاده کرده باشید. شاید متوجه شده باشید که در یاهو مسنجر[[1]](#footnote-1) شخص دیگری هم از نام کاربری شما استفاده می‌کند.

هک به زبان ساده و شاید عامیانه‌ترین تعبیر آن دزدیده شدن کلمه عبور یک سیستم یا حساب کاربری هست.

به‌طورکلی نفوذ به هر سیستم امنیتی کامپیوتری را هک می‌گویند. هکر شخصی است باهوش, فرصت‌طلب, دارای معلومات بالا با افکار سازنده و مطمئناً باوجدان. لازم به ذکر است که هکرها با دزدان اینترنتی و یا الکترونیکی فرق دارند.

دزدان اینترنتی افراد کلاه‌بردار و شیادی هستند که با استفاده از فضای نت سعی در کلاه‌برداری و یا سرقت اطلاعات شخصی یا اطلاعات محرمانه شرکت‌ها و احتمالاً فروش آن‌ها هستند ابزار کار، شیوه عمل و ترفند هکر و دزدان اینترنتی یکی است اما این موضوع ما را به‌اشتباه نیندازد هدف پیشرو هکر یک هدف خوب است زیرا هکرها اکثر از افراد باتجربه خلاق و سرآمد فن‌آوری اطلاعات هستند.

هکرهای واقعی در میان خود مرام‌نامه‌ای دارند که همه پایبند به آن می‌باشند.

## **اهداف هکر**

در اصل هر هکر برای نفوذ به شبکه‌ها و سایت‌ها اینترنتی دو هدف را دنبال می‌کند البته هکرها هم‌قسم‌ها مختلف و نامه‌ای گوناگون دارند اما درمجموع در دلیل عمده بین آنان مشترک است

هکر در موقع هک کردن یک سیستم امنیتی هدفش ضربه زدن (چه مادی و چه معنوی) به شخص یا اشخاصی نیست. او هک می‌کند تا معلوماتش را نشان دهد. در آمریکا و بسیاری از کشورها هکرها را استخدام می‌کنند چون می‌دانند ازنظر سواد فن‌آوری اطلاعات در سطح بالایی قرار دارند.

هکر در جهان به‌عنوان فردی متخصص باتجربه مفید شناخته می‌شود اما مانند هر صنف و سلوک افرادی نامطلوب هم در این قشر قرار دارد، در این میان افرادی هستند که با سوءاستفاده از معلومات خود و یا دیگران هدفشان از هک کردن ضربه زدن به اشخاص است یا به دنبال پر کردن جیب خود می‌باشند. این افراد دزدانی بیش نیستند. لذا منظور از هک در اینجا دزدیدن کلمه عبور حساب‌های بانکی، یاهو مسنجر و هات میل[[2]](#footnote-2) هست که بسیاری از خوانندگان از آن‌ها استفاده می‌کنند. چگونه هک می‌شویم؟!

یکی از متداول‌ترین روش‌های هک کردن, حدس زدن رمز عبور است. روش رایج دیگر خواندن رمز عبور از روی دست کاربر به هنگام تایپ آن هست. یا فرستادن صفحه‌ای مانند صفحه ورودی هات میل و یاهو به‌صورت یک ایمیل که در آن به‌ظاهر کارکنان شرکت سرویس‌دهنده از کاربر خواسته‌اند به‌منظور اطمینان از صحت سرویس‌دهی رمز عبور خود را تایپ کند. که این رمز عبور در همان لحظه برای هکر ایمیل می‌شود.

فراموش نکنید هیچ ارائه‌دهنده خدماتی مابین ارائه خدمات از شما رمز درخواست نمی‌کند و اگر به هر دلیل اختلالی به وجود آید کار از ابتدا شروع می‌شود.

برنامه جالبی وجود دارد که فایل تمامی حرف‌هایی که واردشده است را ذخیره می‌کند. هکر برنامه را اجرا می‌کند و بعد از شما می‌خواهد که رمز خود را بزنید. کلیدهای تایپ‌شده توسط شما درون یک فایل متنی ذخیره می‌شود و هکر بعداً به آن رجوع می‌کند و رمز شمارا کشف می‌نماید.

روش دیگر حدس زدن جواب سوالی است که شما انتخاب نموده‌اید تا در صورت فراموش نمودن رمزتان از شما پرسیده شود. در یاهو استفاده از این روش سخت است زیرا تاریخ دقیق تولد و آدرس و حتی کد پستی را نیز می‌خواهد. ولی در سرویس هات میل به سادگی می‌توانید جواب سؤال را حدس بزنید و رمز را بدست آورید. و نیز هکر می‌تواند به کارکنان هات میل نامه زده و در آن ابراز نماید که حساب کاربری اش مورد هک قرار گرفته و درخواست رمز جدید کند که کارکنان هات میل از او چند سؤال در مورد سن و آخرین دسترسی به حساب و آخرین رمزی که به خاطر دارد می‌کنند و سپس رمز جدید در اختیار او قرار می‌گیرد.

یا برای یافتن رمز حساب‌های اینترنت, به ISP شما زنگ می زند و با دادن مشخصات خواستار تغییر رمز می‌شود. جالب اینجاست که در بسیاری از موارد منشیان رمز قبلی را نمی‌پرسند.

این‌ها همه روشهای ساده ولی رایج و متداول بودند. روش دیگری که در اینجا در موردش صحبت می‌کنم کمی تخصصی است و هر شخصی نمی‌تواند از این روش استفاده کند بلکه باید معلوماتی در خصوص اینترنت و IP و یک سری نرم‌افزارها داشته باشد.

در این روش شخص با فرستادن یک فایل آلوده به ویروس یا RAT سیستم شمارا آلوده می‌کند. با اجرای این فایل, فایل مورد نظر در حافظه جای می‌گیرد و هر زمان که کامپیوتر روشن شود دوباره در حافظه صدا می‌شود. پس با پاک نمودن فایل اولیه مشکل شما حل نمی‌شود. این فایل کامپیوتر شمارا به عنوان یک سرور[[3]](#footnote-3) در می‌آورد و یکی از پورت‌ها را برای استفاده هکر باز می‌گذارد. حال هکر می‌تواند با پیدا کردن IP شما و اتصال به پورت مورد نظر در زمانی که هم شما آنلاین هستید هم هکرتان هر کاری با کامپیوتر شما بکند حتی آنرا خاموش کند و رمزهای موجود در کامپیوتر شمارا بدزدد.

البته ارسال فایل گاهی به‌صورت آنلاین نمی‌باشد. هکر می‌تواند اگر با شما آشنایی داشته باشد به پشت کامپیوتر شما بی آید و فایل مورد نظر را روی آن اجرا کند. جالب اینجاست که اغلب ویروس کش ها از شناسایی RAT های جدید عاجزند. روش‌های ساده را به سادگی و با کمی دقت می‌توان مسدود کرد. مثلاً رمزی انتخاب کنید که حدس زدنش کار هر کسی نباشد. شماره تلفن, اسم, فامیل, شماره شناسنامه یا تاریخ تولید و ترکیبی از این‌ها معمولاً اولین چیزی است که به ذهن هر کسی می‌رسد. سعی کنید در رمز انتخابی خود از پرانتز یا کروشه استفاده کنید یا حتی کاما که اینها به ذهن هیچ هکری نخواهد رسید.

هنگامی که رمز خود را وارد می‌کنید مراقب باشید, کسی نزدیکتان نباشد. یا از کلیدهای منحرف کننده استفاده کنید. مثلاً چند کلید الکلی بزنید و بعد با پسبرد[[4]](#footnote-4) پاکش کنید که اگر کسی هم دید, متوجه رمز شما نشود.

پشت کامپیوتر کسی که به او اطمینانی ندارید, رمزی وارد نکنید. یا اگر مجبورید, با استفاده از کلیدهای Ctrl+Alt+Del و باز نمودن Task Manager کلیه برنامه‌های مشکوک را ببندید.

معمولاً اسامی آن‌ها مانند: Thief، Keylogger یا keyl یا هر اسم مشکوک دیگری می‌تواند باشد. در موقع ثبت نام در سرویسهای هات میل و یاهو به شما تذکر داده می‌شود که کارکنان شرکت سرویس‌دهنده به هیچ عنوان از طریق ایمیل از شما درخواست رمز عبور نمی‌کنند. پس هیچ گاه از طریق هیچ ایمیلی رمز خود را وارد نکنید.

از جایی اینترنت تهیه کنید که امنیت بیشتری دارد و تجربه کارشان بالاست. زیرا علاوه بر منشیان بی تجربه که بعضاً رمزها را برباد می‌دهند, اگر شبکه (ISP) هک شده باشد, دیگر از دست شما کاری بر نمی‌آید و رمز شما و دیگر کاربران در خطر هست.

در صورتی که با شبکه‌ای مهم در ارتباط هستید و یا در حال به روز رسانی سایتی هستید و در هرحال اطلاعات مفید و محرمانه در کامپیوتر خود دارید حدالمقدور از نصب برنامه‌های چت و گفتگو مانند یاهو مسنجر به شدت خودداری کنید حتی در صورت عدم استفاده از این نرم‌افزارها بازهم حفره برای ورود هکر به سیستم هستند. چیزی که جز با پاک کردن برنامه‌های گفتگو امکان پذیر نیست این مقوله تا جایی است که متخصصین امنیت شبکه اینگونه کاربران را از بازدید از هر سایت ناشناخته منع می‌کند!!!

احتمال حمله با روش تخصصی که در بالا توضیح داده شد به کاربرانی که از دستگاه‌های پیام رسانی مانند: یاهو مسنجر، ام اس ان مسنجر[[5]](#footnote-5)، ای سی کیو[[6]](#footnote-6) و ... استفاده می‌کنند بیشتر است چون اینگونه برنامه‌ها به راحتی IP شمارا در اختیار هکر قرار می‌دهند و همواره یک پورت آزاد را اشغال می‌کنند و معمولاً به‌صورت مستقیم با کاربر مقابل در ارتباط هستند. مخصوصاً در مواقع ارسال و دریافت فایل. پس اگر می‌خواهید در امان باشید از این برنامه‌ها استفاده نکنید. ولی امروزه در ایران اینترنت بدون اینگونه برنامه‌ها فایده‌ای ندارد! پس هیچگونه فایلی را که از افراد ناشناس فرستاده می‌شود, باز نکنید. حال اگر کامپیوتر شما از قبل آلوده شده باشد چه باید کرد؟! اگر مطئمن ترین راه را می‌خواهید.

در مورد ویروسهای جدید به خصوص تروجانها نصب مجدد ویندوز کفایت می‌کند، البته ابتدا ویروس را شناسایی و حتماً آن قسمت را فرمت کنید ویا کامل کامپیوتر خود را فرمت نموده و دوباره ویندوز را نصب کنید. زیرا اغلب ویروس کشها قادر به شناسایی یا پاک نمودن بسیاری از این نوع ویروس‌ها نمی‌باشند. ولی معمولاً این روش به صرفه نیست.

### روش‌های نفوذ هکرها و نفوذگران به شناسه کاربری

روش‌های نفوذ هکرها به شناسه کاربری و پست الکترونیکی، مقوله ایست که باید به شدت مورد توجه کاربران اینترنتی قرار گیرد تا از دارایی شخصی مجازی خود دفاع کنند گرچه هنوز پست الکترونیکی و شناسه کاربری در ایران جایگاه حقوقی ندارد و ارزش چندانی ندارد به گونه که در اکثر کشورها، پست الکترونیکی شخص، مانند هویت مجازی اوست تمام نامه‌های رسمی و یا شخصی کاربر، در صندوق پست الکترونیک جا خوش می‌کند، در یک کلام به قول دوستی تمام زندگی‌اش در پست الکترونیکی و هویتش شناسه کاربری او خلاصه می‌شود.

فرض کنید، که رمز عبور مدیریت وبلاگتان را فراموش کردید چه کار می‌کنید، ساده است از سرویس فراموشی رمز عبور که در همه مدیریت‌های وبلاگها درج شده است استفاده می‌کنید، شناسه کاربری وبلاگتان همراه با ایمیلتان را درج می‌کنید (ایمیل مندرج در شناسنامه وبلاگ) رمزعبور جدید به صندوق پست الکترونیکی شما ایمیل می‌شود. حال هکرها چه می‌کنند، ازروشها که خواهیم گفت، به ایمیل شما دسترسی پیدا می‌کنند، سپس از سرویس فراموشی رمز عبور بهره جسته و رمزعبور وبلاگتان را بدست می‌آورد، شاید بتوان گفت، گسترده‌ترین راه تصاحب یک وبلاگ، تصاحب ایمیل مربوط به وبلاگ است پس به پست الکترونیکی خود اهمیت بدهید.

## **اصول ابتدایی برای گریز از کرک[[7]](#footnote-7) شدن**

کرک یا شکستن قفل به معنی این است که ما به نفوذگر و هکر کمک می‌کنیم تا به کلمه عبور و شناسه کاربری ما دست یابد و مانند یک کاربر واقعی وارد پست الکترونیکی و ایمیل ما شود و آن را سرقت یا تصاحب کند البته این شخص کرکر[[8]](#footnote-8) شناخته می‌شود.

این امر چگونه اتفاق می افتد، به جرات می‌توان گفت خود کاربر دو دستی رمز عبور و شناسه کاربری خود را تقدیم نفوذگر می‌کند روشهای بسیار ساده و ابتدایی است که بتوان به این امر خاتمه داد.]2[

در یک کلام در فضای اینترنت به هیچ فرد اعتماد نکنید، قبل از هر کاری فکر کنید تا چه حد امکان هک و نفوذگری وجود دارد، راههای هک آموخته شود و از اخلاق هکرها اطلاع حاصل کرد، که به جای هک، مقابله باهکینگ و روشهای امنیت شبکه را می‌آموزند را مطالعه و مسله را جدی گرفته شود و گرنه حتی اگر خودمتان هم هکر باشید و مسائل امنیت شبکه را رعایت نکنیدم، قربانی می‌شوید.

بسیاری از کاربران از سرویس‌های پست الکترونیکی یاهو، جی میل یا هات میل استفاده می‌کنند تفاوت ندارد، اما در زمینه دانش امنیت شبکه, اطلاعات کمی دارند. لذا در ادامه اطلاعات مختصری در زمینه امنیت شبکه به کاربران ارائه می شود.

راه‌هایی که هکرها معمولاً از آن‌ها استفاده می‌کنند بسیار ساده و عین حال فریبنده است، فریبندگی این مقوله از آنجاست که تمام تلاش شخص نفوذگر این است که ذهن شمارا نسبت به نفوذش منحرف کند، اعتماد شمارا جلب نماید و آنگاه با دست شما، به شناسه کاربری و رمز عبور شما دست یابد راههای نفوذ و کرک توسط کراکر به بدین شرح می‌تواند انجام شود:

در این روش، فرد هکر برای خود در یاهو یک آدرس ایمیل ایجاد می‌کند که شمارا به اشتباه خواهد انداخت و شما تصور خواهید کرد که این آدرس ایمیل مربوط به یکی از دست اندرکاران یاهو است و به آن اعتماد می‌کنید. در این ایمیل درخواست می‌شود برای تمدید امکان استفاده از سرویس وبسایتتان، روی یک کلمه کلیک کنید (انتشار تروجان) یا یک فرم را پر نمایید، یا رمز عبور و شناسه کاربری را برای هکر ارسال کنید.

نرم‌افزارهای زیادی وجود دارد که به راحتی می‌توان صندوق پست الکترونیکی فرد را شیبه سازی کرد به عبارتی می‌توان بدون اینکه به ایمیل فرد دسترسی داشته باشید، بادرج آدرس پست الکترونیکی یک پست الکترونیکی معتبر با نام و آدرس صندوق الکترونیکی فردی به به فرد دیگر ارسال کرد٫ فرد دریافت کننده حتی اگر یک هکر و متخصص تمام عیار در زمینه فن‌آوری اطلاعات باشد نمی‌تواند دریابد که این پست الکترونیکی واقعی است یا از طرف هکر ارسال شده است.

هرگز مدیران وبسایتها مانند یاهو یا جی میل و حتی وبسایتهای فارسی زبان که شما در آن عضو هستید به کلمه عبور شما احتیاج ندارند٫ به یادداشته باشید مسولین وبسایتها درصورت نیاز به کل اطلاعات کاربری در محدوده کاری وبسایتشان دسترسی دارند.

## **استفاده از صفحات جعلی**

در این روش معمولاً هکر، شمارا با حقه‌های جذاب وادار به ورود در صفحه‌ای می‌کند که کاملاً شبیه به صفحه ورود در یاهو است و شما ذره‌ای شک نمی‌کنید. اما با ورود اطلاعات شما برای ایمیل هکر ارسال می‌شود.

تنها تفاوت این صفحات دروغین با صفحات اصلی در آدرس (URL) است که این صفحه را از آنجا بارگذاری می‌شود. به این آدرس در قسمت آدرس باکس مرورگر خود کاملاً دقت کنید تا از اصل بودن آن کاملاً مطمئن شوید و در صورتی که ذره‌ای شک کردید از ورود اطلاعات خودداری کنید.

نحوه ایجاد این صفحات بدین شکل است که هکر یک کپی از روی صفحات اصلی در اینترنت برداشته و با تغییراتی در کدهای آن، سبب می‌شود که نام کاربری و پسورد شما به آدرس ایمیل خاصی که معمولاً آدرس ایمیل خود هکر است ارسال شود. سپس هکر این صفحات را به آدرس ثالثی غیر از آدرس حقیقی خود صفحات اصلی ارسال کرده و منتظر شکار خود می‌ماند. البته در صورتی که صفحه مذکور در پنجره بررسی کد HTML صفحه مذکور است. برای این کار در مرورگر خود بر روی صفحه مورد نظر کلیک راست کنید و از منوی باز شده دستور VIEW SOURCE را اجرا نمائید.

آنچه در روش الف تذکر داده شد را رعایت کنید، فقط به خاطر بسپارید، که برروی هر لینک ناشناس و مشکوک کلیک نکنید و همیشه با بازکردن صفحه جدید، به نگارش کامل آدرس اینترنتی آن دقت کنید مثلاً کرک‌ها به جای [http://www.google.com](http://www.google.com/) از [http://www.googel.com](http://www.googel.com/) یعنی e و L را جابجا نموده، یک صفحه مشابه گوگل و صفحات داخلی جی میل درست می‌کنند و الی آخر گرچه شرکتهای معتبر مانند گوگل و یاهو دامنه‌ها بسیاری شیبه به دامنه آدرس اصلی وب سایت خود روزو کردند اما بازهم نمی‌توان تمام موارد را رزو کنید.

این روش کاملاً به ابتکار هکر در اغفال شما بستگی دارد. به گونه‌ای که ندانسته رمز عبور خود را در اختیارش قرار می‌دهید و به تعداد افراد مبتکر، احتمال وجود روش‌های مختلف هست. یکی از روشهایی را که خیلی معمول شده است بررسی می گردد.

در این روش، فرد هکر برای خود در یاهو یک آدرس ایمیل غلط انداز ایجاد می‌کند که شمارا به اشتباه خواهد انداخت و شما تصور خواهید کرد که این آدرس ایمیل مربوط به یکی از دست اندرکاران یاهو است و به آن اعتماد می‌کنید. هکر وانمود می‌کند که از شیوه‌ای باخبر است که توسط این شیوه شما قادر خواهید بود کلمه عبور هر فردی را که بخواهید بدست بیاورید. شما هم که به دنبال چنین راه حلی می‌گشتید از او درخواست می‌کنید که این راه را به شما بیاموزد و او هم که درصد چنین فرصتی بوده است بی درنگ کار خود را شروع می‌کند.

هکر به شما توضیح می‌دهد که به آدرس ایمیلی که در بالا به آن اشاره شد یک ایمیل بفرست. البته این نامه حتماً دارای شرایطی باشد که وی به شما بگوید. مثلاً موضوعش فلان جمله باشد و حتماً با جمله خاص پایان پذیرد و با ساختن یکسری کدهای خاص ذهن کاربر را منحرف ساخته و کاربر را وادار می‌سازد به‌طور ناخواسته نام کاربری و رمز عبوری خود را در لابلای نامه وارد وارسال نماید و سرانجام منتظر است تا اطلاعات خواسته شده در مورد فرد دیگر را دریافت نماید ولی هرگز چنین نامه‌ای از طرف یاهو به دست او نخواهد رسید.

خوب زمانی ترفندها ابتکاری باشد، مقابله با ترفندها هم ابتکاری و منحصر به فرد است، البته برخی از قوانین است که اجتناب ناپذیر است، از جمله اینکه تا خود کاربر، کمک نکند، هیچ نفوذگری نمی‌تواند کاری انجام دهد، سست‌ترین عنصر در امنیت شبکه، انسان است که درمقابل می‌تواند، نفوذناپذیر عنصر در امنیت شبکه عمل کند. تأمل کنید، به خوبی واضح و بدیهی است.

## **مهندسی اجتماعی چیست؟**

به هنگام ثبت نام در یاهو یا هر سرویس پست الکترونیکی دیگر، نسبت به پیش گزینه وبسایت، سوالاتی در زمینه تاریخ تولد، کد پستی، کشور، سؤال کوتاه و جواب کوتاه و یک آدرس ایمیل برای مواقع اضطراری می‌پرسد که خیلی مهم هستند. این موارد را همیشه به خاطر داشته باشید که اگر کسی رمز عبور خود را فراموش کند و اطلاعاتی را که در بالا به آن‌ها اشاره شد را به خاطر داشته باشد به راحتی می‌تواند رمز عبور خود را به دست آورد.

چگونه؟ بسیار ساده است، سرویس فراموشی رمز عبور، یا در برخی وبسایتها رمزعبور را گم کرده‌ام که عبارتی شبیه به [Forget your ID or password?](http://us.rd.yahoo.com/reg/login1/lisu/forgot/us/ym/*http:/edit.yahoo.com/config/eval_forgot_pw?new=1&.done=http://edit.yahoo.com/config/mail&.src=ym&partner=&.partner=&.intl=us&pkg=&stepid=&.pd=ym_ver%3d0&.last=) در سایت مثل یاهو ویا فراموشی رمز عبور در وبسایتها چنین عمل می‌کند که نام کاربری و ایمیل ثبت نام کردید را می‌گیرد و برایتان یک رمز عبور جدید به ایمیل ارسال می‌کند.

اما اگر رمز عبور ایمیل را فراموش کنید در سایت مثل یاهو یا جی میل یا هات میل در مورد تاریخ تولد، کد پستی، کشور از شما سؤال می‌شود، مهم نیست که به‌صورت واقعی چیست، برای وب سایت مهم است آنچه در زمان ثبت نام از این مشخصه‌ها وارد کردید را دوباره وارد کنید تا مطمن شود که صاحب و مالک صندوق پستی و ای دی خود شما هستید و اینچنین فرصت ورود به پست الکترونیکی شمارا می‌دهد.

حال تصور کنید که هکرها نیز این نکته بسیار ساده را نیز می‌دانند و یکی از شیوه‌هایی که احیاناً به کار می‌گیرند. همین مهندسی اجتماعی است. یعنی به شیوه‌های گوناگون طرح دوستی با شما می‌ریزند و سعی می‌کنند تا اطلاعات کلیدی را از شما جمع آوری کرده و در یک فرصت مناسب از همان ترفندی که در بالا اشاره شد رمز عبور شمارا به دست بیاورند. در بخشهای بعدی نیز در ارتباط با مهندسی اجتمایی بیشتر بررسی می گردد.

برای مقابله با مهندسی اجتماعی با از مهندسی اجتماعی بهره ببرید، ابتدا که سعی کنید، مطالب درج شده، زیاد حقیقی نباشد و حتی نزدیک نباشد، فراتر از کرک شدن ایمیل، سعی کنید، از نام و مشخصات فردی اصلی خود در این سرویسها کمتر استفاده کنید، مگر اینکه مجبور به ورود اطلاعات درست و کامل خود باشید، مثلاً برخی از ارگانها برای ارائه خدمات به وسیله پست الکترونیکی معتبر با مشخصات حقیقی می‌خواهند یا یک وب سایت که اعضا خود جایزه می‌دهد برای احراز هویت شما، به هویت حقیقی اتان در هنگام ثبت نام احتیاج دارد، در یک جمله، سعی کنید که از مشخصات اصلی بهره نبرید.

دوم هم سعی کنید که مشخصات خود را به دوستان و دیگران نگوید، در روی کامپیوتر نگهداری نکنید، و حتی برروی کاغذ اداری خود ننویسید، ممکن است همین دوست شما که گفته‌اید تاریخ مندرج در یاهو چیست فردا شمارا به شوخی کرک کند.

یک نکته اساسی هم در ثبت نام در وبسایتها مختلف از مشخصه‌های واحد استفاده نکنید به خصوص رمز عبور و رمز عبور، دلیلش هم واضح است در صورت افشا شدن مشخصه‌های مندرج در یک وبسایت، بقیه عضویت و شناسه کاربری شما مورد نفوذ قرار می‌گیرد مگر اینکه از مشخصه‌های گوناگون بهره ببرید.

## **تروجان ها**

به بیان خیلی ساده تروجان ها برنامه‌هایی هستند که به‌صورت غیر مجازی روی سیستم شما اجرا می‌شوند و امکان دسترسی به اطلاعات محرمانه و همچنین کنترل سیستم شمارا به فرد هکر می هند. یاهو در این زمینه اقدماتی را انجام داده است که به درد چنین مواقعی می‌خورد.

در چنین مواقعی از امکان فراموشی رمز عبور استفاده شود. اما به چند شرط:

سوالاتی را که یاهو به هنگام ثبت نام می‌پرسد همیشه به خاطر داشت باشید که اگر کسی شمارا هک کرد و بتوانید از این طریق پسوردتان را بگیرید و تغییر دهید.

برای این کار در صفحه ورود روی گزینه Password Lookup کلیک کنید. بعد از وارد کردن این اطلاعات یاهو درست بودن آن‌ها را چک می‌کند. در این مرحله که به‌منظور ایجاد امنیت بیش‌تر ایجاد شده یاهو از شما یک سؤال کوتاه می‌پرسد و شما باید آن پاسخ صحیح دهید. البته دقت کنید که این پرسش و پاسخ را خود شما هنگام ثبت نام تعریف کرده‌اید. بعد از وارد کردن پاسخ کوتاه در صورت درست بودن آن شما قادر خواهید بود به دو صورت موجود رمز عبوری خود را تغییر داده و تصاحب کنید. یکی Display New Password که به شما رمز عبور جدیدتان را نشان می‌دهد و دیگر Email New Password که رمز عبور جدید شمارا به آدرس ایمیلی که به هنگام ثبت نام داده‌اید ایمیل می‌کند. البته استفاده از گزینه اول بهتر است چرا که وقتی که یک نام کاربری هک می‌شود، هکرها ایمیل پشتیبان را نیز هک می‌کنند.

## **تکنیک‌های انتخاب کلمه عبور**

به یاد داشته باشید شناسه کاربری و کلمه عبور رمز عبور تمام هویت مجازی و حق مالکیت شماست، بدین معنی که برای اتصال به اینترنت، ورود به شبکه، انواع و اقسام پیام رسان‌ها و سایتها، چک کردن ایمیل[[9]](#footnote-9)، بالا آمدن ویندوز محافظ صفحه نمایش و خلاصه برای هر تمام سرویسها خصوصی یا اختصاصی در دنیای کامپیوتر شناسه کاربری و کلمه عبور رمز عبور، هویت شمارا احراز می کندو در صورت از دست دادن آن‌ها، مالکیت خود را بر دارایی‌های مجازی خود از دست می‌دهید.

اگر در دنیای کامپیوتر، تا حدی پرسه زده‌اید و با علوم پایه کامپیوتر و فن‌آوری اطلاعات آشنا باشید حتمی می دانید کلمه عبور رمز عبور چیست، یک عبارات از مجموعه حرف، عدد و دیگر کاراکترها که در هنگام ورود به سیستم یا سرویس خاص از کاربر خواسته می‌شود، معمولاً در سیستم‌ها و سرویسهای مختلف از جمله شبکه‌های کامپیوتری با شناسه کاربری و کلمه عبور رمز عبور، هویت شخص محرز می‌شود. البته در دنیا امروزی از علوم بیومتریک، سوییچ‌ها سخت افزاری و ابراز آنلاین برای حفظ و نگهداری رمزعبور وهویت مجازی شما بهره برده‌اند.

امروزه برای حفظ اطلاعات و امنیت بیشتر در دنیای کامپیوتر و اینترنت، نیاز به کلمه عبور انکار ناپذیر است.

به عنوان مثال: برای اتصال به اینترنت، ورود به شبکه، انواع و اقسام پیام رسان‌ها و سایتها، چک کردن، بالا آمدن ویندوز محافظ صفحه نمایش و خلاصه برای هر چیز که فکرش را بکنید، ممکن است کلمه عبور وجود داشته باشد.

از سوی دیگر، به خاطر سپردن این همه کلمه عبور و محافظت از آن‌ها کار مشکلی است. شاید تا بحال برایتان پیش آمده که کلمه عبور خود را فراموش کرده باشید و یا بدون اینکه اطلاع داشته باشید، کسی به کلمه عبورتان دست پیدا کند.

در واقع انتخاب کلمه عبور مناسب و مطمئن که به راحتی توسط افراد سودجو و هکرها قابل دسترسی نباشد و همچنین حفظ آن، خود یک هنر است.

در نظر داشته باشید، ممکن است یک عبارت طولانی و پیچیده که ترکیبی از حروف، اعداد، و علامت‌های مختلف باشد، انتخاب خوبی برای کلمه عبور به نظر برسد.

پست الکترونیکی شما بر سرویسهای معتبر بین المللی مانند یاهو، جی میل گوگل و یا هات میل مایکروسافت هک نمی‌شوند، کمتر اتفاق افتاده که سرویس‌های وبلاگ‌ها مانند پرشین بلاگ، میهن بلاگ و بلاگفا هک شود. بلکه آنچه اتفاق می افتد، از دست دادن رمز عبور ایمیل یا وبلاگ و یا.... توسط خود کاربر است و هرگز هک یا نفوذ دیگری درکار نیست.

به هر صورت فراموش نکنید که در دنیای امروز، اغلب نفوذگران، صرفاً با وقت گذاشتن بر روی کشف کلمه عبور، به سیستم‌ها نفوذ می‌کند و در حقیقت در ۹۰ درصد موارد، اگر کلمه عبور کشف نشود، حتی خبره‌ترین هکرها قادر به هک کردن سیستم‌ها نیستند و با دیواری نفوذ ناپذیر و ستبر مواجه می‌شوند.

تا حدی که می‌توانید کلمه عبور را پیچیده کنید اما این پیچیدگی باعث سردرگمی و فراموشی کلمه عبور شما نشود.کلمات عبور کوتاه بدترین حالت انتخاب رمزعبور است، به سادگی قابل حدس زدن هستند

در نوشتن کلمات از حروف کوچک و بزرگ و اعداد با هم، و به‌صورت ترکیبی استفاده کنید و امنیت آن را بالاتر ببرید. توصیه من این است از کاراکترهای ویژه نظیر (!@#$%^&\* \_) بهره ببرید البته به خاطر سپردن آن کمی مشکل است.

می‌توانید از کلمات پین انگلیش بهره ببرید، مانند سلام به‌صورت Salam پین انگلیش که آشنایی دارید کلمات فارسی با بهره گیری از حروف و کاراکترها انگلیسی با همان طرز تلفظ فارسی را پین انگلیش گفته می‌شود، حتی برخی از سرویسها از کاراکتر فارسی را پشتیبانی می‌کنند و یا ترکیب حروف فارسی و انگلیسی را می‌توانید به کار ببرید. از کلید میانبر Shift هم استفاده کنید،

از کلمات مرتبط با یک موضوع استفاده کنید. مثلاً یک موضوع واحد را در نظر بگیرید، فرضاً یک سفر به یاد ماندنی، یک ماشین جدید، تولد یک بچه یا ... و آن وقت کلماتی را که مرتبط با آن موضوع خاص هستند، در کنار هم بگذارید.

مثلاً در مورد یک ماشین جدید می‌توان رنگ بدنه، قیمت، روز خرید یا ... را در نظر بگیرید. با این کار به خاطر سپردن کلمه عبور برایتان ساده خواهد بود.

البته این روش یک مزیت دارد و این موضوع که کمتر اتفاق می افتد که شما رمز عبورتان را فراموش کنید، این مقوله مطلوب است اما ممکن است دچار مهندسی اجتماعی هکرها شوید.

یکی از روشهای به دست آوردن رمز عبور توسط هکر، به خصوص هکر آشنا، حدس رمز عبور است، اینچنین که حروف مرتبط کنارهم بچینند، هکر با توجه به خلقیات هدف، تجربه و روانشناختی که از آن آگاهی دارد، شاید بتواند راحت‌تر حدس و گمان خود را به واقعیت نزدیک کند.

با کمی تخیل می‌توان ارقام را به حروف شبیه آن تبدیل کرد. با این ترفند می‌توانید در کلمات به جای برخی از حروف، عدد شبیه آن را قرار دهید، به‌عنوان مثال به جای کلمه " BOOK "، عبارت " ۸۰۰K " و یا به جای کلمه " ALIREZA " از عبارت " ۴۱IR۳۷۴ " استفاده کنید.

می‌توانید از اعداد در مبنای هگزا نیز بهره ببرید، مانند 1FA234E به جای شماره شناسنامه شما که 1234 است، اینگونه هر موقع که کلمه عبور را فراموش کردید شماره شناسنامه خود را با کامپیوتر یا ماشین حساب به مبنا هگزا تبدیل می‌کنید و...

یک ترفند دیگر استفاده از حروف و اعداد، بسته به موقعیت مکانی آن‌ها روی صفحه کلید است. سری بالایی ردیفهای حروف صفحه کلید QWERTYUIOP را در نظر بگیرید، در بالای هر یک از این حروف یک عدد وجود دارد و شما می‌توانید حروف را با این اعداد جایگزین کنید. مثلاً به جای کلمه " blue " از عبارت " bl۷۳ " استفاده کنید.

همان گونه که قبلاً هم گفتیم بهتر است از ترکیبی از حروف کوچک و بزرگ استفاده کنید. مثلاً به جای بزرگ نوشتن اولین حرف هر کلمه، حرف دوم تمامی کلمات را بزرگ بنویسید، و یا حروف دوم و سوم تمامی کلمات را بزرگ بنویسید. مثلاً " bOoK " یا " wHiTe ".

این کار با گرفتن کلیدصفحه کلید به نام Shift و یا رها کردن آن امکان پذیر است، بازهم تاکید می‌کنم وجود منطق و مبنا در رمز عبور، باعث می‌شود که آن را فراموش نکنید اما ممکن است حدس زدن هکر و به اصطلاح مهندسی اجتماعی وی را راحت و سهل کنید.

منظورم همان کلمه عبور یا رمز عبور است، سعی کنید که به‌طور متوالی و ممتد کلمه عبورتان را تغییر دهید

در موارد ویژه که کلمه عبور دارای اهمیت خاص بوده و تقریباً از لحاظ حفظ منافع اطلاعاتی یا اقتصادی دارای اهمیت حیاتی باشد، برای در امان ماندن از دست افراد سود جو / رقبا و ...، آن‌ها را به‌طور هفتگی یا حداکثر ماهیانه عوض کنید.

اگر مجبور شدید در اماکن عمومی مانند کافی نت، یا مرکزکامپیوتر دانشگاه از رمزعبورتان استفاده کنید، در فضا امن مانند کامپیوتر شخصی، در اولین فرصت رمز عبور را تغییر دهید، ضمن اینکه در هنگام تغییر کلمه رمز، هرکز از کلمات و اطلاعات مشابه استفاده نکنید. در واقع کلماتی مانند Alijan۰۱، Alifeb۰۲، Alimar۰۳ و ... مناسب نیستند، چرا که اگر فردی کلمات عبور قبلی شمارا پیدا کرده باشد، به راحتی می‌تواند کمله عبور جدید شمارا حدس بزند و با کمی سعی و تلاش به آن دست بیابد. حتی منطق و مبنا و چیدمان آن را جدید کنید، مثلاً از ترکیب حروف کوچک و بزرگ استفاده کرید این بار ازترکیب اعداد و کارکتر ویژه (&^%$#) بهره ببرید.

این توصیه برای افرادی که در چندین وبلاگ، ایمیل و سرویسها مختلف دارای کلمه عبور هستند البته داشتن چند کلمه عبور به دلیل تنوع خدمات آنلاین امری گریزناپذیر است، برخی برای حل کردن مشکل فراموشی کلمه عبور سعی می‌کنند از یک کلمه عبور واحد در سرویسهای مختلف بهره ببرند، خوب مشکل مرتفع شد اما اگر به هر دلیل یکی از رمزهای عبور شما گم یا سرقت شود شما تمام سرویسها و دارایی مجازی خود را از دست می‌دهید که مطلوب نیست.

### استاندارد ISO ۱۷۷۹۹

شاید برایتان جالب باشد اگر بدانید برای انتخاب کلمات عبور، یک استاندارد جهانی وجود دارد. در این استاندارد راهنمایی‌های خوبی در زمینه انتخاب کلمه عبور ارائه شده است که چند نمونه از آن را مشاهده می‌کنید:

1- تعداد کاراکترهای یک کلمه رمز، باید حداقل شش حرف باشد. البته بهتر است طول را کمی بیشتر از شش حرف بگیرید و حداقل هشت حرف را در نظر داشته باشید. مطمئن باشید که حدس زدن کلمات عبور که کوتاه‌ترند، برای هکرها بسیار ساده است، ضمن اینکه در زمان کمتری به کشف آن نائل می‌شوند. در حقیقت کافی است توسط یک برنامه ویژه کشف رمز، به روش سعی و خطا، ترکیبی از تمامی حروف، ارقام و علامتها را چگ کنند تا در نهایت به کلمه رمز شما دست پیدا کنند.

2- هیچ گاه در کلمات عبور، از حرف یا کلمات پشت سر هم یا متوالی (چه ازنظر الفبایی و چه بر اساس موقعیت روی صفحه کلید) استفاده نکنید. به عنوان مثال کلمات، " asdfghkl "، " ۳۴۵۶۷۸۹ "، "abcdefg " مناسب نیستند.

3- تمامی کاراکترهای کلمه عبور، نباید فقط حرف یا فقط کلمه باشند.

4- از استفاده مجدد یا دوره نموده کلمات عبور قدیمی جداً بپرهیزید.

5- کلمات عبور را هر چند وقت یک بار تغییر دهید

6- اگر مدیر یک شبکه هستید و در هنگام معرفی کردن کاربران به شبکه، برای آن‌ها کلمه عبور گذاشته‌اید، آن‌ها را مجبور کنید تا وقتی برای اولین بار به شبکه وصل شدند، کلمه عبور (کلمه عبور پیش فرض) خود را تغییر دهند.

7- از استفاده از کلمه عبور اشتراکی برای کاربران بپرهیزید. سری به سایت www.secaritystats.com بزنید و از قسمت Awareness tools آن، گزینه strength رمز عبور را انتخاب کنید. با این ابزار جالب می‌توانید کلمات عبور خود را ازنظر میزان امنیت، پیچیدگی و قابل حدس بودن بسنجید.

به عنوان مثال یک کلمه عبور ساده مثلاً abcd را وارد کنید، به شما می‌گوید که این کلمه خیلی ضعیف است و به شماراهکارهایی برای انتخاب کلمه عبور قویتر ارائه می‌کند. به عنوان مثال پیشنهاد می‌کند تعداد حروف را افزایش دهید و از اعداد و علامتها هم استفاده کنید. هم چنین کلمات متفاوت را امتحان کنید و نتیجه را بررسی کنید. همانگونه که در خود سایت ذکر شده است، کلمات عبوری که وارد می‌کنید، در هیچ جایی ثبت و ذخیره نمی‌شود، ولی از آن جایی که محیط اینترنت بسیار ناامن است، بهتر است هیچ گاه کلمات عبور واقعی خود را در این سایت وارد نکنید. البته می‌توانید از کلماتی مشابه با کلمات اصلی رمز خود استفاده کنید.

البته امروزه در دنیا با استفاده از علم بیومتریک و مشخصه طبیعی نظیر، اثرانگشت، ساختار عینبیه چشم، ترکیب صورت کاربر، دیگر لازم نیست کلمه عبور داشت، ولی در مجموع هنوز این علم جای کلمه عبور در قالب کاراکترها را نگرفته است.

یک روش دیگر هم سوییچ‌ها نگهدارنده رمزعبور که در این خصوص کارها و آزمایشاتی انجام شده است، به گونه‌ای که رمز عبور به وسیله سخت افزارهای قابل حمل که به کامپیوتر وصل می‌شود، ذخیره می‌شود و در هنگام استفاده از رمز عبور، سخت افزار را به کامپیوتر وصل نموده و از آن استفاده می‌کنند.

یک روش دیگر، نگهداری آنلاین رمزعبور در اینترنت است، با عضو شدن در برخی از وبسایتها، می‌توانید تمام کلمات عبور و شناسه کاربری همراه با نام وبسایت و سرویس مربوط به آن را یکجا ذخیره می‌کنید شما به ازای نگهداری و حفظ دهها رمزعبور وبلاگ، ایمیل، شبکه و .... یک رمزعبور وب سایت مذکور را حفظ می‌کنید، البته این وبسایتها از لحاظ امنیت شبکه و حفظ اسرار شما مطمن و دارای گواهینامه معتبر بین المللی IIS هستند.

## **فیشینگ[[10]](#footnote-10) چیست؟**

فیشینگ، به معنای کپی همانند سازی شده از یک صفحه اینترنتی آشنا است که کاربر را گمراه کرده و در واقع وسیله‌ای برای به دست آوردن اطلاعات شخصی وی به شمار می‌آید.

همه روزه درباره نامه‌های الکترونیکی دروغین یا تقلبی مطالبی به گوش می رسد. این نامه‌های دروغین، که وسیله فریب به شمار می‌آیند، در ظاهر از یک آدرس اینترنتی قانونی و با یک خواسته موجه برای اشخاص ارسال می‌شوند و معمولاً برای این منظور به کار می‌روند که اطلاعات شخصی یا جزئیات حساب‌های اینترنتی یا بانکی شمارا بررسی و نسخه برداری کنند.

یک مثال می‌تواند این باشد که شما ایمیلی دریافت می‌کنید که ظاهراً از بانک فرستاده شده و در آن از شما خواسته شده که بر روی یک لینک کلیک کرده و مشخصات بانکی خود را بازبینی نمایید. معمولاً در چنین مواقعی یک اخطار در برابر تعقیب نکردن لینک وجود دارد، از جمله اینکه کلیک نکردن آن موجب بسته شدن یا معلق شدن حساب بانکی شما خواهد شد.

هدف فرستنده این ایمیل، این است که شما اطلاعات خصوصی خود شامل رمز عبور، شماره ملی، شماره حساب بانکی و مانند آن‌ها را فاش کنید. به فرستادن چنین ایمیل‌هایی فیشینگ نیز میگویند. ]9[

ممکن است گیرنده چنین ایمیلی در نگاه اول متوجه نشود که این نامه از طرف شرکتی که با او کار می‌کند نیست و اصلاً هیچ پشتوانه قانونی ندارد. بخش فرستنده یا from در این ایمیل می‌تواند حاوی آدرس واقعی شرکت یا کمپانی مورد اشاره باشد و لینک موجود هم ظاهراً قرار است کاربر را به وب سایت قانونی و رسمی شرکت رهنمون شود، اما در واقع کاربر به یک سایت جعلی راهنمایی می‌شود. ]8[

ظاهر یک ایمیل برای فیشینگ می‌تواند بسیار فریبنده باشد اما مهم این است که این نامه‌ها هرگز از طرف شخص یا جایی که ادعا می‌کند، فرستاده نشده است.

به خاطر داشته باشید، مدیران فنی وبسایتها به ایمیل شما، رمز عبور و شناسه کاربری و ... و تمام اطلاعات شما دسترسی کامل دارند، بدین معنا که با مراجعه به نرم‌افزار مدیریت محتوا وبسایت کلیه مشخصات یک کاربر و حتی صفحات بازدیدشده شمارا دارند، پس به شما ایمیل زده نمی‌شود که پسوردی داده شود. در مقابل نیز فراموش نکنید به‌منظور احراز هویت، مالکیت، نظرسنجی، امارگیری و هر دلیل و بهانه‌ای دیگر مدیر وبسایت با شما تماس نمی‌گیرد و یا اینکه بخواهد فعالیتها ازجمله کلیک، ارسال پیام و ... انجام دهید، اگر این را به عنوان یک اصل امنیت شبکه در کار با اینترنت به کارببرید فیشینگ نمی‌شوید. ]12[

### مشخصات عمومی و مشترک بین پست الکترونیکی با هدف فیشینگ

1-   آدرس موجود در قسمت مربوط به فرستنده یا فرم، ظاهراً از طرف کمپانی قانونی است. مهم این است که بدانیم تغییر دادن اطلاعات این قسمت کار بسیار ساده‌ای است.

2-      این ایمیل‌ها معمولاً شامل نشانه یا تصاویری هستند که از وب سایت کمپانی اصلی برداشته شده‌اند.

3-   ایمیل دارای یک لینک قابل کلیک شدن است که با توضیحی همراه است که برای معتبر ساختن یا تمدید اعتبار باید آنرا کلیک کرد. به محض انتخاب کردن این لینک می‌توان در گوشه چپ صفحه آدرسی را مشاهده کرد که در اصل آدرس واقعی وب سایتی است، که در صورت کلیک کردن به آن خواهد رفت. توجه کنید که این لینک به آدرس قانونی‌ای که انتظار می رود منتهی نمی‌شود.

افرادی که در پس پرده فیشینگ هستند، به پسورد، شناسه کاربری، کدملی و .... دیگر مشخصات مجازی شما کار دارند، حتی ممکن این این فرد برادرتان باشد که می‌خواهد از موجودی بانکتان خبردارد شود یا همین دوستتان، شاید خورده حسابی باهم دارید و هر فردی که مشخصات و هویت اینترنتی شما برایش فایده دارد. البته ممکن است افرادی هم نه شما قربانی را بشناسند و نه شما او را حتی کشور و منطقه شمارا نمی‌دانند، این افراد، متخصصین جعل اینترنتی هستند. آن‌ها به معنای واقعی کلمه، میلیون‌ها ایمیل جعلی را پست می‌کنند به امید اینکه در نهایت تعداد اندکی به آن‌ها پاسخ داده و اطلاعات خود را در اختیارشان قرار دهند.

هر کسی که دارای یک آدرس ایمیل باشد در خطر دریافت چنین نامه‌هایی هست حال ممکن است شما شناخته شده و هدفمند انتخاب شوید، همان مثالی که زدم مثلاً فلان دوستی برای دستیابی به صندوق پست الکترونیکی یا ایمیل باکس شما، سعی می‌کند با یک فرم جعلی آن را از شما بگیرد.

شاید هم شما به‌عنوان قربانی میان میلیونها نفر باشد، آدرسی که با وارد کردن آن در گروهها، خبرنامه‌ها و دیگر وب سایتهای خدماتی، در اینترنت جنبه عمومی پیدا کرده باشد بیشتر در معرض فیشینگ خواهد بود زیرا نشانی الکترونیک می‌تواند توسط اسپایدرهایی[[11]](#footnote-11) برنامه‌هایی که به‌صورت خودکار در وب می‌گردند و اطلاعات را جمع آوری می‌نمایند) که کارشان تصرف هرچه بیشتر آدرس الکترونیک است، غصب شود. به این ترتیب به دست آوردن اطلاعات اولیه برای جاعلان خرجی ندارد.

### قانون طلایی مواجهه با عملیات فیشینگ

1-   یادتان باشد، ممکن است عمل فیشینگ توسط هر فرد و یا با هر عنوانی انجام شود، شایدهم افرادی با جعل ایمیل دوستان نزدیک یا خانواده اتان سعی کنند برخی از اطلاعات مالی شمارادریابند پس به هیچ ایمیل و صفحه اینترنتی اعتماد نکنید، به یادداشته باشد همه صفحات قابل جعل و تقلب هستند.

2-   یادتان باشد از سوی هیج یک از مدیران وبسایتها، اطلاعات شما درخواست نمی‌شود، احراز هویت، نظرسنجی، تغییر سرور و کلمات گاه گیج کننده باعث نشود که شما اطلاعات خود را در اختیار افراد سودجو و خلاف کار اینترنتی قرار دهید.

3-   قانون طلایی برای جلوگیری از فریب خوردن توسط فیشینگ، این است که هرگز بر روی لینکهای موجود در متن نامه کلیک نشود و همواره چنین ایمیلی را بلافاصله پاک کرده و پس از آن قسمت زباله[[12]](#footnote-12) را هم خالی کرد تا از کلیک اتفاقی بر روی آن جلوگیری شود.

اگر به هر دلیل غریبی دارای احساس آزارنده‌ای شدید که ممکن است این یک ایمیل واقعی باشد و آنرا باز کردید هم، به قانون طلایی توجه کنید و روی هیچ لینکی کلیک نکنید. کسانی که واقعاً از به مخاطره افتادن حساب خود وحشت دارند و می‌خواهند اطلاعات خود را تأیید نمایند، باید یک صفحه جدید باز کرده و نشانی وب سایت "واقعی" را در محل آدرس مرورگر وارد کنند و همانطور که همیشه وارد این وب سایت می‌شده‌اند به آن واردشده و اطلاعات شخصی خود را چک کنند.

این کار را در جریان آخرین اخبار سایت و حساب خودتان قرار می‌دهد و هرگونه احتمال پاسخ به یک نامه جعلی را هم برطرف می‌نماید.

البته وبسایتها معتبر، هر گاه یک نظر سنجی یا فعالیتی منحصر به اعضا خود داشته باشند علاوه بر ارسال پست الکترونیکی، در قسمت اخبار مربوطه به وبسایت و یا وبلاگ مدیر وبسایت قرار می‌دهند، بدین صورت هم به مسله مطمن می‌شوید، البته ممکن است، یک نفوذگر از فرصت استفاده کند و موازی مدیر وبسایت عمل کند، برای جلوگیری از هر نوع دزدی وسرقت هویت و مشخصات مجازی، وبسایتها سعی می‌کنند که نظرسنجی، آمارگیری و .... در صفحه اصلی وبسایت و از طریق صفحات وبسایت انجام دهند تا امکان تقلب دیگران صفر شود. پس اول و تنها به وبسایتتا ن مراجعه کنید.

برخی از نرم‌افزارها هم با درج آدرس اینترنتی از معتبر بودن یا جعلی بودن آدرس بدون هرگونه خطری را اعلام می‌کنند البته این نرم‌افزارها همیشه کارایی ندارد.

می‌توان برای تأثیر بیشتر در سرنوشت ایمیل‌ها، مراتب را به کمپانی یا وب سایت اطلاع داد. بسیاری از شرکتها و کمپانیها نگران سوءاستفاده از نام شرکت خود هستند و چنین نامه‌های جعلی را پیگیری می‌کنند.

یکی از این روشهای فیشینگ، متمرکز شدن بر یک کاربر خاص یا یک حوزه خاص در یک تشکیلات است. نامه جعلی ظاهراً بدون هیچ مورد غیر قانونی از طرف یکی از اعضای کمپانی ارسال می‌شود و طوری نوشته شده است که گویا شخص فرستنده تنها به شخص گیرنده اعتماد دارد و از او کمک می‌خواهد و خواسته است تا او رمز یا رمزهای عبور و یا شناسه کاربری را برایش بفرستد.

این روش با بهره بردن از ذکر نام یک شخص حقیقی به جای یک سیستم پشتیبانی، اعتماد بیشتری را جلب می‌کند و گاهی از کاربر می‌خواهد که به دلیل خاصی اطلاعات خود را به روز درآورده یا صحت آن‌ها را بررسی کند. به این ترتیب جاعلان و سوءاستفاده گران وارد سیستم امن شبکه یک شرکت می‌شوند.

یک روشی که آخرین بار برای کاربران وبسایت گوگل اتفاق افتاد این بود که به وسیله و ترفند مختلف مانند کلیک کردن بر روی یک لینک، نرم‌افزارهای جاسوسی[[13]](#footnote-13) را وارد سیستم می‌کند. این جاسوس افزار که در قالب یک کد مخرب است هیچ تخریب یا عمل دیگری انجام نمی‌دهد. اما هنگامی که کاربر آدرس یک وبسایت مانند گوگل [http://www.google.com](http://www.google.com/) درج می‌کند، این نرم‌افزار به کار افتاده و کاربر را به‌صورت خودکار به یک وبسایت جعلی که مانند گوگل هست هدایت می‌کند حال شما می‌خواهید پست الکترونیکی خود در جی میل چک کنید وارد باکس جی میل البته در وبسایت جعلی شده و با وارد کردن پسورد و شناسه کاربری، شما پسورد وشناسه کاربری اصلی گوگل خود را از دست می‌دهید یا در مواردی گوگل جعلی از شما می‌خواهد که مشخصات یک فرم را پر کنید، و اینگونه بدون هیچ مشکلی فیشینگ می‌شود. ]10[

## **روش‌های معمول حمله به کامپیوترها**

قصد داریم بطور خلاصه به معمول‌ترین روش‌هایی که مورد استفاده خرابکاران برای ورود به کامپیوتر یا از کارانداختن آن قرارمی‌گیرد، اشاره کنیم.

1)      برنامه‌های اسب تروآ

2)      درهای پشتی و برنامه‌های مدیریت از راه دور

3)      عدم پذیرش سرویس

4)      وساطت برای یک حمله دیگر

5)      اشتراک‌های ویندوزی حفاظت‌نشده

6)      کدهای قابل انتقال Java، JavaScript و اکتیو ایکس

7)      اسکریپت‌های Cross-Site

8)      ایمیل‌های جعلی

9)      ویروس‌های داخل ایمیل

10)   پسوندهای مخفی فایل

11)   سرویس‌گیرندگان چت

12)   شنود بسته‌های اطلاعات

### برنامه‌های اسب تروآ

برنامه‌های اسب تروآ روشی معمول برای گول زدن شما هستند (گاهی مهندسی اجتماعی نیز گفته می‌شود) پیکربندی سیستم شمارا تغییر می‌دهند، یا کامپیوترتان را با یک ویروس آلوده می‌کنند.

روی کامپیوترهای ویندوزی، معمولاً سه ابزار توسط مزاحمین برای دسترسی از راه دور به کامپیوترتان استفاده می‌شود. BackOrifice، Netbus و SubSeven، این برنامه‌های درپشتی یا مدیریت از راه‌دور وقتی نصب می‌شوند، به افراد دیگر اجازه دسترسی و کنترل کامپیوتر را می‌دهند.

نوعی دیگر از حمله، DOS[[14]](#footnote-14) یا عدم‌پذیرش‌سرویس نام دارد. این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از حد کامپیوتر تا حد غیرقابل‌استفاده شدن می‌شود. در بیشتر موارد، آخرین وصله‌های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می‌گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود.

مزاحمین به‌کرات از کامپیوترهای مورد حمله قرارگرفته برای پایگاهی برای حمله به دستگاه‌های دیگر استفاده می‌کنند. یک مثال آن چگونگی استفاده از آن‌ها به‌عنوان ابزار حملات DoS توزیع‌شده است. مزاحمین یک عامل را (معمولاً از طریق یک اسب تروآ) نصب می‌کنند که روی کامپیوتر مورد حمله قرارگرفته اجرا می‌شود و منتظر دستورهای بعدی می‌ماند. سپس، هنگامی که تعدادی از عامل‌ها روی کامپیوترهای مختلف در حال اجرا هستند، به تمام آن‌ها دستور داده می‌شود که یک حمله DOS را روی یک سیستم پیاده کنند. بنابراین، هدف نهایی حمله، کامپیوتر شما نیست، بلکه سیستم شخص دیگری است، کامپیوتر شما فقط یک ابزار مناسب برای یک حمله بزرگتر است.

 اشتراک‌های شبکه ویندوزی محافظت‌نشده می‌توانند توسط مزاحمین تحت یک روش خودکار برای قراردادن ابزارها روی تعداد زیادی از کامپیوترهای ویندوزی متصل به اینترنت مورد سوءاستفاده قرار گیرند. از آنجا که برای امنیت سایت روی اینترنت وابستگی بین سیستمها وجود دارد، یک کامپیوتر مورد حمله قرارگرفته نه تنها مشکلاتی برای صاحبش فراهم می‌کند، بلکه تهدیدی برای سایتهای دیگر روی اینترنت محسوب می‌شود. عامل بالقوه بزرگی در گستره وسیع برای ظهور ناگهانی سایر ابزارهای مزاحمت وجود دارد که از اشتراکهای شبکه ویندوزی محافظت‌نشده استفاده می‌کند.

گزارش‌هایی در مورد مشکلات با کدهای سیار مانند جاوا[[15]](#footnote-15)، جاوا اسکریپت[[16]](#footnote-16) و اکتیو ایکس[[17]](#footnote-17) وجود داشته است. این‌ها زبانهای برنامه‌سازی هستند که به توسعه‌دهندگان وب اجازه نوشتن کدهای قابل اجرا در مرورگر را می‌دهند. اگرچه کد عموماً مفید است،‌ اما می‌تواند توسط مزاحمان برای جمع‌آوری اطلاعات (مثلاً وب‌سایتهایی که سر می‌زنید) یا اجرای کدهای آسیب‌رسان روی کامپیوتر مورد استفاده قرار گیرد. امکان از کار انداختن جاوا ، جاوا اسکریپت و اکتیو ایکس در مرورگر وجود دارد. توصیه می‌شود که اگر در حال مرور وب‌سایتهایی هستید که با آن‌ها آشنا نیستید یا اطمینان ندارید، این کار را انجام دهید، اگرچه از خطرات احتمالی در استفاده از کدهای سیار در برنامه‌های ایمیل آگاه باشید. بسیاری از برنامه‌های ایمیل از همان کد به‌عنوان مرورگرهای وب برای نمایش HTML استفاده می‌کنند. بنابراین، شکافهای امنیتی که بر جاوا، جاوا اسکریپت و اکتیو ایکس اثرگذارند، اغلب علاوه بر صفحات وب در ایمیلها هم قابل اجرا هستند.

### اسکریپت‌های Cross-Site

یک برنامه نویس وب با افکار بدخواهانه ممکن است اسکریپتی به آنچه که به یک وب سایت فرستاده می‌شود، مانند یک URL، یک عنصر در شکلی خاص، یا درخواست از یک پایگاه داده، بچسباند. بعداً، وقتی وب سایت به در خواست پاسخ می‌دهد، اسکریپت زیان رسان به مرورگر منتقل می‌شود.

می‌توان مرورگر وبت را توسط روشهای زیر در اختیار اسکریپتهای زیان رسان قرار داد:

1. تعقیب لینک‌ها در صفحات وب، ایمیل‌ها یا پیام‌های گروه‌های خبری بدون دانستن به آنچه لینک داده شده است.
2. استفاده از فرم‌های محاوره‌ای روی یک سایت غیرقابل اطمینان
3. دیدن گروه‌های بحث آنلاین، مجمع‌ها یا دیگر صفحاتی که بصورت پویا تولید می‌شوند در جایی که کاربران می‌توانند متنهای شامل تگ‌های HTML ارسال کنند.

### ایمیل‌های جعلی

این حالت زمانی اتفاق می افتد که یک ایمیل به‌ظاهر متعلق به منبعی هست درحالیکه در حقیقت از منبعی دیگر ارسال شده است. اغلب برای گول زدن کاربر بمنظور این که اطلاعات حساس (مانند کلمات عبور) را افشاء کند بکار می‌رود.

1. ایمیل جعل شده می‌تواند گستره‌ای از شوخی‌های بی ضرر تا اقدامات مربوط به مهندسی اجتماعی داشته باشد. مثال‌هایی از مورد دوم اینها هستند:
2. ایمیل ادعا می‌کند که از مدیر یک سیستم است و از کاربران تقاضای تغییر کلمات عبورشان را به یک رشته مشخص دارد و آن‌ها را در صورت عدم تابعیت به تعلیق اکانتهایشان تهدید می‌کند.
3. ایمیل ادعا می‌کند از یک شخص با اختیارات لازم است و از کاربران تقاضا می‌کند که یک کپی از فایل کلمات عبور یا سایر اطلاعات حساس را برایش ارسال کنند.

وقتی سرویس دهندگان گه گاهی تقاضا می‌کنند که کلمه عبور را تغییر دهید، معمولاً مشخص نمی‌کنند که به چه کلمه‌ای تغییر کند. همچنین، بیشتر سرویس دهندگان قانونی از شما هرگز تقاضای ارسال کلمات عبور را از طریق ایمیل نمی‌کنند.

 ویروس‌ها و سایر کدهای آسیب رسان اغلب به‌عنوان پیوست ایمیلها گسترش می‌یابند. قبل از بازکردن هر پیوستی، از شناخته شده بودن منبع آن اطمینان حاصل کنید. اینکه ایمیل از آدرسی باشد که شما می‌شناسید، کافی نیست. ویروس ملیسا دقیقاً به این علت گسترش یافت که آدرس فرستنده آن آشنا بود. همچنین، کدهای آسیب رسان ممکن است در برنامه‌های سرگرم کننده یا فریبنده گسترش پیدا کنند.

هرگز برنامه‌ای را اجرا نکنید، مگر اینکه توسط شخص یا شرکتی نوشته شده باشد که به آن اعتماد دارید. بعلاوه، برنامه‌هایی را که از منابع ناشناخته دریافت می‌کنید، صرفاً بخاطر اینکه سرگرم کننده هستند، برای دوستان یا همکاران خود ارسال نکنید.

### پسوندهای مخفی فایل

سیستم عاملهای ویندوز انتخابی را در اختیار شما قرار می‌دهند که پسوند فایلهایی که نوع آن‌ها شناخته شده است را پنهان می‌کند. این انتخاب بصورت پیش فرض فعال است، اما ممکن است یک کاربر این قابلیت را بمنظور به نمایش درآمدن پسوند تمام فایلها توسط ویندوزغیرفعال کند. ویروس‌های داخل ایمیل از پنهان ماندن پسوند فایلهای شناخته شده بهره برداری می‌کنند. اولین حمله عمده که از این قابلیت بهره گرفت کرم VBS/LoveLetter بود.

فایل‌های پیوسته به ایمیلها که توسط این ویروسها فرستاده می‌شوند، ممکن است بی ضرر بنظر برسند، فایل‌های متنی (.txt)، فایل‌های تصویری (.mpg) یا (.avi) یا دیگر انواع فایل در حالیکه در حقیقت این فایل یک اسکریپت یا فایل اجرایی آسیب رسان است برای مثال.vbs یا.exe  برنامه‌های چت اینترنتی، مانند برنامه‌های پیام رسانی سریع و شبکه‌های IRC، مکانیسمی را فراهم می‌کنند تا اطلاعات بصورت دوطرفه بین کامپیوترهای متصل به اینترنت منتقل شود. برنامه‌های چت برای گروههایی از افراد، امکان مکالمه، تبادل URL و در بسیاری موارد انتقال انواع فایلها را فراهم می‌کنند.

چون بسیاری از برنامه‌های چت اجازه تبادل کدهای قابل اجرا را می‌دهند، خطراتی مشابه برنامه‌های انتقال ایمیل را ایجاد می‌کنند. مانند برنامه‌های ایمیل، باید دقت کافی برای محدودکردن توانایی برنامه‌های چت برای اجرای فایلهای دانلود شده، بکار گرفته شود. مثل همیشه، باید مواظب تبادل فایل با طرفهای ناشناس باشید.

### شنود بسته‌های اطلاعات

یک برنامه شنود بسته‌های اطلاعاتی، برنامه‌ای است که دیتا را از اطلاعاتی که در حال انتقال در روی شبکه هستند، در اختیار می‌گیرد. این دیتا ممکن است شامل نام کاربران، کلمات عبور و هر اطلاعات اختصاصی دیگری باشد که روی شبکه و بدون اینکه رمز شده باشند، حرکت می‌کنند. با شاید صدها یا هزاران کلمات عبور گرفته شده توسط این برنامه، مزاحمین می‌توانند حملات گسترده‌ای را روی سیستمها پیاده کنند. نصب چنین برنامه‌ای لزوماً به سطح دسترسی مدیر احتیاج ندارد.

نسبت به کاربران DSL و خطوط تلفن سنتی، کاربران مودمهای کابلی در معرض خطر بیشتری برای شنود قرار دارند، زیرا که تمام کاربران مودمهای کابلی همسایه بخشی از یک LAN هستند. یک برنامه شنود نصب‌شده روی کامپیوتر هر کاربر مودم کابلی ممکن است بتواند دیتا ارسال شده توسط هر مودم کابلی دیگر را در همان همسایگی دریافت کند.

تهدیدهای جدیدی که هویت و اطلاعات کاربر را هدف قرار داده‌اند،رویکردهای جدید امنیتی را طلب می‌کند.

امروزه، حملات فیشینگ ساده‌تر و کم خطرتر از تهدیدهای آنلاینی که در حال تجربه شدن هستند، به نظر می‌رسند. حملات فیشینگ به آسانی شناخته می‌شوند و می‌توان به سرعت آن‌ها را از کار انداخت. جرائم سازمان یافته از این حد گذشته و پیچیدگی آن‌ها به طرز چشم گیری افزایش یافته است. امروزه، کاربران با اشکال موذیانه‌تری از حمله مواجه می‌شوند و کشف و مقابله علیه آن‌ها بسیار مشکل‌تر است.

### حملات pharming

گونه‌ای جدید از حمله این گونه جدید حمله به‌عنوان pharming شناخته می‌شود. Pharming بجای اینکه کاربر را گول بزند تا به یک ایمیل تقلبی پاسخ دهد تا او را به یک وب سایت جعلی هدایت کند، برای فریب دادن کاربر برای تسلیم هویت و اطلاعات حساسش، از روش‌های زیرکانه‌تری استفاده می‌کند. این حملات از اسب‌های تروآ (تروجان) برای نصب برنامه‌های کلیدخوان و برنامه‌های هدایت کننده استفاده می‌کنند تا به یک نفوذگر اجازه دهند کلمات عبور و شماره کارت‌های اعتباری را بدست آورد، بدون اینکه کاربر مجبور به انجام کاری غیرعادی باشد.

در اینجا دو مثال از نحوه این حمله آورده شده است

1-   کاربر یک ایمیل ظاهراً صحیح را باز می‌کند که او را تشویق می‌کند تا فایل الحاقی به ایمیل را باز کند. این فایل الحاقی بصورت مخفیانه یک کلیدخوان (برنامه‌ای است که کلیدهایی را که توسط کاربر زده می‌شود، ثبت می‌کند) نصب می‌کند. هنگامی که کاربر به بانک آنلاین خود سر می زند، کلیدخوان این را تشخیص می‌دهد و ورودی‌های صفحه کلید کاربر را هنگامی که وی اسم و کلمه عبور را تایپ می‌کند، ثبت می‌کند. سپس این اطلاعات برای نفوذگر ارسال می‌شود تا برای دسترسی به حساب کاربر استفاده شود.

2-    یک کاربر ممکن است با دانلود کردن یک فایل یا مشاهده یک وب سایت که حاوی اکتیو ایکس control است، سهواً یک هدایت کننده[[18]](#footnote-18) را روی سیستم خود نصب کند. این کار باعث می‌شود که فایل‌های موجود در سیستم دچار تغییراتی شود و هنگامی که کاربر به بانک آنلاین خود سر می زند، به وب سایت نفوذگر هدایت شود. این عمل می‌تواند با مسموم کردن سرور DNS انجام گیرد که برای آدرس بانک آنلاین کاربر، IP وب سایت نفوذگر را می‌فرستد. حملات پیچیده‌تر می‌توانند ارتباط را با بانک کاربر برقرار کنند و هنگامی که پروسه در حال انجام است، ترافیک عبوری بین کاربر و بانک (شامل کلمات عبور و اطلاعات شخصی) را مشاهده کنند. در اصل نفوذگر خود را بین کاربران و بانک قرار می‌دهد.

ازنظر تاریخی، رویکرد امنیتی که برای این نوع از حملات بکار گرفته شده است، مشابه مفهوم گارد مرزی[[19]](#footnote-19) بوده است. ورود موارد زیان رسان را به کامپیوتر متوقف کنید و جلوی کاربر را از رفتن به مکان‌های بد بگیرید. ابزارهایی مانند آنتی ویروس، ضدجاسوس، فایروال‌ها و تشخیص دهندگان نفوذ، همگی چنین رویکردی دارند. به هرحال، همچنانکه حملات به رشد خود ادامه می‌دهند و پیچیده‌تر می‌شوند، نمی‌توان از احتمال نصب شدن موفقیت آمیز یک کلیدخوان یا هدایت کننده علیرغم این گاردهای مرزی، غافل ماند.

برای سروکار داشتن با این احتمال، رویکرد متفاوت دیگری مورد نیاز است. علاوه بر ابزارهایی که ذکر آن‌ها رفت، نیاز است که هویت و اطلاعات کاربران توسط محافظ شخصی[[20]](#footnote-20) مراقبت شود. یعنی، نیاز است که هویت و اطلاعات شخص بدون در نظر گرفتن نوع حمله و جایی که اطلاعات کاربر به آنجا می‌رود، همواره امن باقی بماند. این نوع امنیت قابلیت‌های محافظ شخصی را برای هویت کاربر ایجاد می‌کند و اهمیتی ندارد که اطلاعات کاربر به کجا فرستاده می‌شود و کلیدخوان نصب‌شده است و یا اینکه نفوذگر می‌تواند ترافیک اینترنت را نظارت کند.

دو قابلیت امنیتی وجود دارد که می‌تواند توانایی این محافظ شخصی را پیاده کند.

اولی تصدیق هویت قوی[[21]](#footnote-21) است. امروزه، کاربران عموماً برای محافظت از هویتشان به یک کلمه عبور اطمینان می‌کنند، اما احتمال زیادی وجود دارد که کلمه عبور توسط کسی که نظاره گر ورود است، دزدیده شود. داشتن یک عامل اضافی برای تصدیق هویت، یعنی چیزی که کاربر باید بصورت فیزیکی داشته باشد علاوه بر آنچه که می‌داند، می‌تواند یک هویت آنلاین را در برابر حمله محافظت کند. این کار قابل مقایسه با چگونگی تأیید هویت کاربران در ماشین‌های خودپرداز بانک است. کاربران هم کارت بانکی دارند و هم رمز را می‌دانند. با تصدیق هویت قوی، اگر کلیدخوان هم نصب‌شده باشد، می‌تواند تنها کلمه عبور را بگیرد و نه عامل فیزیکی استفاده شده در پروسه تصدیق هویت را. کلمه عبور به تنهایی و بدون فاکتور فیزیکی نمی‌تواند توسط نفوذگر برای دسترسی به حساب کاربر مورد استفاده قرار گیرد.

توانایی مهم دوم رمزنگاری مداوم است. امروزه، SSL[[22]](#footnote-22) از اطلاعات ارسال شده توسط کاربران بگونه ای محافظت می‌کند که انگار تنها به سرور هدف ارسال می‌شوند. برای مثال، اگر یک کاربر کلمه عبور خود را وارد کند، به راحتی تا زمان رسیدن به و ب سرور در طرف دیگر، قابل مشاهده است. در مورد یک حمله هدایت کننده، ارتباط امن در سایت نفوذگر پایان می‌پذیرد و قبل از اینکه به سازمان آنلاین قانونی ارسال شود، دیتای کاربر در معرض افشاء قرار می‌گیرد. رمزنگاری مستمر می‌تواند از دیتا، بدون در نظر گرفتن امنیت ارتباط، محافظت کند. ورودی‌های کاربر قبل از ترک کامپیوتر کاربر رمز می‌شوند و می‌توانند تنها توسط سازمان قانونی که به سرورهای طرف دیگر دسترسی دارد، رمزگشایی شوند. حتی اگر دیتا به این سرور نرسد، رمزشده باقی خواهد ماند و برای یک نفوذگر قابل استفاده نیست.

این دو قابلیت به همراه هم، می‌توانند نقش محافظ شخصی را برای محافظت از هویت و اطلاعات کاربر در دنیای خصمانه اینترنت ایفاء کنند.

### بررسی دنیای واقعی

چند انتخاب وجود دارند که می‌توانند امنیت محافظ شخصی را فراهم کنند اما باید با استفاده از نیازهای دنیای واقعی اینترنت ارزیابی شوند. چنانچه کاربر با یک فنّاوری احساس راحتی نکند، آن را نخواهد پذیرفت. اگر فنّاوری خیلی گران باشد، نه برای کاربر انتهایی قابل تهیه خواهد بود و نه برای سازمان مربوطه.

چندین عامل وجود دارد که باید به هنگام تشویق کاربران به پذیرش فنّاوری مورد نظر مورد توجه قرار گیرند:

1- نرم‌افزار کلاینت ـ هر نیازی به دانلود و نصب نرم‌افزار به عنوان یک مانع است...

2- واسط نرم‌افزار ـ خطرات و پیچیدگی که کاربر برای پیاده سازی تجربه می‌کند...

3- راحتی استفاده ـ مخصوصاً برای تصدیق هویت دو عامله!، راحتی استفاده شامل قابلیت حمل، دوام است. سهولت کار با واسط کاربر نیز مورد توجه جدی است.

مشخصاً زمانی که از این نوع فناوری با مقیاس بالا بکارگرفته شود، هزینه این رویکرد می‌تواند در امکانپذیری آن مؤثر باشد. اگر هزینه کل سیستم خیلی بالا باشد، سازمان‌ها برای برقراری این امنیت اضافی برای یک مورد تجاری مورد قبول، نیاز به مطالبات مالی از کاربران دارند. در این موارد کاربران به راحتی راضی به پرداخت‌های اضافی برای برقراری این امنیت بیشتر نمی‌شوند.

به این منظور تکنولوژی‌های محافظ شخصی باید سطح بالایی از امنیت را در حالی که هزینه کمی در بردارند و برای استفاده آسان هستند، فراهم کنند.

### دیوار آتش

دیوار آتش در فرهنگ کامپیوتر یعنی محافظت از شبکه‌های داخلی در مقابل شبکه‌های خطاکار. معمولاً یک شبکه کامپیوتری با تمام دسترسی‌ها در طرف و در طرف دیگر شبکه تولیدات شرکت را دارید که باید در مقابل رفتارهای مخرب محافظت شود. اعتبار کمپانیها در اینترنت به تبلیغات تولیداتشان هست. اینترنت به‌صورت شگفت انگیزی در حال رشد است.

مانند یک فروشگاه بسیار بزرگ بیشتر مردم به طرف اینترنت می‌آیند وهمانطوریکه در یک فروشگاه باید محصولات سالم باشند و بعد از فروش گارانتی بشوند اطلاعات و داده و انتقالات آن‌ها نیز باید به‌صورت امن و گارانتی شده باشد.

حال باید مکانیزمهایی برای حفاظت از شبکه داخلی یا اینترنت شرکت در مقابل دسترسی‌های غیر مجاز ارائه دهیم

## **منظور از دیوار آتش چیست؟**

دیوار آتش‌های مختلفی با ساختارهای مختلف وجود دارد ولی عقیده اصلی که پشت آن‌ها خوابیده یکسان است. به شبکه‌ای نیاز هست که به کاربران اجازه دسترسی به شبکه‌های عمومی مانند اینترنت را بدهد و برعکس.

مشکل زمانی پیش می‌آید که کمپانی بدون در نظر گرفتن معیارهای امنیت بخواهد به اینترنت وصل شود و شما در معرض دسترسی از طرف سرورهای دیگر در اینترنت هست. نه تنها شبکه داخلی کمپانی در مقابل دسترسی‌های غیر مجاز آسیب پذیر است بلکه تمام سرورهای موجود در شبکه کمپانی در معرض خطر هستند. بنابراین به فکر محافظت از شبکه می افتید و اینجاست که نیاز به یک دیوار آتش احساس می‌شود. به هر حال قبل از فکر کردن درباره دیوار آتش باید سرویسها واطلاعاتی که می‌خواهید روی اینترنت در دسترس عموم قرار دهید مشخص کنید.

می‌توان مجوزهای دسترسی, انتقال فایل و اجرای راه دور و همچنین منع مجوزهای ورود دوباره، Telnet، Ftp، SMTP و دیگر سرویس‌ها. اگر از این سرویسها استفاده کنید نیاز به دیوار آتش دارید به هر حال دیوار آتش چیست؟ اساساً یک فایروال جداکننده شبکه‌های امن از ناامن در اینترنت است. دیوار آتش تمام اتصالاتی که از اینترنت به شبکه‌های محافظت وارد می‌شوند را فیلتر می‌کند.

قبل از تعریف اینکه چه نوع از دیوار آتش‌ها بهترین مجموعه برای نیازها است, باید توپولوژی شبکه را برای تعیین اجزای آن مانند هاب[[23]](#footnote-23)، سویچ[[24]](#footnote-24)، مسیریابها[[25]](#footnote-25) و کابل کشی آنالیز کرد تا بهترین دیوار آتش که مخصوص این توپولوژی باشد انتخاب شود. برای ایجاد امنیت در شبکه نیاز به بررسی شبکه داخلی از لحاظ مدل لایه بندی ISO آن هست بطوریکه تکرار کننده ها[[26]](#footnote-26) و هاب ها در لایه اول، سویچ ها و پلها[[27]](#footnote-27) در لایه دوم و مسیر یاب ها در لایه سوم، یک دیوار آتش در تمام لایه‌های شبکه می‌تواند عمل کند (از جمله در هر هفت لایه) لایه‌ها مسئول پاسخگویی به کنترل و ایجاد نشستها و بکارگیری آن‌ها می‌باشند. بنابراین با یک دیوار آتش می‌توان جریان اطلاعات را در طول ایجاد کنترل کرد. دیوار آتش‌ها امکان مدیریت دروازه‌های ورود به وب را می‌دهد و امکان تمرکز روی پروژه اصلی را می‌دهد.

### هدف از یک دیوار آتش

دیوار آتش‌ها به تنهایی نمی‌توانند امنیت شبکه را برقرار کنند آن‌ها فقط یک قسمت از سایت شمارا امن می‌کنند و به‌منظور امنیت شبکه باید محدوده‌ای از شبکه را مشخص کنید و نیاز به این دارید که چیزهایی در شبکه که باید محدود شوند را تعیین کنید ویک سیاست امن را گسترش دهید و مکانیسمهایی برای اعمال سیاستهای مورد نظر روی شبکه را ایجاد کنید البته مکانیسمهایی پشت دیوار آتش‌ها هستند که می‌توانید به‌صورت عجیبی سطح امنیت را بالا ببرید. این مکانیسمها بعد از اعمال سیاست امنیت مشخص می‌شوند و نه قبل از آن، برای ایجاد یک مکانیسم امن برای محافظت از وبسایت شما باید یک دیوارآتش برای نیازهای خود مشخص کنید وآن را پیاده سازی کنید.

ایجاد امنیت از سازمانی به سازمان دیگر متفاوت است البته این بستگی به چیزی که آن‌ها مخواهند توسعه دهند دارد. شما دقیقاً به بستر اجرایی مورد نظر خود دقت کنید همانطور که اجرای پروژه را مشخص می‌کنیم باید سطوح امنیت را نیز مشخص کنیم تا بتوانیم آن را پیاده سازی کنیم. این یک روش برای موفقیت در پیاده سازی مکانیسمهای امنیت است. دیوار آتش ها علاوه براین که امنیت واقعی را برقرار می‌کنند یک نقش اساسی در مدیریت امنیت را پوشش می‌دهند دیوارآتش ها امنیت در شبکه را برقرار می‌کنند و ریسک سرورهای روی شبکه را با فیلتر کردن کاهش می‌دهند به عنوان مثال: شبکه دارای ریسک کمتری هست به علت اینکه پروتکلهای مشخص شده روی دیوارآتش می‌توانند روی شبکه اعمال وظیفه کنند.

مشکل دیوارآتش ها محدودیت آن‌ها در دسترسی به و از اینترنت است و شما مجبور می‌شوید که از سرور پروکسی[[28]](#footnote-28) استفاده کنید.

### دیوار آتش ارائه کنترل دسترسی

سرورها می‌توانند از بیرون قابل دسترس باشند مثلاً کسی ویروسی را با ایمیل می‌فرستند و بعد از اجرا, فایروال را از کار می‌اندازد. بنابراین تا جایی که امکان دارد از دسترسی مستقیم به سرورها جلوگیری کرد.

می‌توانیم به جای محدود کردن سرور، یک سرور را با تمام دسترسیهای ممکن به اینترنت وصل کرد و سرور دیگر را پشت دیوار آتش به عنوان پشتیبان از سرور قبلی داشت. با هک شدن یا خرابی سرور اولی می‌توان آن را بازیابی کرد. روش‌های دیگر برای اعمال امنیت روی شبکه ممکن است موجب تغییراتی روی هر سرور شبکه شود، ممکن است تکنیکهای بهتری نسبت به دیوار آتش‌ها باشد ولی دیوار آتش‌ها برای پیاده سازی بسیار آسان هستند برای اینکه دیوار آتش‌ها فقط یک نرم‌افزار مخصوص هستند.

یکی از مزایای دیوار آتش‌ها استفاده آن‌ها برای اینکه بتوان با ضبط کردن دسترسی به سایت آمار دسترسی‌های به سایت را مشخص کرد.

### مزایا و معایب دیوار آتش

دیوار آتش‌ها دارای مزایای بسیاری می‌باشند با این وجود دارای معایب نیز هستند. بعضی از دیوار آتش در مقابل محدود کردن کاربران و درهای پشتی[[29]](#footnote-29) که محل حمله هکرهاست که امنیت ندارند.

دسترسی‌های دیوار آتش برای ایجاد امنیت بعضی از سرویسها مانند Telnet، Ftp و Xwindow را از کار می‌اندازند و این تنها محدود به فایروال‌ها نمی‌شود. بلکه در سطح سایت نیز می‌شود این کار را انجام داد.

### چالش‌های درپشتی: تهدید مودم

تا حالا مشخص شد که امنیت درهای پشتی کمپانی به وسیله دیوار آتش تأمین نمی‌شود بنابراین اگر شما هیچ محدودیتی در دسترسی به مودم نداشته باشد این در بازی برای هکرها است.

SLIP, PPP از راههای ورودی می‌باشند و سئوال پیش می‌آید که اگر این سرویسها وجود داشته باشند چرا از دیوار آتش استفاده می‌شود.

# فصل دوم

**به کارگیری اصول امنیت**

## **مقدمه**

امنیت در دنیای مجازی اینترنت پیچیده‌تر از دنیای واقعی است که در آن زندگی می‌کنید شعارها، و کلاهبرداریهای تجاری معمّا را پیچیده‌تر می‌کند اما به عقیده متخصصّان دنیای اینترنت روز به روز خطرناک‌تر می‌شود چگونه این اتفاق می افتد؟ چگونه راه حل‌های همه سویه نتوانسته مشکلات ابتدای را حل نماید جواب ساده نیست؟ چرا که مشکلات بسیار پیچیده است ایجاد و نگهداری امنیت مشکل هست امنیت پیچیده است، مشکل این است که دنیای ارتباط مستقیم حول یک سیستم از پروتکل‌ها و قواعد نیا نهاده شده است اما متأسفانه این قواعد کامل و دائم پیروی نمی‌شوند، ترکیب دستگاه‌های کامپیوتری امروزی و نرم‌افزارها غالباً برنامه‌هایی را ایجاد می‌کند که به واسطه خط مشی‌های عملی اینترنت به‌صورت پیش بینی نشده‌ای عمل می‌کند. لذا یک پتانسیل زیاد برای شلوغ کاری حجیم نیاز هست هم چنین بدست آوردن و نگهداری سطح مناسبی از امنیت نیازمند منابع هست و افرادی با مهارتهای فنی و تجاری متعادل نیاز هست زمان، انرژی، پول نیاز دارد امنیت ارزان نیست مفهوم امنیت می‌تواند به عنوان یک هدف تغییر پذیر دائمی به نظر برسد که این تهدیدات را در برگرفته و مشابه یک فرایند زندگی با تغییرات وفق داده می‌شود، در دنیای تجارت الکترونیکی افرادی که از حفاظت‌های امنیت سود می‌برند. بیشتر کسانی هستند که فراپند را به همراه امنیت در ذهنشان شروع کرده‌اند، چگونه امنیت را باید در کانون شروع قرار داد چه نقش‌هایی بایستی بازی کرد و چگونه آن را به دست آورد و بودجه پروژه را تعیین کرد از آنجا که مسئولیت دفاع از یک سایت در حال ایجاد با یک سایت تجارت الکترونیکی را داریم نقش‌هایی را که بایستی بازی کرد و فرآیندی که وضعیت سایت را بهبود بخشد کاوش خواهد شد.

## **امنیت به عنوان یک زیربنا**

راحت‌ترین موفق‌ترین و بهترین راه برای ایجاد امنیت یا یک محیط امن، شروع امنیت در ذهن هست این بدان معنی است که اعمال اصول ایمنی سازی به عنوان یک زیر بنا در سرتاسر پروژه در نظر گرفته شود اصول اولیه امنیت عبارتند از صحت و قابلیت دسترسی، جهت موفقیت پروژه باید این اصول در تمام مراحل بکار گرفته شود.

## **امنیت فراتر از یک کلمه رمز**

باید امنیت در سازمان فراتر از یک کلمه رمز یا یک گروه امنیت باشد امنیت بایستی در فکر و ذهن تک تک افراد بوده و جلودار عملیات روزانه باشد در داخل شرکت اعضای گروه امنیت با گروههای دیگر به عنوان همکار و مشاور کار می‌کنند آن‌ها باید قابل نزدیک شدن باقی بمانند و همانند پلیس شبکه به نظر نرسند، هنگامی که تمامی افراد متوجه عوامل اختلال در سایت و یا در معرض خطر قرار دادن مشتریان باشند امنیت به بهترین نحو کار خواهد کرد کلید رسیدن به این سطح از آگاهی، آموزش است.

آموزش ابزاری است که با بکارگیری آن می‌توان مهاجمینی را که به واسطه ارتباط نامناسب طراحی ضعیف فرایندها و خونسردی و بی مسئولیتی افراد قصد سوءاستفاده دارند را خلع سلاح کرد برخی هجوم‌ها که هکرها آن را مهندسی اجتماعی[[30]](#footnote-30) می‌نامند بهترین راه برای مقابله با این حملات آموزش کارکنان در مورد سیاست‌های مرتبط با امنیت و پوشیدگی مشتری هست هنگام اعمال نمودن تغییرات سیاست‌ها نیازمند تذکر دهنده تازه کننده‌ها و روز آوریهای متناوب هست جهت دست آوری و دست‌یابی به موفقیت و نگهداری درازمدت آن بایستی بالاترین سطح مدیریت و سیاست‌ها و اجزای آن را پشتیبانی کرد. چنانکه تیم امنیت مستلزم پشتیبانی مدیریت است هر فردی نیازمند این هست که احساس کند گروه امنیت قابل نزدیک شدن هست و هراسی از گزارش چیزهای مشکوک نداشته باشد کارمندان بایستی دقیقاً بدانند که یا چه کسی باید تماس داشته و زمانی که مشغول صمیمت با گروه امنیت هستند به جای سوء ظن یا احترام رفتار شود.

همه چیز یا خطر شروع می‌شود: نقطه شروع با خطرات زمانی است که می‌خواهید محیط خود را آزمایش کنید یا خطرات را هنگام بررسی سایت خود لمس نمایید مخاطرات بایستی امتحان شده و جهت از بین بردن آن‌ها سایت خود را اشکال زدایی و یا بازبینی نمایید. پیچیدگی و اندازه سایت شما ممکن است تعداد کم و یا بی شماری از آسیب‌پذیری‌ها را بیابید جهت مشاهده آسیب پذیرهای شناخته شده سایت www.evemitro.org مراجعه شود هر کدام از آسیب پذیرها ممکن است در معنی یا مفهوم فرق داشته باشد ابزاری که جهت بررسی و شرح مخاطرات مرتبط با هر آسیب پذیری به کار می‌رود به یاد داشته باشید که در برخی حالات آسیب پذیرهای سطح پایین و متوسط می‌تواند برای ایجاد یک مشکل بزرگ و عمده برای سایت شما بکار رود و می‌تواند حتی عدم پذیرش سرویس DOS را ایجاد کند.

## **اول خطرات سطح بالا و مهم‌تر را برطرف شود**

هنگامی که یک گزارشی از آسیب پذیرهای خود تهیه نمودید و ضربات یافت شده در محیط خود را امتحان نمودید برحسب خطرها عملیات لازم جهت اشکال زدایی آن‌ها به کار برید سطح خبر برای هر آسیب پذیری بسیار ساده است مخاطرات را با سرمایه‌های حقیقی مرتبط سازید یا وقت گذاری برای تعیین سرمایه‌ها و ارزشهای شرکت ارزیابی و سنجش خطر ساده‌تر می‌شود راجع به شرکت و تجارتی که می‌خواهد انجام گیرد با صرف وقت باید خوب فکر کرد هر خطری که سعی در اختلال یا به خطر انداختن این ارزشها را داشته باشد بالاترین رتبه خطر را خواهد داشت مواردی روی یک ارزش تأثیر می‌گذارد در سطح متوسط باید در نظر گرفت و کمترین سطح خطر را آنهایی دارد که ضربه کمتری به ارزشها وارد می‌سازد، ابتدا آسیب پذیر هایی را که دارای بالاترین سطح هست باید رفع نمود هنگامی که کارمندان شرکت مشغول به تکمیل ملحقات و یا اصلاحات می‌باشند غالباً یک ایده خوب برای فرد نشاندن خطرها از طریق راههای دیگری نظیر مسدود نمودن درگاههای خاص روی دیوار آتش و یا مسیر یابها هست به‌طور کلی باید مطمئن شد که تک تک فرایندها و برنامه‌های کاربردی که روی دستگاه‌های شما مشغول اجرا هستند دارای آخرین و جدیدترین نسخ و ملحقات باشد باید به سرویس‌های عمومی نظیر POP, FTP, SNMP, SMTP, HTTP IMAP و برنامه‌های مرتبط با امنیت نظیر دیوار آتش‌ها یا برنامه‌های تشخیص غیر مجاز IDS توجه خاص داشته شود با شروع اصلاح، از خطرات بزرگتر به سایت کمک کرده‌اید تا سیستم‌ها و اطلاعات حیاتی خود را محافظت نمایند چنانچه اگر سیستم اخطار، یک آسیب پذیری عمده، روی سیستمی را گزارش دهد که مأموریت اساسی ندارد و اطلاعات مهمی را به کار نمی‌برد و یا به قدر کافی توسط دیوار آتش محافظت شده است به همین دلیل اطلاعات دریافتی از ابزارهای اخطار دهنده می‌بایست درست سنجیده شود پس از این که کار را تفکیک و اولویت بندی نمودید فرایند اعمال اشکال زدایی و باز بینی‌ها به محیط را شروع کنید و آن‌ها را به کار گیرید سپس با استفاده از فهرست افدام به انجام تغییرات روی دستگاه‌های گوناگون انجام دهید وقتی کار تمام شد این فرایند دوباره تکرار شود تا مطمئن شوید که این تغییرات موارد جدیدی بوجود نیاورده است.

## **امنیت به عنوان یک محدودیت**

بزرگ‌ترین دغدغه‌ای که تیم‌های امنیت با آن روبرو هستند این است که یا چه دیدی به آن‌ها نگاه می‌شود در خیلی از سازمانها سابقه تیم امنیت یا نقش‌های نگهبانان امنیت فیزپکی در هم پیچیده شده است. بسیاری از تیم‌های امنیت توسط هم قطران خود به عنوان پلیسان شبکه یا نگهبانان کامپیوتر نظاره می‌شوند. نقش اعضای تیم امنیت اغلب کار یا تیم منابع انسانی هست یک مشکل ایجاد می‌شود این علل باعث خرابی فرایند امنیت می‌شود یا دور کردن کارمندان دیگر، تیم امنیت به سختی می‌تواند وظایفش را انجام دهد. با اعضای تیم کمتر و کمتر همکاری می‌شود و نخواهند توانست با گروههای دیگر ارتباط مناسبی برقرار سازند.

دلیل آنست که تصاویر اشتباهی است که به کارمندان دیگر نشان داده شده است تصویر این است که امنیت یک محدودیت است اغلب پس از بکارگیری کنترل‌ها با نرم‌افزار مونیتور پنگ برای مدیریت بهتر است استفاده از منابع شبکه یا کارایی در ساعات کاری در صورتی که تکنولوژی‌ها هیچ گناهی ندارند اغلب آن‌ها به‌عنوان روش «برادر بزرگ» می‌شناسند در این صورت از خطرات بازی نقش «پلیس شبکه» مصون خواهید بود اگر کاربرد دچار اشتباه شده و در دام یک تهاجم مفهومی بیفتد و کلمه عبورش را به دیگران بدهد، او را خواسته و از او توضیح بخواهد، نه اینکه او را تنبیه و کیفر بدهد.

## **تهاجم DDOS چیست؟**

برای درک یک حمله DDOS و پیامدهای آن ابتدا نیاز داریم تا اصول حملات DDOS را بشناسیم شناخت DDOS به سمت DDOS و پی بردن به تفاوت این دو بسیار مهم است باعث شگفتی نیست که یک تهاجم DDOS برای تضمین این که یک سرویس که معمولاً زیربنای محاسباتی دارد تأثیر منفی داشته باشد با دقت هدف گیری نموده این نوع از تهاجم باعث توقف سیستم مقصد نمی‌شود معمولاً یک حمله موفق DDOS کیفیت ارائه سرویس را طوری تنزّل می‌دهد که همیشه در دسترس نباشد موضوع اصلی این است که هدف یک حمله DDOS یک هک سرور است البته در همه موارد این طور نیست هدف اصلی یک هجوم DDOS تنزل سرویس است خواه این سرویس توسط یک سرور میزبانی شده باشد یا توسط کل ساختار شبکه!

تعریف یک هکر و فعالیت‌های آن در طی بیست سال گذشته دست خوش تغییرات بسیاری شده عموماً یک هکر مترادف یا اشخاصی است که عطش و اشتیاق فراوانی برای داشتن و دانستن توانایی توسعه تک کدهای زیبا و صاف و ساده دارند آن‌ها برای توسعه ایده‌ها و فنونی که صنعت را شکل می‌دهد مفید هست معنی کلمه هکر می‌تواند گمراه کننده باشد شاید پنداشته شود که هکر شخصی است که عهده دار فعالیت‌های روی شبکه و سیستم‌ها بوده و به دنبال وارد نمودن ضرر و زیان به مالکین خود هست هکرها غالباً به 2 گروه تقسیم می‌شوند هکرهای کلاه مشکی و هکرهای کلاه سفید یک هکر کلاه سفید سعی در رخنه به دستگاه‌های کامپیوتری به‌منظور شرارت یا نفع شخصی ندارد از سوی دیگر کلاه مشکی یا نفوذی‌ها جنبه تاریک‌تری از هکر را نشان می‌دهد.

## **تهاجمات مصرف منبع**

منابع محاسباتی به خاطر طبیعتشان خیلی محدود هستند. هر چند ما آرزو داریم این طور نباشند مدیران شبکه گرداگرد جهان از این که زیرسازی شبکه آن‌ها فاقد پهنای باند شبکه، سیکل‌های CPU، ARM، و محل ذخیره سازی ثانویه است نالان هستند همیشه نبود این منابع باعث تنزل سرویسی که زیرساخت محاسباتی داشته و به ایستگاه‌های کاری ارائه می‌شود می‌گردد. این حقیقت که منابع محدود است یک نقصان است یکی از عادی‌ترین گونه‌های هجوم DDOS هدف‌گیری پهنای باند شبکه است خصوصاً ارتباطات اینترنت و دستگاههای پشتیبانی شده یک هدف آغازین برای این نوع تهاجم است به این علت که پهنای باند پدیداری آن‌ها روی سرتاسر اینترنت محدود شود تجارتهای کوچک در موقعیت مناسب برای تهاجمات مصرف پهنای باند قرار دارند و پهنای باند اضافی برای اینترنت در نظر می‌گیرند تا بتوانند بطور سریع به درخواست‌های مشتریانشان سرویس دهند در چنین حالیت یک تهاجم مصرف پهنای باند می‌تواند یک شرکت را به زانو درآورد.

تهاجمات مصرف منبع معمولاً خارج از شبکه محلی تولید می‌شود و این تهاجمات به شکل تعداد زیادی بسته‌های اطلاعاتی[[31]](#footnote-31) که به سمت هدف هدایت شده ظاهر می‌شود. این تکنیک معمولاً به نام سیل Floodins شناخته می‌شود یک شبکه هدف گیری شده وقتی می‌تواند سیل زده شود که یک مهاجم پهنای باند قابل دسترسی بیشتری داشته باشد این حالت برای سایت‌های تجارت الکترونیکی کمتر اتفاق می افتد چون در بیشتر حالات کانال وسیع‌تر و بزرگ‌تر از مهاجمانشان دارند از طرف دیگر دسترسی به پهنای باند ارتباط، خطوط پرسرعت اینترنت را به خانه‌های کاربران در اقصی نقاط جهان برده همانطور که کاربران خانگی (مودم‌های آنالوگ) خود را با (مودم کابلی) و خطوط DSL جای گزین می‌کنند احتمال وقوع این نوع تهاجم زیاد است. راه دیگر مصرف پهنای باند، استفاده از شبکه‌هایی که بطور صحیح و اصولی پیکربندی نشده در این حال ارسال ترافیک به سمت هدف امکان‌پذیر هست اگر شبکه‌های کافی در دام این نوع رفتار بیفتد شبکه مورد هدف به آسانی دچار سیل زدگی می‌شود این نوع تهاجمات تقویت Amplitication, Attecks نامیده می‌شود. رد سرویس Attacks DDOS دارای معنی وسیعی است لذا به سبب شرایط محیطی که ظهور آن را احاطه کرده است تهاجمات DDOS را از حد گذرانده یک مثال کلاسیک از این سناریو ویروس ملیسا Melissa است که یا چنان سرعتی تکثیر می‌شود که منابع شبکه را مصرف نموده است و نتیجه آن یک DOS است به‌طور خلاصه تعداد زیادی از حملات DOS در اینترنت است.

### کالبدشکافی یک تهاجم سیل SYN

یک تهاجم سیل SYN از طریق دست کاری در مکانیزم های شروع یک ارتباط TCP تأثیر خود را می‌گذارد جریانهای ارتباطی ایجاد شده توسط پروتکل TCP برخلاف UDP جهت داده شده توسط ارتباط Connection-Oriented هست این بدان معنی است که قبل از اینکه دو کامپیوتر مبدأ و مقصد بتوانند تبادل اطلاعات کنند می‌بایست یک نشست ایجاد شده باشد توسط روش three – way-hand shake که در آن هر مرحله فقط وقتی آغاز می‌شود که مرحله قبل کامل شده باشد نشست ایجاد می‌شود. مراحلی که در TCP یا استفاده از روش فوق بین دو ماشین (ایستگاه کاری و سرور) نشست ایجاد می‌کند عبارتند از یک SYN از ایستگاه کاری به سرور فرستاده می‌شود. یک بسته SYN از یک پورت ایستگاه کاری به یک پورت خاص ردی سرور که منتظر تماسهای ایستگاه کاری است ارسال می‌شود یک ISN نیز به همراه بسته فرستاده می‌شود TCP یک پروتکل قابل اعتماد است و نتیجتاً یک مکانیزم برای بازیابی ارسالات ناموفق و برای کمک به بازسازی بسته اطلاعات نیاز هست ISN کمک می‌کند که بسته‌ها با ترتیب درست دریافت شود یک SYN/ACK از سرور به ایستگاه کاری ارسال می‌شود.

سرور یا پس فرستادن ISN ایستگاه کاری به اضافه یک، به ایستگاه کاری پاسخ می‌دهد سیگنال ACK SYN (AcknowIedge) ایستگاه‌های کاری را تصدیق می‌نماید یک SYN مربوط به سرور به ایستگاه کاری نشان می‌دهد که سرور قادر است یک نشست با ایستگاه کاری ایجاد نماید SYN ارسالی از سرور به ایستگاه کاری دارای ISN خود سرور است که با ISN ایستگاه کاری متفاوت است.

یک ACK از ایستگاه کاری به سرور پس فرستاده می‌شود. ایستگاه کاری با یک ACK که شامل ISN سرور به اضافه یک هست به SYN/ACK می‌رود پاسخ می‌دهد حالا ایستگاه کاری و سرور یک ارتباط TCP برقرار می‌سازند. در طی برقراری عادی یک نشست TCP مراحله سه گانه انجام می‌شود یک حمله سیل SYN یا شروع ارتباط TCP و ارسال یک SYN به سرور مورد نظر بوجود می‌آید مهم‌ترین اختلاف بین این SYN و اصل آن که از طرف یک کاربرد مشروع ارسال می‌شود این است که آدرس مبدأ در این تهاجم حمل شده است به خاطر طبیعت IPV4 پس از آنکه یک بسته دستکاری و جعلی شده میزبان مبدأ را ترک و شروع به تعیین میسر کرد چک کردن آن بسیار مشکل است و لذا IPV6 تکنیک مطلوبی است که توسط هکرها به کار می‌رود.

### کالبد شکافی یک تهاجم DDOS

برخی نمونه‌های تهاجمات DDOS می‌تواند توسط چندین واسطه تقویت شود. اما قدم اول برای ایجاد یک هجوم DDOS از یک ماشین برداشته می‌شود حملات DDOS نوع خطرناکتر و پیشرفته DDOS است تهاجمات DDOS به‌صورت یک ردیفی مانند سیل SYN و دو ردیفی مانند اسمورف ظاهر می‌شود هم اکنون سبک شناسی های هزین هجوم شامل دنیای محاسبات چند ردیفی توزیع شده یکی از اختلافات مهم در سبک شناسی یک هجوم DDOS است که شامل دو فاز مجزا است فاز اول مایل به مخاطره انداختن کامیوترها در اینترنت پراکنده می‌شود.

فاز دوم میزبانان در معرض خطر، که آن‌ها را با نام زومبی ها[[32]](#footnote-32) می‌شناسیم از طریق واسطه‌هایی جهت یک هجوم تعلیم داده شد، صدها یا شاید هزاران (زومبی) توسط هکرهای پرتلاش به خدمت گرفته می‌شود سپس با استفاده از کنترل نرم‌افزار هر یک از این زومبی ها می‌تواند برای سوار کردن هجوم DDOS خود بر روی هدف به کار رود تأثیر جمعی یک حمله زومبی غوطه ور ساختن یک هدف با یک ترافیک بسیار شدید یا تهی کردن منابع نظیر صفحه‌های ارتباط هست. یک مدل چند ردیفی از تهاجمات DDOS و توانایی آن‌ها در جعل بسته‌های اطلاعاتی و رمزگذاری ارتباطات باعث می‌شود که متجاوز واقعی ردگیری نشود یک فرایند حقه بازه چه چیزی یک مهاجم را برای ویرانی شرکتها تحریک می‌کند؟

نظریات بسیاری از مردم راجع به انگیزه‌های حکم رانی تهاجمات DDOS و انجام هک پرسیده شده. روان شناسان اقتصاد دانان کوشش نمودند تا تئوریهای جامعی را ارائه دهند. حقیقت آن است که هر شخصی که در پشت یک هجوم قرار دارد دارای انگیزه‌های مخصوص به خود هستند. کوشش برای تقسیم اینترنت به طبقاتی که تعریف شد راهی برای مقابله با نیات بی نظمی و هرج و مرج در وب که دیگران را به مخاطره می‌اندازد هست باید دانست که از چیزهای خوب می‌توان در راه ناپسند استفاده کرد این حقیقت به تهاجمات رو به افزایش است انکارناپذیر است این تعداد در سال 2000 به تعداد هشدار دهنده 5823 افزایش یافت اگر کلمه hacking را در اینترنت جستجو کنید نزدیک به 620000 مورد را خواهید یافت در بسیاری از شرکتها اگر هجومی صورت گیرد هیچ کس بازخواست نمی‌شود. ]3[

### ابزارهای مهاجمین برای انجام خدمات DDOS

تعداد برنامه‌های DDOS که به‌طور رایگان قابل دریافت از اینترنت است رو به فزونی است چندین نسخه که عمومیت بیشتری دارد دست خوش تعمیرات است مشابه سیکل‌های توسعه برای نرم‌افزار تجاری، توسعه دهندگان ابزار DDOS دارای یک تکنیک توسعه یافته به نام مدل متن باز هستند که بسیاری از نرم‌افزارهای تجاری فاقد آن هستند.

ایده‌ای که مدل متن باز ارائه می‌دهد این است که کد استفاده شده برای نوشتن یک برنامه بطور رایگان برای تغییر و پخش مجدد قابل دسترسی هست استفاده از مدل متن باز برخی اشخاص مهم را به توسعه جدیدی از ابزار DDOS تشویق می‌کند همکاری هکرها در انواع زمینه‌ها کد برنامه را در جهات حیرت انگیزی توسعه می‌دهد رشد نرم‌افزار DDOS به جایی رسیده که تنها توسط استادان فن قابل استفاده است نرم‌افزارهای مختلف برای تجار عمده مهیا شده مشابه حملات فوریه دو هزار چندی که این ابزار در آن مشترک است، میزبانان باید به شکلی به مخاطره افتند، اشاره می‌کند که ایمن نمودن منابع شبکه مهم‌ترین کار است.

### روش‌های اساسی حفاظت

آگاهی از تهاجمات DDOS در سالهای اخیر رشد یافته تعداد میزبانان لازم برای انجام یک هجوم بزرگ DDOS می‌تواند قابل توجه باشد و خیلی از مهاجمان روال‌های خودکار را برای ردیابی میزبان‌هایی که به‌طور مناسب برای اجرای فرایند Daoemon پیکربندی شده است به کار می‌برند، پیمایش سایت‌ها می‌تواند زنگ خطری باشد برای مدیران هزینه بری DDOS معمولاً شامل فیلترسازی خروجی آدرس‌های جعلی و فیلترسازی ورودی بسته‌های انتشاری هست. فیلترهای خروجی شامل فیلتر کردن ترافیک خروجی است. در حالی که فیلترسازی ورودی وابسته به فیلتر نمودن ترافیک ورودی شبکه است.

تقریباً هر IDS نوین مکانیزم شخصی برخی گونه‌های DDOS را دارد مکانیزم های دیگر حفاظت، شامل به کارگیری دیوارهای آتش و پراکسی‌ها هست، دیوارهای آتش برای متوقف نمودن ابزار DDOS نظیر TFN2K زمان زیادی را صرف می‌کند چون این ابزار از طریق پورت‌های مشخصی هجوم نمی‌کنند یا ارتباط برقرار نمی‌سازند پیکربندی دیوارهای آتش می‌تواند یک کار پیچیده و بیهوده باشد بازرسی حالت دار[[33]](#footnote-33) ترافیک، توانایی دیوارهای آتش برای مدیریت ارتباط‌ها را بالا می‌برد و یا توانایی آشکارسازی یک فعالیت آزاردهنده که توسط مدیر تشخیص داده شده آهنگی دارد. راه‌هایی وجود دارد جهت کمینه کردن بهره برداری توسط DDOS روزآمد کردن نحوه امنیت! اجرای یک فرآیند که به واسطه آن آخرین الحاقات و پیکربندیها در مورد میزبان‌ها و دستگاههای شبکه اعمال شده به عنوان یک ساختار امنیت عمومی، و نه فقط برای DDOS متمم است، دستگاه‌های عامل برای چشم پوشی انتشارهای جهت داده شده، سیل متحد SYN قابل بازگشت، ایجاد کلمه‌های عبور توان مند و غیر فعال کردن تمامی سرویسهای غیر لازم پیکربندی شود، مهاجمین وقتی می‌توانند یک هجوم شبکه را ایجاد کنند که میزبانان یا شبکه‌ها به‌طور ضعیف ایمن شده باشند.

### تهیه شرح حال از خصوصیات و مشخصات ترافیک

سعی شود میزان سختی وقوع یک هجوم را بدون در نظر گرفته توزیع عادی ترافیک و مشخصات ترافیک ورودی و خروجی تعیین کنید اگر یک توقف از نوع خاصی از ترافیک ICMP ظاهر شد بدون داشتن یک شاخص برای مقایسه تغییر این اطلاعات می‌تواند سخت شود.

### تقسیم کردن شالوده NDS

مجزا نمودن شالوده‌های DNS داخلی و خارجی پا گذاشتن روی اساس شبکه را مشکل‌تر می‌کند این کار ازدیاد زومبی ها در سمت «پاک» دیوار آتش را مشکل‌تر می‌سازد.

### متعادل ساختن بار

ارائه کردن یک سایت بازگشت و خطاپذیر، تلورانس خطا کلیدی است برای موفقیت هر سایت تجارت الکترونیکی یا استفاده از متعادل سازی یار، نه تنها دسترسی و سمت بهبودی می‌یابد بلکه باعث تحمل در برابر هجومهای DDOS می‌شود یک دگرگونی دقیق در این باره، استفاده از سرویس‌های میزبانی توزیع شده نظیر

هست گسترش سایت‌ها در عرض یک شبکه توزیع شده با استفاده از DNS و مکانیزم های دیگر، تحمل سایت‌ها در برابر هجوم‌های DDOS می‌بخشد.

### فیلتر سازی ورودی و خروجی

اطمینان از اینکه ترافیک‌های ورودی و خروجی شبکه کاملاً شناخته شده هست، احتمال اینکه یک سایت به عنوان قسمتی از شبکه زومبی‌ها استفاده شود و نیز شانس آنکه میزبانان به مخاطره بیفتد را کم می‌کند ISP شما به فیلتر سازی ورودی نیاز دارد که به شناسایی زومبی های شبکه کمک می‌کند.

## **محکم کردن پیکربندیهای دیوار آتش**

به‌طورفرض، تمامی سرورهایی که به اینترنت دسترسی دارند بایستی در DMZ ها قرار گیرند ایجاد کنترل شدید، تغییرات برای ویرایش‌های قاعده دار و اطمینان اینکه کمترین تعداد پورت‌ها و پروتکل‌ها از میان دیوار آتش اجازه عبور دارد امری است حیاتی و مهم، به عنوان مقال فیلترسازی خروجی پاسخ اکوهای CMP توسط دیوار آتش و هم چنین بسته‌های برچسب زمانی پاسخ برچسب زمانی درخواست اطلاعات پاسخ اطلاعات و زمان انقضاء را در نظر بگیرید معمولاً سایت‌ها می‌بایست با در دسترس قرار دادن پورت Tep شماره 80 شروع کنند و سپس توسعه و گسترش را ادامه دهند هر گونه توانایی دفاع، برای دیوار آتش محلی بافر کردن فرآیند ارتباط TCP یا آشکارسازی فعالیت آزار دهنده را فعال کنند. گزارش گیری و منحرف نمودن اطلاعات به سمت Sysloget را فعال سازید.

دستگاه‌های پیرامون خود را ایمن سازید و از نمود ترافیک بهره مند شوید برخی احتیاط‌ها در مورد کنترل دسترسی ترافیک خروجی و ورودی دستگاههای پیرامون لازم است، محدودیتی که پروتکل‌ها و پورت‌ها برای استفاده از این دستگاه‌ها دارد نیاز دارد که در آینده توسط پیکربندی دیوارهای آتش توسعه داده شود مکانیزم های حفاظتی را که برای دستگاه محلی هست نظیر lete limiting, TCP intercept for cisco routers را فعال سازید.

## **ایجاد یک IDS**

ایجاد یک IDS که به‌طور کامل طراحی شده باشد این قدرت را به مدیران می‌دهد که برخی مکالمات را آشکار سازند IDS می‌بایست هم برای میزبان و هم برای شبکه اجرا شود.

### اجرای یک مرور کننده [[34]](#footnote-34)آسیب پذیری

یک همراه لازم برای IDS مرورکننده آسیب پذیری است که گزارش‌هایی را مربوط به آسیب پذیرهای موجود روی میزبانها و دستگاههای شبکه ارائه می‌کند لازم است که یک مرورگر آسیب پذیری IDS توسط جدیدترین فهرست آسیب پذیرها روزآمد شود.

## **ایجاد سرورهای پراکسی**

پیکربندی نمودن ترافیک ورودی و خروجی شبکه از طریق عبور از یک پراکسی، می‌تواند ظهور تهاجمات DDOS را کم نماید. سرورهای پراکسی هم چنین می‌تواند محقق سازد که در آینده مندرج اطلاعات مفیدی بعد از وقوع یک حمله در اختیار خواهید داشت.

برداشت‌ها[[35]](#footnote-35) و صحت پیکربندی‌های موجود را بازبینی کنید به علت اینکه یک تغییر در پیکربندی می‌تواند باعث یک DOS شود. از اینکه بیشتر پیکربندی‌ها حتی الامکان به‌طور متمرکز پشتیبان گرفته شده بازبینی‌های صحت را طبق یک زمان بندی برای میزبانها باید انجام داد هدف یک بازبینی صحت این است که حالت فعلی یک میزبان با حالت مبنای آن مقایسه شود با این کار یک مدیر می‌تواند صحت فایل و فهرست را بازرسی می‌نماید و هر تغییری که توسط مهاجمین انجام شد، آشکار سازد ابزاری که برای یونیکس[[36]](#footnote-36) طراحی شده Trip wire هست.

## **پیکربندی کردن فداکارانه میزبانها**

ایجاد میزبانها با هدف گمراه کردن هجوم‌ها یا جمع آوری اطلاعات در مورد پتانسیل مهاجمان یک مبحث جنجالی است و بسیاری از فاکتورها قبل از اجرای آن بایستی در نظر گرفته شود.

## **افزایش مدیریت میزبان و شبکه**

توسط مونیتور نمودن استفاده از یک منبع در شبکه و میزبانها تأثیرات DDOS ممکن است هنگام مقایسه با عملیات عادی پدیدار شود خیلی از برنامه‌های مدیریت می‌تواند اطلاعات جامع راجع به نرم‌افزار و سرویس‌های که روی میزبانها در حال اجرا است ارائه کند: نگهداری پک روال پاسخ تمام مباحثی که برای تحلیل یک هجوم DDOS نیاز است. باید قبل از این که یک هجوم اتفاق بیفتد در نظر گرفته شود.

## **گسترش بیشتر تکنولوژی‌های امنیت**

برخی از تکنولوژی‌ها برای محافظت در برابر DDOS و رفتارهای مرتبط با آن‌ها توسعه یافته است تکنولوژیهایی نظیر IPVG، امنیت (IPSEC) IP و DNS ایمن (Secure PNS) امکان حفاظت بیشتری را در اختیار قرار می‌دهد. اگر یک هجوم ظاهر شود باید یک روال پاسخ تعریف شده طرح‌های عملکرد، روال‌های تعدیل قیمت و جزییات تماس را داشت.

## **گردآوری اطلاعات**

تماس با یک ISP از ISP باید خواست که برای سایت و پتانسیل تهدید زومبی های شبکه روال‌های شگفت آوری را تنظیم نماید. به کار بردن فیلترهای بیشتر برای متجاوزین!

لیست فیلترها و کنترل دسترسی روی دستگاه‌ها برای کاهش بسته‌های هجومی تغییر داده شود. قواعد محدود سازی بکار رود. اطمینان باید حاصل شود که کمترین تعداد پروتکل‌ها و پوست‌ها از شبکه خارج و یا وارد آن می‌شود برای رسیدن ترافیک مشروع و قانونی به سرورهای مقصد می‌بایست پهنای باند لازم را در اختیار داشت.

## **راههای مختلف جهت مسیردهی**

گزینه‌های مسیردهی را که برای ورود ترافیک قابل دسترسی است تغییر داده شود.

سعی کنید حمله متوقف شود یا استفاده از ابزارهای موجود نظیر zombie zapper ممکن است بتوان به زومبی ها فرمان داد تا حمله را متوقف نماید. تغییر آدرس IP مورد هدف، انجام این کار تاکتیک مناسب برای خیلی سایت‌ها است. اگر یک Daemon که مشغول اجرا روی زومبی ها است یا نام میزبانها پیکربندی شده باشد نه آدرس IP ها، ممکن است این تاکتیک بی فایده شود.

## **مقایسه قابلیت‌های امنیت سرور وب**

هر چند دیوارهای آتش، نرم‌افزارهای ضد ویروس و یک سیستم عامل مطلوب برای طراحی یک سایت ایمن مهم هست اما هیچکدام از این‌ها بانداز قابلیت‌های امنیت خود سرور وب اهمیت ندارد. یک سرور وب شالوده و بنیان یک سایت تجارت الکترونیکی محسوب می‌شود که هر برنامه کاربردی با آن کار می‌کند مبلغی که می‌خواهند هزینه کنند و پلت فرمی[[37]](#footnote-37) که می‌خواهید سرور وب روی آن اجرا شود. مشخص نمایید آنگاه یه موقعیت مقایسه قابلیت‌های امنیت که توسط سرورهای مختلف ارائه می‌شود، می‌رسید.

اگر یک سرور وب تمامی قابلیت‌هایی را که به دنبال آن هستید داراست آنگاه این مورد مهم‌تر از عناوینی است که قبلاً شرح داده شد، اگر یک سرور سایت را ایمن نگه می‌دارد و باعث یک سیستم پایدار است دیگر جای هیچگونه خاستی نیست حداقل هزینه یک سرور با قیمت از دست دادن اطلاعات با بازسازی یک سایت مختل شده مقایسه می‌گردد، در مورد بررسی سرورهای مختلف می‌بایست به برخی از خصوصیات مواردی چون تصدیق کنترل استفاده از پروتکل مبادلات الکترونیکی ایمن تنظیم حقوق و مجوزها و استفاده از برنامه‌های کاربردی CGI توجه شود.

## **تصدیق**

تصدیق یک امر حیاتی برای امنیت اینترنت و سایت‌های اینترنتی هست. چرا که به واسطه مجاز بودن یک کاربر، سرویس یا برنامه‌های کاربردی به ثبوت می‌رسد به عبارت دیگر هویت یک کاربر می‌تواند برای دسترسی به قسمت‌های مختلف یک سیستم مدیریت را بدست گرفته و در شبکه محلی راهی برای خودش ایجاد نماید تصدیق عموماً توسط سیستم عاملی که سرور وب روی آن اجرا می‌شود ارائه می‌گردد چند روش موجود برای انجام تصدیق عبارتند از:

کلمات عبور لایه سوکت های ایمنی SSL گواهی نامه‌ها و امضاهای[[38]](#footnote-38) دیجیتالی کارت‌های هوشمند، کوکی‌ها.

## **کلمات عبور**

کلمات عبور متداولترین روش برای تصدیق است که در وب و شبکه‌های امروزی استفاده می‌شود وارد نمودن یک کلمه، یا کد در یک فیلد در این حل دخالت دارد کلمه عبوری که وارد می‌شود با دیگری که هنگام ایجاد یک شناسه کاربر واردشده مقایسه می‌شود در بیشتر موارد کلمه عبور با یک نام کاربر ترکیب می‌شود. بنابراین کلمه عبور و نام کاربر هر دو می‌بایست قبل از تصدیق کاربر، یکی باشد. انواع مختلفی از تصدیق که یا کلمات عبور درگیر هست وجود دارد و نوع آن را سرور و سیستم عاملی تعیین می‌کند این تصدیق‌ها عبارتند از:

1- بی نام[[39]](#footnote-39)

2- مقدماتی یا متن محض Clear text یا Basic

3- مقدماتی یا رمزکاری SSL

4- مطالبه/ پاسخ ویندوز [[40]](#footnote-40)

کاربران بی نام بسیار شبیه به یک شناسه میهمان عمل می‌کند و هر کاربری اجازه دسترسی می‌دهد این روش برای مشاهده کنندگان سایت برای دسترسی به اطلاعات عمومی نظیر صفحات وبی که محصولات موجود برای فروش را نشان می‌دهد.

* 1. گواهی نامه‌ها و امضاهای دیجیتالی:

روش دیگر تصدیق گواهی نامه‌ها و امضاهای دیجیتالی است این روش‌ها برای اثبات فایل‌ها و پیام‌ها از طرف کاربر یا سازمان ارسال شده تغییر نکرده است به کار می‌رود، در واقع امضاء دیجیتالی یک خلاصه رمز شده از متنی که ارسال می‌شود هست.

هنگامیکه دریافت می‌شود رمزگشایی شده و یا متن دریافتی مقایسه می‌شود اگر هر دو یکی باشد آن گاه درستی و صحت پیام به ثبوت می‌رسد چنانچه سندی پس از ارسال تغییر داده شده باشد خلاصه رمزگشایی شده یکی نخواهد بود به جای امضاء دیجیتالی می‌توان از گواهی نامه دیجیتالی استفاده نمود اطلاعات گواهی نامه CA بستگی به اطلاعاتی که مالک گواهی نامه عرضه می‌کند، گواهی نامه را صادر می‌کند. سپس کاربر یک کلید عمومی که به‌طور دیجیتالی توسط CA امضاء شده را ارسال می‌کند هنگامی که یک فایل به گیرنده ارسال می‌شود گواهی نامه به همراه پیام رمز شده ارسال می‌گردد تا بازبینی شود که فرستنده واقعاً همان شخصی یا سازمانی است که دارنده گواهی نامه است.

گواهی نامه‌های دیجیتالی توسط اشخاص ثالث که در اینترنت استفاده شده یا با استفاده از یک سرور گواهی نامه که روی سرور وب اجرا شده می‌تواند ارسال گردد. برخی از سرورهای وب سرورهای گواهی‌نامه یک پارچه دارند که قادر می‌سازد این سرویس را ارائه دهید.

## **به کارگیری برنامه‌های کاربردی CGI**

پشتیبانی از CGI خصیصه عمومی دیگری از سرورهای وب هست. CGI رابطی است برای دسترسی به اطلاعات بانک‌های اطلاعاتی که از طریق سرویس‌های HTTP روی اینترنت به کار می‌رود CGI برای ارسال یک درخواست به یک برنامه کاربردی به کار می‌رود پس اطلاعات به شکل یک سند HTML به کاربر فرستاده شود، کاربرد CGI دارای برخی اشکالات هست.

## **IIS**

در کنار Netscape, Apache یادگیر بزرگ دیگر در سرورهای وب IIS باشد. IIS 4.0 یا نصب Pack NT Option بطور رایگان برای سرورهای ویندوز NT4.0 ارائه شده.

NT Option pack را می‌توانید از سایت وب مایکروسافت دریافت کرد. یکی از بهترین ویژگی‌های IIS داشتن یک OUI برای نصب و نگهداری سرور وب است که یک روش مساعد – کاربر برای مدیریت سایت شما عرضه می‌کند پشتیبانی ASP ODBC و API های مایکروسافت صورت گرفته است ASP یک روش دینامیک بازگشت اطلاعات از طریق سندهای HTML است ODBC به شما اجازه می‌دهد صفحاتی که با انواع مختلف بانکهای اطلاعاتی ارتباط برقرار می‌کند را ایجاد کنید اشکال این سرور وب این است که فقط برای سیستم عامل‌های NT و ویندوز 2000 سرور قابل استفاده است. IIS 5.0 تمامی ویژگی‌های IIS 4.0 را در بر می‌گیرد و اختلاف آن‌ها این است که در IIS 5.0 ویزارد جدیدی وجود دارد که عملیات متعارف مدیر وب را ساده می‌کند اجازه می‌دهد که وب و تنظیمات امنیت NTFS را Setup می‌کنید. IIS 5.0 همچنین تعدادی از استانداردها را به‌طور وسیع پشتیبانی می‌کند که عبارت‌اند از Fortezza که یک استاندارد امنیت جدید هست که توسط سازمانهای امریکایی به کار رفته است.

## **پورت‌ها، سرویس‌ها و اجزاء بلا استفاده را غیر فعال کنید**

دانستیم که چگونه فیلترسازی بسته و پورت می‌تواند برای کنترل دسترسی به سرور وب مفید باشد هم چنین دیدیم که سرور وب تعدادی از پورت‌های معروف را برای شنود درخواست‌های کامپیوترهای سمت کاربر به کار می‌رود چنانچه سرویس‌هایی ارائه نشود می‌بایست پورت‌هایی مرتبط با این سرویس‌ها را ناشنوا (خاموش) نمود مثال اگر یک سرویس FTP استفاده نمی‌گردد در گاه‌های 20 و 21 می‌بایست مسدود گردد از آن جائی که این پورت‌ها به کار نرفته است. تأثیری در کارایی سایت نخواهد داشت اما یا مسدود کردن آن‌ها امنیت سایت بهبود می‌بخشد سرورها روش‌های مختلفی را برای مسدود کردن پورت‌های بلا استفاده به کار می‌برند.

سرویس‌هایی که نمی‌خواهید توسط سایت ارائه شود حذف یا غیرفعال نمائید مثال اگر در سایت خود سرویس FTP را ارائه نمی‌کنید آن را حذف یا غیر فعال نمائید FTP و غیره انجام دهید.

اگر یک سرور دب دارای یک رابطه مدیریتی باشد سرویس‌های که فعال هست را تعیین کنید.

برای تعیین سرویس‌هایی که قابل دسترسی می‌باشند می‌توان یک مرورگر، یک برنامه FTP یا نرم‌افزار دیگری را به کار ببرید.

هنگامیکه یک سرویس حذف می‌شود کار به اینجا ختم نمی‌شود، اگر یک سرویس طوری تنظیم شده که به‌طور خودکار اجرا شود این سرویس‌ها پس از راه اندازی مجدد سیستم، باز هم قابل دسترسی خواهد بود اگر یک سرویس روی سیستم باقی بماند یک هکر می‌تواند به‌طور بالقوه آن را از دور و یا استفاده از دستوراتی برای فعال کردن آن آغاز نماید. قدم مهم برای ایجاد یک سایت تجارتی الکترونیکی ایمن، حذف، و پاک کردن اجزاء غیر لازم هست.

در مورد آپاچی[[41]](#footnote-41) دیدیم تعدادی از ماژول‌ها برای افزایش قدرت عملیاتی این سرور وب به کار می‌رود.

گونه‌های دیگر سرور وب ممکن است اجزاء یا plug-in های مشابهی را ارائه کند حفره‌های امنیت در اجزاء می‌تواند به‌منظور عملیات غیر مجاز و ناخواسته مختلفی به کار رود.

## **اسکریپت‌ها و فایل‌های غیر لازم را پاک کنید**

هنگامی که سرورهای وب نصب می‌شود مجموعه‌ای از اسکریپت‌های نمونه که می‌تواند برای پکیر بندی سیستم شما یا انجام وظایف متعارف مرتبط با سرور به کار رود نصب می‌گردد اگر این فایل‌ها بر روی سرورها شود احتال دارد که هکرها قادر به دسترسی، تغییر و یا اجزای آن‌ها بشوند یا این کار یک هکر می‌تواند وقایع ناخواسته یا غیرمجازی از جمله Shout down کردن یا خراب کردن سرور را بوجود آورد اگر به اسکریپت‌های خاصی نیاز نداشته یا آن‌ها را پاک کنید یا به فهرستی منتقل کنید که فقط مدیر شبکه یا وب آن دسترسی دارند.

## **هک کردن کلمه عبور و ابزار تجزیه و تحلیل**

دست‌یابی به یک سایت یا شبکه از طریق شناسه وکلمه عبور کاربران دیگر، متداول‌ترین روش هک هست در مورد سیاست‌های کلمه عبور و محافظت شناسه و سایت خود از هک کردن کلمه عبور نکات زیر را به خاطر داشته باشید.

1- سیاست‌ها را روی کلمات عبور معتبر تنظیم کنید.

2- برای کلمات عبور محدودیت زمانی در نظر گرفته و مرتباً آن‌ها را تغییر داد.

3- کلمات عبور مخفی نگه داشته شود.

4- ترمینال‌ها را بدون مراتب و سروسها را بدون انجام امور حفاظتی ترک نکنید.

5- سیاست‌های شناسه را تداوم بخشید.

6- اطلاع از کلمات عبور مدیر را محدود سازید

7- به کاربران اطلاع دهید که مشکلات مشکوک را گزارش نمائید.

در مورد چگونگی انتخاب کلمات عبوری که هک کردن آن‌ها سخت هست به کاربران آگاهی دهید در بسیاری از موارد می‌توان با دقت در آیتم‌های میز کار یا در دفتر هک کاربر کلمه عبور او را بدست آورید بهترین کلمه عبور شامل حروف کوچک و بزرگ (AZ-az) اعداد (0/9) و کاراکترهای ویژه هست بدترین کاری که می‌توان انجام داد که یک کلمه عبور را با کلمه عبور دیگری عوض کنید. برای کلمات عبور می‌بایست محدوده زمانی در نظر گرفت بکار بردن یک کلمه عبور در زمان طولانی، برای کاربر، این خطر را دارد که دیگران آن را کشف کنند.

مورد متداول دیگر وقتی است که کاربران، کلمات عبور را به اشتراک می‌گذارند به جای آن که منتظر حصول مجوزهای مناسب باشند، آن‌ها کلمه عبور خود را از دیگران می‌گیرند. حتی در برخی موارد این قضیه در ین اعضای IT مشاهده می‌شود.

مشکل دیگر رها کردن کامپیوترها بدون مراقب هست ممکن است هنگامی که با دیگر اعضای مدیریت Login شود یک کاربر در شرکت پشت ایستگاه کاری نشسته و روی سایت تأثیر بگذارد با بازبینی مداوم شناسه‌های کاربردی، می‌توان تعین نمود که به کاربران دسترسی به فهرست‌ها و فایل‌های ویژه‌ای داده شده یا نه می بایتس حقوق و مجوزهای داده شده به کاربران را بازبینی نمود.

از گزارش سوءاستفاده از شناسه‌ها و یا مشاهدات مشکلات امنیت تقدیر به عمل آید! بسیاری از اوقات کاربران قبل از شما در می‌یابند که یک هکر به سیستم واردشده اطلاعات مورد دسترسی غیرمجاز قرا رگرفته یا حفره‌های امنیت یا زمانده.

به علت این آن‌ها مسب مشکل قلمداد نشوند به مدیر وب چیزی نمی‌گویند و کاربری که مشغول مشاهده سایت هست به‌طور اتفاقی یک راه مخفی پیدا می‌کند وبه فهرستی که شامل اطلاعات حساس و مهمی است لیز بخورد اگر کاربران بدانند که با دادن چنین اطلاعاتی از آن‌ها قدردانی و تشکر می‌شود آنگاه حفره امنیت را قبل از آن که توسط یک کاربر مالیخولیائی هک شود اصلاح نمائید.

# فصل سوم

**متدولوژی هک کردن**

## **مقدمه**

احتمالاً با حمله سال 2000 به سایتهای یاهو – آمازون وچند سایت معروف٫ که حتی به سایتهای تبلیغاتی نیز حمله شد، همه آن حمله‌ها از نوع توزیع شده در سطح شبکه بود (DDos) و همه در سطح سرویس‌دهنده اختلال ایجاد نموده حملات مختلف و شبیهی نیز در در شبکه‌های مبادله اطلاعات IT اتفاق افتاده سرورها با تجهیز خود توانستند جلوی حملات دیگر را بگیرند ولی هکرها نیز هر روز زیرکتر – باهوش‌تر و زرنگ‌تر شدند و به سوی ایجاد حملات به سوی برنامه‌های کاربردی رفتند.

چرا سایت ما مورد حمله قرار می‌گیرد، به وسیله چه کسی و به چه مقداری این حمله رخ می‌دهد. در این پایان نامه قصد بر آن است که انواع حملات را که از نوع تعیین شده یا شانسی معرفی و در صورت حمله راهکارهای دفاع یادآوری گردد. اگر قبل از فرستادن برنامه کاربردی از حفره‌های مختلف ایجاد شده در برنامه با شبیه سازی مطلع شوید راه ورود برنامه‌های ویروسی را بسته‌اید هر هک کننده‌ای از هکر ناآزموده و بی تجربه که مانند مردی بی هدف و فقط برای جلب توجه به وسایل زیبای شما صدمه می زند تا هکر حرفه‌ای که توانایی دستبای به منافع مالی و بانک اطلاعاتی حساب شمارا داراست همگی جزء هکرها حساب شده و شما باید آمادگی حمله همه آن‌ها را داشته باشید.

با بردن اسم «کوین میت تیک» تمام نظرها به سوی او جلب می‌شود. او یک هکر معروف است که اکنون در زندان به سر می‌برد که در بنی جامعه هکرها به عنوان گوسفند قربانی معروف است و در جامعه باور غلطی وجود دارد که آن اهمیت ندادن به جرائم اینترنتی در بین مردم است.

در ادامه مباحث خواهید فهمید که استراق سمع تلفن و هک اطلاعات یک مسئله خطرناک و مهم است.

این پایان نامه در ایجاد / نوشتن / ارتقا دادن و همچنین بالا بردن سطح کیفیتی برنامه‌های امنیتی برنامه‌های کاربردی کمک زیادی خواهد نمود.

## **درک شرایط و سطوح**

برای درک مفهوم هکر زمان کوتاهی توضیح دادن کافی است. برای درک مفهوم یک هکر راههای مختلفی وجود دارد. به این معنی که در هر لغت نامه‌ای معانی گسترده‌ای به هکر نسبت داده شده است.

در لغت نامه «وبستر»[[42]](#footnote-42) هک کردن به عنوان راههای مختلف برای دزدیدن – خراب کاری و قرار دادن طعمه برای تخریب و سوءاستفاده از اطلاعات دیگران هست. هکر در معنای کلی می‌تواند فردی باشد که مشتاق به انجام کاری در سیستم شما باشد. هر هکری بداندیش و هر هک کردی برای نابودی کار شما نیست. در فنّاوری فناوری اطلاعات هکر می‌تواند خوش نیت و با اخلاقیات کار کند. در دستگاه‌های دولتی هکرها وظیفه فاش کردن و بیان صریح مشکلات و نقایص برنامه را با انجام هک دارند.

در فرهنگ خود هکرها، هکرهایی نام «هکر با کلاه سفید» برای خود در نظر می‌گیرند که مفهوم آن هکر خوب است. یعنی این گونه هک کننده‌ها بداندیش ومضر نیستند در مقابل «هکر با کلاه سیاه» با ورود خود به سیستم شبکه قصد آسیب رسانی دارند. در کل هکرها ازنظر قدرت واقعی نفوذشان طبقه بندی شده و رقابتشان مربوط به قدرت نفوذشان هست. در کل کسانی که با وارد کردن کدهای برنامه نویسی ویروس گونه اسمی در تغییر کار دیگران دارند یا اینکه با شکستن قفلهای نرم‌افزاری صرفاً قصد ورود به سیستم دیگران را دارند جزء هکرها محسوب نمی‌شوند و فقط ماجرا جویی می‌کنند.

در پایان نامه پیش روی شما منظور از هکر در هر بحث منظور فردی است کار آزموده که به‌صورت مهمانی ناخوانده وارد برنامه شما شده و سعی در سوءاستفاده از برنامه کاربردی شما دارد.

## **خلاصه‌ای بر تاریخچه هک کردن**

آغاز هک کردن فعالیتی است مربوط به سال 1940 و 1950 که بر اثر این کار افرادی سعی در استراق سمع مکالمات پلیس و سیستم نظامی حکومت داشتند.]6[ این عمل برای پیدا کردن آگاهی از اتفاقات رخ داده در آن زمان در کشور انجام می‌شد. این عمل برای بدست آوردن طالاعات مهم از بین اطلاعات بی ارزش برای اطلاع از وضع موجود و در مرحله بعد سهیم کردن شبکه‌های رادیویی و اطلاع رسانی آن به کل مردم بود. هک کردن و فنّاوری بسیار زود در 60 سال اخیر به هم پیوند خوردند.

عنوان هک شدن و هک کردن با عنوان هک کردن کامپیوتر در ابتدا برای تخلیه اطلاعاتی کامپیوترهای MIT برگزیده شده در چند سال بعد این سیستم با استفاده از فنّاوری هوش مصنوعی (AI) کار هکرها را پیچیده و سخت کرد.

سال 1960 با راه اندازی آرپانت ARPANET به عنوان شبکه گسترده اولین تشکل مجزای گروه هک کننده‌ها شکل گرفت که پایه کار هک رکدن را در آمریکا پایه ریزی کردند. در این هنگام تنها والدین فرصت برای هکرهای توسط شبکه‌های ARPANET داده شده تا درجهت سود شبکه کار کنند و بتوانند همکاری مسالمت آمیزی داشته باشند.

### سیستم هک کردن تلفن

با بردن اسم «جان دراپر» هم معنی خوبی برای هک کردن تلفن خواهید یافت! او با اطلاع از طول موج سیستم صوتی تلفن که 2600Hz بود توانست روشی برای استراق سمع پیدا کند.

در سال 1970 «ایستووزنیک» و «استیوجابز» با «دراپر» همکاری کردند و «جعبه آبی» را برای استراق سمع تلفن‌های مختلف ساختند.

جعبه مذکور توانایی به خاطر سپردن فرکانس تمامی مکامات را دارا بود تا در آینده نیز نتواند به آن مکالمات گوش دهد. این دستگاه توانایی مسیریابی و دنبال آمدن به سمت فرکانس مورد نظر را دارا بود.

قسمتی از مقصود سازنده ماهر «جعبه آبی» برای استراق سمع و قمستی برای استفاده‌های مجانی از تلفن دیگران برای کار خود بود و با این کار «جان دراپر» در دام قانون افتاد و در سال 1970 به زندان فرستاده شد که در آنجا مشغول تکمیل کار خود است. ]1[

### سیستم هک کردن کامپیوتر

اولین روش هک کردن به ایجاد اولین ساختار شبکه در سال 1950 بر می‌گردد. در هم گیر شدن آرپانت در سال 1969 و NSFNet دستگاه‌های تحت شبکه زیاد شدند. اولین شبکه بین دانشگاههای «کالیفرنیا» در ایالت لس آنجلس، «استن فورد» «وسانتا باربارا» و دانشگانی از «اتوا» ایجاد شد.

برای هک کردن این سیستم‌ها باید حداقل یک هرک در یکی از 4 نقطه اصلی شبکه قرار می‌گرفت و چون این سیستم‌ها معمولاً در دانشگاه تجمع داشتند این کار تقریباً سخت بود. ]5[

با گسترش شبکه و ایجاد اینترنت سیستم هک کردن نیز پیشرفت کرد به‌طوری که افرادی با آموزش تیمی خاص و جمع آوری افراد خبره در کار هک کردن برای انجام این کار کوشش می‌کردند. در این حال دانشگاههای چون «استن فورد» با استفاده از سیستم هوش مصنوعی این روند را مخاطره انداخت.

در این زمان شرکت DEC که سازنده مینی کامپیوتر در آن زمان بود با پیشنهاد خود مبنی بر ساخت و تولید سری کامپیوترهای شخصی برای تهیه دانشگاهها با نرخ پائین نظر دانشگاه «استن فورد»را جلب نمود و برای گسترش سیستم شبکه اقدام نمود.

آرپانت به عنوان یک شبکه از کامپیوترهای DEC فعالیت خود را آغاز کرد. در گذر زمان انواع کامپیوترهای داخل شبکه از PDP-10به PDP-15 تغییر کرند. یا تغییر شبکه‌ها، کامپیوترها نیز تغییر کرد به‌صورتیکه دستگاه‌های اشتارک زمانی وارد شد در این مسیر شرکت سازندة DEC ساختاری را طراحی کرد که برای خودش مورد استفاده و راحت باشد. در مسیر تغییرات زبان برنامه نویسی اولیه که ITS نام داشت تبدیل به زبان قوی، قابل انعطاف و مورد استفادة ساده به نام LISP شد.

در این هنگام تشکلی به نام BBS برای تجمع و گردآوری اطلاعات هکرهای حرفه‌ای بنا شد و بر اساس این کار هر هک کننده‌ای باید برای شناسایی به عنوان هکر در این کلوپ ثبت نام می‌کرد.

تا سال 1981 که IBM کامپیوترهای شخصی کوچک متشکل از CPU و سخت افزار و حافظه را طراحی نکرده بود تمامی سیستمها همچنان در انحاصر دانشگاه‌ها و دستگاه‌های دولتی بودند. با آمدن کامپیوترهای شخصی IBM به بازار کم کم آرپانت تبدیل به اینترنت شد، تعداد اعضای BBS زیاد و جرائم اینترنتی رو به گسترش نهاد. برای این جرائم از قبیل استراق سمع email شخصی افراد یک سال زندانی تعیین شده فقط بانک شیکاگو از این جرائم 70 میلیون دلار متضرر شد!

گروه هکرهای حرفه‌ای کم کم از هم جدا شدند و هر کدام تشکیل یک گروه هکر جدید را دادند. فقط در یک فقره، کرم طراحی شده به دست روبرت موریس باعث آلودگی 6 هزار سیستم در کل آمریکا شد. آمراها کم کم وحشتناک و وحشتناک‌تر می‌شد به‌صورتیکه 95% شرکت‌ها دست کم مورد حمله 500 گونه برنامه خطرناک و 20 تا 30 درصد نیز به‌طور کلی از طرف این حمله‌ها اطلاعتشان به سرقت رفته است.

بسیاری از دستگاه‌های شرکت‌های بزرگ به تجهیزات مختلف مجهز شدند تا در جلوگیری از هک شدن موفق باشند ولی برنامه‌های هکرها به دستگاه‌های بی دفاع کاربران نهایی نیز حمله می‌کند.

## **عوامل تحریک هکرها چیست؟**

معروفیت به بدنامی، مشهور شدن، رقابت، خستگی از کارهای خسته کننده و انتقام تنها قسمتی که از عوامل محرک هکرها می‌باشند. در کل هکرها با قصد بر وارد این کار نمی‌شوند. یعنی هر هکری ابتدا فقط برای آگاهی از مهارت خود و شاید کمی کنجکاوی به این کار دست بزند ولی در مرور زمان و با بالا رفتن مهارت، کم کم به‌صورت پتانسیلی در وجود خود هر این قدرت نهادینه شده و متوجه عمل کار خود در سیستم‌ها خواهد شده تصور غلط این است که هر هکری می‌خواهد با عمل خود به قصد شخصی خود برسد ولی این اشتباه است چون هر هکری با انجام این کار به خود ثابت می‌کند که می‌تواند.

علت اصلی شهرت یابی، حسادت، خود کم بینی و کلاً مشکلات شخصیتی باعث انجام این کار می‌شود. (متأسفانه این عوامل وقتی شناخته می‌شود که شخص در دادگاه به سر می‌برد)

علت دیگر رقابت و سلطه جویی فکری هست. به این معنی که یک هکر توانایی پیدا کردن حفره‌ای در سیستم هست که دیگران نمی‌توانند.

### مقابله در برابر هک کننده‌های بداندیش

آیا مورد تهدید هکرها قرار گرفته‌اید. اغلب جواب این سئوال مثبت است و شما به علت‌های مختلف مورد هک و تهدید قرار گرفته‌اید. در این مسیر افراد متخصص در امر امنیت داده‌ها سعی در آن دارند که با جست وخیز در اطلاعات بانک خود راههای احتمالی را سهواً پیدا کنند تا جلوی آن را در مقابل هکرهای سارق اطلاعات بگیرند. آن‌ها برای همین کار مورد خطاب قرار می‌گیرند و به علت اینکه توانایی پیدا کردن مشکلات برنامه‌های کاربردی را دارند حقوق می‌گیرند. همچنین آن‌ها باید اطلاعاتی را که از ضعفهای سیستم برنامه کاربردی پیدا کرده‌اند را جایی فاش نسازند. این تلاشهای انجام شده توسط گروه هکرهای خیرخواه برای جلوگیری از انجام موفقیت آمیز هک بوسیله هکرهای بداندیش هست.

در سوی دیگر هکرهای بداندیش می‌خواهند تا از حفره‌ها و نقایص سیستم استفاده کرده و آن را به ترتیبی خاص در اختیار افراد سودجو قرار دهند تا در نهایت صدمه به سیستم بزنند. در کل کار هکرها از هر 2 نوع خود قابل تأمل هست. به‌طوری که اگر حتی هکری خوب بوده و کار را درست انجام داده باشد باز مثل هکر بداندیش اطلاعات را می‌داند و اگر بخواهد می‌تواند به سیستم صدمه برساند پس اگر شرکتی درخواست نیاز به هکر یاری دهنده نداشته باشد اصلاً نباید برای این کار اقدام کرد.

### کار کردن با حرفه‌ای‌های عرصه امنیت داده‌ها

آخرین راهکار مقابله با حمله هکرهای ناخوانده و بداندیش استفاده از حرفه‌ای‌های امنیت داده‌ها به عنوان کارمند شرکت‌ها هست. این روش را به راه آوردن هکرها گویند. در این روش شرکتها قصد دارند تا به بکار گرفتن قدرت نهفته هکرها آن‌ها را کنترل کنند.

این روش بهترین و منطقی‌ترین روش برای جلوگیری از هک شدن و گسترش برنامه‌های کاربردی هست. در بسیاری موارد افراد حرفه‌ای به خدمت شرکتها در می‌آیند و به‌صورت تمام وقت کار انجام می‌دهند و هر از گاهی با زیر نظر گرفتن سیستم امنیتی موجود اشکالات آن را بیان کرده و در مسیر ترقی سیستم پیشنهاد می‌کنند.

حرفه‌ای‌های عرصه امنیت داده‌ها به روشهای هکرها آشنا بوده و طریقه حمله آن‌ها را می‌شناسند. با آگاهی از روش‌های آن‌ها برای مقابله با هک شدن کارهایی انجام می‌دهند. کارهایی که این متخصصیان انجام می‌دهند باعث پیشرفت سطح امنیت سیستم برنامه کاربردی می‌شود.

### کم کردن مشکلات با به خدمت گرفتن سیستم امنیتی

به کار گیری افرادی که در امر مبارزه با حملات هکرها خبره هستند بسیار سودمند است و غیر قابل چشم پوشی است. این افراد حرفه‌ای موقعیت خاصی را فراهم می‌کنند تا تمام خطاهای برنامه‌های کاربردی ما معلوم شده و کاملاً فاش گردند. این کار مثل یک تمرین می‌ماند. واضح و مبرهن است که افراد کارآزموده در امر امنیت داده‌ها نمی‌توانند تمهیداتی برای جلوگیری از حمله اینترنتی در آینده باندیشند.

این پتانسیل در هر هکری باشد که با بدست آوردن اطلاعاتی بتواند به سری جدیدی از منابع اطلاعاتی دست پیدا کند که او را در انجام کار خود در آینده یاری کند. پس چگونه باید شرکتها خود را حفظ کنند؟ قدم اول پیدا کردن افراد حرفه‌ای قابل اعتماد است. روش کار آن‌ها نیز مهم است: آیا آن‌ها برنامه را مرور می‌کنند یا به برنامه حمله می‌کنند یا اینکه نقاط ضعف کار را پیدا می‌کنند. این به کارگیری از نگاه شرکتها نیز متفاوت است. یک شرکت دنبال کسی می‌گردد که «درهای پشتی» سیستم برنامه کاربردی تهیه شده توسط شرکت را نشان دهد و شرکتی دیگر به دنبال کسی می‌گردد که امنیت داده را از پایه بسازد و آن را ایمن کند. برای این کار بهتر است اهداف مشخص باشد. تمام نقشه‌ها، الگوها و آینده نگری ها یادداشت شده و نیازمندی‌ها کاملاً مطرح گشته و کار ادامه یابد.

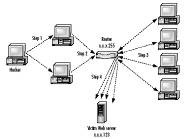
## **شناخت انواع حملات در دستگاه‌های موجود**

دزدان کارت اعتباری- راهزنی اطلاعات و دزدان هویت نمونه‌هایی از دزدی‌هایی هستند که قصد ورود به بانک‌های اطلاعاتی یا شبکه ما را دارند. بعضی از حمله‌ها جنبه تخریب ندارند و بعضی برای قطع و از کار انداختن کارهای ما هست مثل عملی خرابکارانه DDos، ویروس‌های هک کننده، اسب تروآ، کرم‌ها، لیب زهرآلود و... از نمونه‌هایی از این خرابکاری‌ها هست که در این پایان نامه به آن‌ها پرداخته می شود.

## **Dos/ DDos**

بر اساس آمار سی ان ان[[43]](#footnote-43) جدیدترین حمله DDOs که در سال 2000 اتفاق افتاد باعث متحرز شدن شرکت‌های مربوط در حدود یک میلیارد دلار شد. این هزینه برآورد شده همچنین شامل هزینه‌های سنگین قوی کردن سیستم‌ها توسط شرکت‌های امنیت داده‌ها نیز هست. این نکته مهم است که این هزینه برآورد شده همچنین شامل هزینه‌های سنگین قوی کردن سیستم‌ها توسط شرکت‌های امنیت داده‌ها نیز هست، این نکته مهم است که این هزینه به جهت تأخیر یک تا دو ساعته دستگاه‌های کاربردی در شبکه هست. در واقعیت بزرگترین شرکت متضرر در این حمله شرکت یاهو بود که سایت در حدود 5 ساعت از کار افتاد. ]11[

سیستم هک کردن DDos اینگونه است که سرویس‌دهنده را در حین ارسال اطلاعات غافلگیر می‌کند. در این نوع هک کردن یک پیام همه گیر[[44]](#footnote-44) برای همه کامپیوترها ارسال می‌شود و از آن‌ها آدرس حقیقی را می‌خواهد (X.X.X.255 در زیر شبکه) و بوسیله یک آدرس دروغین اطلاعات آدرسی کامپیوترهای قربانی را دریافت می‌کند. این مرحله اول است. ]7[

بعد از آن که دستور به مسیریاب داده شد روتر تمام آن‌ها را در مسیرهای خود کپی می‌کند و آدرس ICMP را از کامپیوترها می‌خواهد. با این روش تمام کامپیوترها در خدمت روتر قرار گرفته و خود روتر ها نیز تحت فرمان هکر قرار می‌گیرد و آن‌ها در مقابل هر درخواست روتر تسلیم شده و اطلاعات حیاتی را ارسال می‌کنند. با تحت فرمان قرا رگرفتن روترها شبکه از مدار اصلی خود خارج شده و تبدیل به دست یک فرد می‌شود. در این هنگام به علت مدیریت ناکافی و اشتباه و غیر اصولی هکر روترها توانایی هماهنگی سیستم‌ها را در دریافت و ارسال نخواهد داشت به همین دلیل کم کم بالانس شبکه از بین رفته و دیگر امکان سرویس دادن از بین می‌رود و شبکه در حالت DOS قرار می‌گیرد. ]4[

شکل (3-1)

نمونه قابل دسترس این کار در مورد ادعای شرکت ماکروسافت در ساخت برنامه‌ای بود که به نظر خودش بسیار زیرک و سریع بود و قابل هک شدن نبود. در این هنگام هکرها با حمله‌ای سراسری سیستم را پائین آوردند ونشان دادند که هکرها قدرتمندتر از آن هستند که به نظر می‌رسد و توانستند فروش online این محصول را چند ساعت به تعویق بیاندازند.

بعد از حادثه سال 2000 «کوین میت نیک» توصیه‌ای به صاحبان شرکتها در همین زمینه کرد که متن این توصیه نامه اینگونه است سه پیشنهاد برای جلوگیری از هک شدن.

1. از ابزارهای کنترل کننده شبکه استفاده کنید تا پاکتهای رسیده شده را با نام و تاریخ و مبدأ جدا کند.
2. سیستم کامپیوتری خود را (از جمله کامپیوتر شخصی تا شبکه بزرگ خود) در چندین زیر شبکه قرار دهید و امکان ارسال و دریافت را درهر سه شبکه فعال کنید تا مورد سوءاستفاده غیر قانونی قرار نگیرد (بر اساس انواع پروتکل‌های زیر شبکه‌ها)
3. نرم‌افزارهای کاربردی را در سیستم خود نصب کنید تا پاکتهای غیره عادی و بدون نام و Broadcast را جدا کرده و با تشخیص خود حذف و بازارسال به مبداء کند.

## **ویروس‌های هک کننده**

ویروس‌ها در معنای عام به عنوان برنامه‌های خود مختاری معرفی شده‌اند که می‌توانند بانفوذ خود به سیستم کامپیوتری دستورات را تخریب، تغییر و مورد سوءاستفاده قرار دهند. ویروس‌ها بر اساس دوری کردن از برنامه‌های جستجوگر طراحی می‌شوند. مثل هر برنامه‌ای برنامه ویروس توانایی اجرا در سیستم کامپیوتری شمارا دارا هست و می‌تواند با اجرا شدن در کامپیوتر شما امور سیستم شمارا در دست خود بگیرد. این اجرا می‌تواند تبعاتی چون پاشیدگی اطلاعات شما، ناپدید شدن اطلاعات، پدیدار شدن پیام خاص و یا باعث اشتباه عمل کردن برنامه شما شود.

اکنون روش تکثیر ویروسهای کامپیوتری را بیشتر بررسی می شود. این که برنامه نویسی شهر با کپی کردن خود به روی حافظه کامپیوتری دیگر تکثیر شده و باعث خرابی در شبکه می‌شود. این نقل و انتقال می‌تواند با وسایل بسیار ساده‌ای چون فلاپی و هارد دیسک، برنامه‌های قانونی شبکه و حتی حرکت در بین شبکه‌ها اتفاق بیافتد یک سمت این مبادله یک کامپیوتر آلوده است. به یاد داشته باشید که برنامه حتماً باید اجرا شود تا ویروس شکل بگیرد. برای این کار حتماً باید برنامه را اجرا شود به همین دلیل این برنامه‌ها با پسوندهای مختلفی چون OS، Sis فرستاده می‌شود تا کاربران را اجرا نماید نوع دیگر به برنامه در هنگام شکلگیری نصب، راه اندازی و دادن کد صحیح حمله می‌کنند.

انواع ویروسها بسیار زیاد هست که نمی‌توان به راحتی آن‌ها را دسته بندی کرد. این مشکل از آن جهت حادتر می‌گردد که توسعه دهندگان ویروسها که هکرهای ماهری هستند از این حرفی نمی‌زنند تا راز کار خود را مخفی نگاه داشته و این باعث آن می‌شود که هیچ راه مطمئنی برای جلوگیری از اجرای این برنامه‌ها نتوان پیدا کرد. در زیر شش دسته مختلف که در مورد ویروسها متفاوت است (ازنظر طریقه حمله و تلاش برای پیروزی) بیان شده:

1. پارازیت (انگل): این نوع ویروسها بر روی فایلهای اجرایی داخ کامپیوتر تأثیر دارند. این ویرسها به‌صورت نمونه شکل فایل سیستم میزبان هیچ چیزی را تغییر یافته نمی‌یابد ولی در حقیقت که ویروس‌ها اول اجرا شده است.
2. بخش خود گردان: این نوع ویروس در قسمت اول دیسک سخت جای می‌گیرد، این منطقه شامل فلاپی دیسک هم می‌شود. این ویروس در محل ذخیره اطلاعات روی دیسک فلاپی قرار می‌گیرد وبا ورود بر روی روال شروع کار سیستم و همان عمل boot شدن کامپیوتر تأثیر می گدارد و باعث خاموش شدن و دیگر روشن نشدن سیستم می‌شود.
3. چند قسمتی: این روش به قسمتهای مختلفی تقسیم می‌شوند که این قسمتها را می‌توان از هم پنداشت، مثل قسمت ویروس پارازیتی یا ویروس تأثیرگذار بر روی عمل Boot
4. هم دم بودن: این روش به این صورت عمل می‌کند که یک برنامه هم نام با یک برنامه موجود و قانونی در سیستم توسط ویروس ایجاد می‌شود و OS آن را بر اساس تصور قانونی بودن اجرا می‌کند و ویروس در سیستم، حافظه و دیگر دستگاههای جانبیو حتی بشکه پخش می‌گردد.
5. پیوسته (Link): ویروس در سیستم، حافظه و دیگر دستگاههای جانبی و حتی بشکه پخش می‌گردد. اجرا و بعد برنامه درخواستی اجرا می‌شود. در نتیجه این ویروسها بسیار خطرناک هستند چون می‌توانند تمام اطلاعات اولیه اعم از توابع کتابخانه‌ای را تحت تأثیر و خرابی قرار دهند. تمام برنامه‌های اجرایی وتوانند هدف این نوع ویروس قرار گیرند.
6. فایل اطلاعات: ویروس فایل اطلاعاتی می‌توانند باز شوند، دستکاری کنند و بسته گردند. به همین علت این نوع ویروس باز بانهای خاصی نگارش می‌شوند تا به‌طور اتوماتیک وقتی برنامه‌ای قانونی اجرا شد آن‌ها نیز باز شوند و در سطح سیستم‌ها پخش گردند.

## **روش‌های صدمه و دفاع در برابر حمله**

بهترین روش پشتیبان گرفتن قسمت حفاظتی دیسک فلاپی را بندید تا در مقابل ورود ویروسها دفاع خوبی انجام گیرد. با استفاده از برنامه‌هایی که منبع درست و موثقی دارند در شرکت آن‌ها معلوم است نیز می‌توانید در برابر ورود ویروس به سیستم کاری کرده باشد. همیشه برنامه‌ها را بروری دستگاه‌های مخصوص تست، آزمایش و اجرا کنید تا مطمئن شوید که این برنامه بدون ویروس است.

## **اسب تروآ**

این نوع ویروس از انواع قدیمی و ویروسهای هک کننده هستند که در قالب بی خطر قرار گرفته ولی بعد از اجرا مثل یک ویروس خطرناک سیستم را تحت تأثیر قرار می‌دهد. نام این نوع ویروس از ایلیاد هومر گرفته شده است. که داستانی چون داستان اسب تروآ در سواحل یونان باستان دارد. داخل یک قالب بی خطر ویروس نهفته می‌گردد تا بعد از باز کردن برنامه خطر ساز شود. این نمونه ویروس معمولاً به‌صورت یک برنامه خنده دار یا یک بازی کوتاه تغییر قیافه می‌دهد. این نوع ویروس در برنامه کوتاهی نهفته است و بعد از خروج و اجرا شدن می‌تواند کل دیسک سخت شمارا خراب کند.

هم اکنون، تمام برنامه‌های اسب تروآ خطرناک نیستند و برنامه‌های بداندیشانه در خود ذخیره نمی‌کنند ولی به‌صورت پتانسیلی در خود نهفته دارند. بعد از دسترسی به محل مناسب ویروس می‌تواند به دیگر مناطق سیستم خود را کپی کند و در این حالت مثل یک کرم نرم‌افزاری عمل می‌کند.

راه معمول برای آلوده کردن سیستم شما به ویروس اسب تروآ آن است که یک فایل از طرف کس به شما ارسال شود که در ضمیمه آن فایلی اجرایی موجوداست که شما باید آن را اجرا نمائید این برنامه می‌تواند به سادگی یک برنامه اجرایی٫ یک بازی ساده یا حتی یک شوخی یا طنز تصویری باشد. با چشمان عریان شما (بدون هیچگونه علمی از ساختار برنامه‌های ویروسی) هیچ چیز عجیبی در هنگام اجرا شدن برنامه برای سیستم شما اتفاق نمی‌افتد. فقط چیز قابل بیان این است که برنامه ویروسی تروآ اکنون در سیستم شما نصب‌شده است یا مقادیر اولیه آن در سیستم ایجاد شده است! چیز ترسناک در این برنامه این است که برنامه تروآ می‌تواند مانندیک ماشین دارای کنترل از راه دور عمل کند! از این به بعد هر کسی که این برنامه را برای شما ارسال کرده می‌تواند از طری شبکه به محتویات سیستم شما دسترسی داشته باشد. هکرها به برنامه‌های پیشرفته‌ای مجهز هستند که می توانندبفهمند کدام سیستم برنامه تروآ را اجرا کرده است. بعد از پیدا کردن کامپیوتر شما توسط برنامه جستجوگر پیشرفته، هکر می‌تواند به تمام اطلاعات شما دسترسی پیدا کند. 2 نوع مورد توجه در ویروس‌های تروآ Back orfice و Net Bus هستند.

نوع اول Back orfice با قرار دادن طعمه‌ای برای کاربر برنامه را اجرا و بعد از آن سیستم کاربر به‌صورت ناخواسته آن کار را با بقیه سیستم انجام می‌دهد. به این صورت که سیستم کاربر با اجرای برنامه اسب تروآ، تمام منابع اطلاعاتی حیاتی خود و دیگر سیستم‌ها را برای هکر می‌فرستد و از این نظر این روش بسیار خطرناک است.

این روش چهار مزیت برای هکرها نیز دارد: 1- این روش برای سیستمی که سیستم عامل آن فعال است ایجاد می‌شود پس بیشتر مواقع این روش کاربرد دارد. 2- همچنین این عمل که اجرا شدن یک برنامه در سیستم است در Task Bar آورده نمی‌شود و با چشمان ما دیده نمی‌شود و به‌طور کلی روشی بسیار مخفی وپنهان است.

روش دیگر یا نوعی دیگر از ویروسهای اسب تروآ "Subserver" نامیده می‌شوند. این نوع از ویروسهای تروآ به همراه پست الکترونیکی ارسال می‌شوند و در ضمیمه ایمیل قرار می‌گیرند. به این معنا که با قرار گرفتن بر روی سیستم و اجرا شدن پیغامی برای کاربر ارسال می‌کند که باعث گمراهی او می‌شود. این پیغام بیانگر قصد و نیبت خیر نشده است. این ویروس امکان کاملی به هکر می‌دهد تا به‌طور کامل به تمام منابع اطلاعاتی شما در کامپیوتر خود را به او بدهید و حتی هکر توانایی حذف فایل و پوشه‌های شمارا داشته باشد. این ویروس حتی توانایی نمایش صفحه نمایش قربانی را نیز دارا هست.

در آگوست سال 2000 نوع جدیدی از ویروسهای تروآ معرفی شد به نام اسب تروآی مدل QAZ. این نوع ویروس توانایی حمله به شبکه مایکرسافت را دارا بود و می‌توانست تمام منابع که برنامه‌های شرکت ماکروسافت را غارت کند. این ویروس از طریق زیر شبکه‌های کوچک پخش شد و در داخل برنامه نوت پد[[45]](#footnote-45) به‌صورت اجرایی موجود بود.

آن چیزی که این نوع ویروس اسب تروآ را خطرناک و مخرب می‌سازد آن است که این ویروس با تحت اختیار گرفتن پرت 7597 که برای ارتباط با شبکه است سیستم کامپیوتر شمارا در اختیار هکر از راه هدر می‌گذارد و هکر می‌تواند به راحتی به اطلاعات شما دستیابی داشته باشد. این نوع ویروس تروآ که نوع آن QAZ هست قابل انتقال از طریق ایمیل و یا چت روم هست، به همین طریق در شبکه‌های محلی نیز قابل انتشار و تخریب هست.

کاربر با اجرا کردن نوت پد ویروس را به حالت فعال در می‌آورد. این ویروس در سطح شبکه به دنبال کامپیوتر تنهایی می‌گردد که نوت پد را داشته باشد. اولین کار ویروس تغییر نام Note pad.exe به Notepad.com هست و با این کار ویروس در سیستم آماده است. حال ویروس فایل Notepad.exe مخصوص خود که حاوی ویروس است را به سیتسم ارائه داده که حجم آن حدود 320 و 120 بایت است. حال دیگر ویروس منتظر اجرای ویروس توسط کاربر می‌ماند و پس از آن پورت 7597 را تسخیر می‌کند.

## **کرم‌ها**

شما اگر با کامپیوتر خود کار می‌کنید حتماً ویروسهایی چون ویروس Iloveyou[[46]](#footnote-46) یا ویروس ملیسا را می‌شناسید. این 2 ویروس از نمونه هی کرم‌ها هستند. جدیدترین کرمی که به شبکه حمله کرده است کرم آناکورنیکووا می باشدکه در سال 2001 ظاهر شد.

این کرم توسط پسری 20 ساله در هلند تولید شد، کسی که خود را با نام بر بال پرواز معرفی می‌کرد. چیز ترسناک این بود که این کرم توسط کسی تولید شده بود که علم چندانی در مورد هک کردن نداشت. او تقریباً در این کار جزء تازه کارها قلمداد می‌شده او از برنامه ویروس کش خاصی برای ایجاد کد خود استفاده کرد که این برنامه توسط هکر معروض به نام K ساخته شده بود. این برنامه توانایی تولید و زیاد کردن برنامه کرمها را در سطح شبکه برای هکر ایجادمی کرد. ]5[

این برنامه‌ها نوعی ویروس هستند که باعث خرابی در سیستم نمی‌شوند و بروری حافظه جانبی قرار گرفته و از خود نسخه دومی تهیه می‌کنند و توسط شبکه در سطح شبکه پخش می‌شوند. این کرمها سیستم را درست می‌گیرند و از منابع استفاده می‌کنند و طوری عمل می‌کنند که از دید کاربر مخفی به نظر می‌رسند. کرم‌ها زمانی به سیستم حمله ور می‌شوند که سیستم دیگر دفاعی ندارد و در برابر خطر کاملاً بی دفاع است. این کرم‌ها می‌توانند برای برآورده کردن مقاصد شوم سازندگانشان نیز مناسب باشند. طریقه انتقال کرمها از طریق ایمیل یا ازطریق اتاق چت هست.

کرم "Iloveyou" در سال 2001 توانست به سرعتی فوق العاده در شبکه پخش شود و تمام شبکه را طبخ کند. این ترم ابتدادر اروپا و بعد در آمریکا مورد پیگیری قرار گرفت. این ترم به عوان یک ایمیل در ابتدا با نام love-letter-for-you برای همه ارسال شد و وقتی این نامه توسط کاربر باز شد کرم بعد از خورج و ورود به سیستم کاربر این نام را کپی و به تمام آدرسهای موجود در دفترچه آدرسهای کاربر ارسال کرد. به این علت سرعت پخش این کرم در شبکه بسیار زیاد بود. این ویروس توانست در طی 12 ساعت یک میلیون و نیم کامپیوتر را در سطح زمین آلوده کند.

در کل راهی برای جلوگیری از حمله کرمها در سطح شبکه وجود ندارد به همین علت تنها راه جلوگیری آگاهی و تدابیر امنیتی و اطلاعاتی هست. با این توصیفات کاربر بهتر است ایمیل‌های ناشناس را باز نکند و برنامه‌ای از روی سایت دانلود نکند که قابل اطمینان نیست. در اصل کل کار جلوگیری از حمله کرم در دستان کاربر نهایی هست. کاربران سطح بالای شبکه‌ها بایددر راه آموزش کاربران نهایی کوشش کنند و اطمینان دهند که کرمها تا شما آن‌ها را اجرا نکنید قابلت حمله به سیستم شمارا ندارند.

## **برنامه‌های ولگرد**

کدهای تحت سیستم راه دور که به زبان جاوا، جاوا اسکریپت و اکتیو ایکس هست کدهایی بسیار سودمند هستند که بسیار برای ایجاد برنامه‌های کاربردی و application مؤثر می‌باشند. این کرمها همچنین راه مناسبی برای انتقال اطلاعات و کدهای مخرب می‌باشند این برنامه‌ها کلاً برای دو نسخه ایجاد کردن خود و تکثیر زیاد طراحی نمی‌شوند و بیشتر برای حمله به سیستم و دزدی اطلاعات شما مناسب هستند و حتی در مواردی به تخریب و گاهی باعث خاموشی دستگاه شما می‌شوند. همانطور که در قسمت‌های قبلی پروژه ما خوانده‌اید نرم‌افزارهای جاوا و اکتیو ایکس برای ایجاد نرم‌افزارهای قدرتمند جهت جلوگیری از دزدی اطلاعات به کار می‌روند ولی در نوع برنامه‌های ولگرد کاربردی ندارند.

منظور از سیستم راه دور (تلفن همراه) به این معنی است که این برنامه‌ها توانایی ارتباط با هکر به سیستم شمارا از راه دور می‌دهد. به همین دلیل کاربر می‌تواند با دقت به منفع از غیر قابل اعتماد بودن منبع اطلاع کسب کند. کدهای راه دور از جمله برنامه‌های سطح پائین هستند که در پائین سطوح آن را خواهید دید:

1. کنترل دستیابی: این قسمت چک می‌کند که آیا دسترسی مجاز هست یا خیر؟
2. تأیید کاربر: تست درستی شماره کاربر
3. تست دیتا: تست اینکه که دست نخوارده است.
4. درصد اعتماد به اطلاعات: درصد اعتماد به اطلاعات چک می‌شود.
5. رسیدگی: برای کنترل برنامه راه دور تمام مسیر پیمایش می‌شود.

برنامه‌های ولگرد مثالی خوب از برنامه‌های مخرب هستند. با دانستن بهتر در مورد چگونگی عملکرد برنامه‌های مخرب بهتر می‌توانید برای جلوگیری از حمله آن‌ها تمهیدایت باندیشید.

## **دزدیدن**

وقتی اسم دزدیدن در شبکه به میان می‌آید مسئله بسیار پیچیده می‌شود. وقتی بچه‌ای می وید دامن امروز دزدی کردم! این جمله می‌تواند دزدیدن یک شکلات، یک جفت کفش، یک ماشین یا میلیونها دلار باشد. آیا آن‌ها از دوستشان یا از بانک یا از یک مغازه دزدید کرده‌اند؟ ما در تمام موارد عنوان «دزدی کردن» را به کار می‌بریم.

برای دزدی کردن در شبکه فقط دزدی پول مطرح نیست. دزدی یک هویت، دزدی یک نسخه دارویی به‌طور کلی دزدی اطلاعات ضروری می‌تواند عنوان دزدی را بگیرد.

### دزدان کارت اعتباری

از نگاه مصرف کنندگان دزدات کارت اعتباری نوعی هکر هستند. بر اساس تفکر بسیاری از کسانی که به کامپیوتر اعتماد ندارند و برای خرید خود از اینترنت استفاده نمی‌کنند، کار با شبکه و خرید اینترنتی بسیار خطرناک بوده و در این زمینه افسانه‌های بسیار زیادی در مورد کلاهبرداری اینترنتی در زندگی شهرنشینی نقل می‌شود! آن‌ها می گویند هر گاه از کارت اعتباری در اینترنت استفاده کرده اندکسی آمده و تمام اطلاعات آن‌ها را دزدیده و پول حساب آن‌ها را خالی کرده است. همچنین کسانی عقیده‌ای بر عکس دارند! آن‌ها می گویند روش خرید از اینترنت امن‌ترین و راحت‌ترین راه است. واقعیت دراین میان خوابیده است! آیا دزدی کارت اعتباری واقعیت دارد؟

بزرگ‌ترین دزدی کارت اعتباری مربوط به سایت Egghead.com بود که چندین هکر به آن حمله کردند ول تکنسینهای مختلف شرکت توانستند در مقابل این نوع حمله دفاع کنند. این پایگاه داده شامل اسم، فایل، آدرس، شماره کارت، تاریخ شروع، تاریخ انقضای کارت و آدرس email مشتری بود.

حمله تازه‌تر در سال 2000 اتفاق افتاد. سایت CDuniverse.com شامل اطلاعاتی در مورد دانشکده موسیقی بود. هنگام وقوع این حمله بسیاری از افراد از کارت اعتباری در اینترنت استفاده می‌کردند. این حمله توسط پسری 18 ساله که در روسیه زندگی می‌کرد اتفاق افتاد. او با ورود به سایت توانسته بود حفره سایت را پیدا کند. او با ارسال درخواستی خواستار پرداخت صد هزار دلار از طرف شرکت به او شد و او در عوض پول دریافتی حفره برنامه کاربردی را به آن‌ها خواهد گفت. با رد کردن درخواست وی توسط شرکت او به سایت حمله کرد و اطلاعات چندین هزار کارت را دزدید که شامل شماره کارت، تاریخ انقضاء و ایمیل مشتری بود. او توانسته بود بیش از سیصد هزار رکورد را از شبکه بدزد.

بعد از این عمل پسر 18 ساله تمام اطلاعات حساب سرقتی خود را بر روی سایت شخصی خود قرار داد تا به همگان ناامن بودن شرکتهای کارت اعتباری را نشان دهد وی بعد از چنددقیقه ارتباط سایت او با شبکه توسط قطع ISP سرویس‌دهنده وی قطع شده بعد از آن شرکت سیستم امنیتی را قوی‌تر کرد و پسر 18 ساله‌ای که خود را «ماکسیوس» معرفی می‌کرد هرگز دستگیر نشد.

### دزدی هویت

علت مهم بعدی هک کردن دزدی هویت هست. هیچ فرقی نمی‌کند که اطلاعات دزدیده شده مربوط به یک سپت مهم در داخل حکومت آمریکا باشد یا اطلاعات یک شرکت کوچک در هر 2 صورت برای بدست آوردن اطلاعات بدرد بخور توسط هکرها باید تمام اطلاعات از قبل ردیابی شود. علاوه بر اسم قربانی اطلاعاتی چون لیست پائین نیز از دزدی هویت حاصل می‌گردد.

آدرس / شماره محرمانه فرد در قسمت تأمین اجتماعی / اطلاعات کارت اعتباری / روز تولد شماره گواهینامه رانندگی این اطلاعات به راحتی می‌توانند قربانی را وادار به اطاعت از هکر کننده دزدان هویت این روش را برای تصاحب کردن اموال فردی دیگر استفاده می‌کنند. علاوه بر استفاده غیرقانونی از اسم و شماره کارت اعتباری و خدمات اجتماعی قربانی توسط هکرها، آن‌ها می‌توانند اهداف شوم‌تری را دنبال کنند.

اطلاعات مشتریان می‌تواند برای هکر راهی را باز کند که بتواند به بانک قربانی نیز حمله کند و با استفاده از اطلاع حساب قربانی به تمام اطلاع حسابها از طریق حفره‌ای وارد شود.

مهندس اجتماعی نیز راه دیگری برای غارت اطلاعات هویتی افراد است. این روش بسیار ساده است. از طرف هکر ایمیل خاصی با عنوان فرستنده ISP به کاربر فرستاده می‌شود و از کاربر می‌خواهد تا برای بالا بردن سطح نمایش سیستم کد خاص خود را بفرستد. هیچ کاربری حس نمی‌کند که چیزی غلط است. پس اطلاعات را می‌فرستد و هکر به راحتی می‌تواند به اطلاعات شما دستیابی پیدا کند. وقتی شما با یک هکر هویت مواجه می‌شوید همه چیز اینگونه تمام می‌شود: کارت اعتباری یان از بین محدود، تمام اطلاعات شما در دست شخص دیگری است و راه بلند قانون در جلدی شما قرار می‌گیرد تا حقتان را بگیرید. یکی از علل ایجاد دستگاه‌های جلوگیری کننده از ورود هکرها برای جلوگیری از اینگونه هک‌های هویت است.

### دزدان و راه زنان اطلاعات

این نوع دزدان به پایگاه داده‌های عظیم شرکتها حمله می‌کنند و جهت عملکرد آن‌ها برای اطلاع از چگونگی عملکرد شرکت‌ها هست. این اتفاق برای شرکت مایکروسافت نیز افتاد و این شرکت اعلام کرد که طی 20 روز قسمت عمده‌ای از اطلاعات مهم این شرکت مورد راه زنی قرار گرفته‌اند. آن‌ها به منبع کد برنامه سیستم عامل ویندوز و برنامه آفیس دست یافتند. شرکت مایکروسافت به جهت اطمینان حاصل کردن از آنکه که اصلی دست نخورده مانده باشد 2 هفته با تمام نیروکار کردند و در نهایت اطمینان حاصل نشد که کد دست نخورده است و کار درست انجام می‌شود. بعد از این اتفاق شرکت مایکروسافت خواستار پیگیری شدید توسط FBI شد که در نهایت ثمری گذاشت. هکرها از طریق سیستم خانگی یک کارمند وارد سیستم شدند و با فرستادن یک ویروس اسب تروآ به شبکه توانستند از «درپشتی» وارد شوند. بعد از آن آن‌ها با نرم‌افزاری قفل بعدی را باز کردند. وقتی این حمله مشخص شد که شناسه جدیدی در شبکه ایجاد شده و در سیستم کارکرد.

## **درک شیوه سیستم پیشگیری کننده امنیتی برنامه‌های کاربردی و تهدیدات آن**

حملات به برنامه‌های کاربردی به‌طور کلی بسیار سخت است و طبیعتاً دفاع در مقابل این حملات سخت‌تر. بسیاری از شرکت‌های کامپیوتری و کمپانی‌های بزرگ همچنان سعی و تلاش می‌کنند تا سیستم و برنامه‌های کاربردی خود را توسط برنامه‌های ویروس یاب، دیوار آتش‌ها و همچنین ترقی دادن و استفاده جدیدترین نوع برنامه‌های دفاعی، از دست هکرها محفوظ نگهدارند.

ولی حقیقت آن است که برنامه‌های کاربردی در سطح شبکه با داشتن این برنامه‌های حفاظتی از دسترسی هکرها در امان نیستند. یعنی تاکنون چنین برنامه امنی ساخته نشده است. حمله به برنامه‌های کاربردی انواع مختلفی دارد مثلاً نوعی از حمله از D Dos استفاده می‌کند یا یکی دیگر از ویروسهای مختلف.

هک کردن برنامه‌های کاربردی به هکر اجازه استفاده از اطلاعات سودمند بدست آمده را می‌دهد. چون برنامه‌های کاربردی تحت شبکه محل نگهداری مقادیر زیادی اطلاعات از جمله اطلاعات مهم و حیاتی و حساس همچون اطلاعات حساب مشتری شماره کارت اعتباری و دیگر اطلاعات مهم شخصی است به همین دلیل مورد تجاوز و تهدید هکرهای به اندیش قرا رمی گیرد. روش‌های متفاوت نگهداری از برنامه‌های کاربردی چیست؟ اخلال‌های پنهان، پارامترهای پنهان، برش ابتدایی، پر شدن و سرریز شدن با فر و شیرینی زهرآلود فقط چند نوع اولیه و ابتدایی برای مقابله است. ما در این پروژه‌ها موارد مطرح شده را به زبانهای مختلفشی گرا محاوره به زبان جاوا یا XML بیان می‌کنیم. همه این برنامه‌ها قابل برنامه ریزی به زبانهای دیگر نیز می‌باشند.

### اخلال‌های پنهان

در این روش هکر بادستکاری کردن اطلاعات و به روز کردن اطلاعات هب صورتی که به نفع خود باشد به عمل هک کردن دست می زند. بر فرض مثال هکری با تغییر دادن و دستکاری کردن قیمتی یا فیلدی در خصوصیات وسیله‌ای آن را به نفع خود خریداری می‌کند چیز قابل توجه این است که این کار می‌تواند توسط برنامه‌های کاربردی تحت HTML به سادگی انجام شود.

### پارامترهای جعلی و پنهان

این نوع از حمله کردن به‌صورت یک روش خاص برای دستیابی به اطلاعات مهم در داخل یک سیستم عمل می‌کند به‌طوری که با جعل یک آدرس می‌تواند به سیستم شما بدون داشتن رمز عبور یا نام کاربری وصل شود.

### برش ابتدایی

این روش که به‌طور مخفف CSS نیز نامیده می‌شود یک توانایی برای دستیابی برنامه‌های خطرساز و ویروس گونه به برنامه‌های کرابردی تحت شبکه شما در هنگام ایجاد شدن هست.

این برنامه‌ها به شکل یک برنامه قانونی حاوی اطلاعات بدون مشکل در می‌آیند (مانند یک دستور از طرف کاربر) و با این تغییر چهره زیرکانه سرویس‌دهنده به آن پاسخ داده و برنامه را اجرا می‌کند. این اجرا باعث ایجاد خرابی در سیستم یا برداستن اطلاعات می‌شود. هکرهای بداندیش از روش CSS برای ورود برنامه‌های مخرب خود به برنامه‌های تحت وب استفاده می‌کنند. قسمتی از مشکل به آن دلیل است که برنامه کاربردی تحت شبکه توانایی چک کردن کد داخل برنامه دانلود شده را ندارد وفقط به اجرای آن می‌پردازد (پس از تخمین غیرخطرناک بودن برنامه) بعد از پیاده شدن برنامه در سیستم برنامه توانایی انجام هر کار بداندیشانه مورد درخواست هکر را دارند از دزدیدن اطلاعات تا پاک کردن یا فرمت کردن دیسک سخت.

بهترین راه برای مقابله با این حمله‌ها به دست کاربر نهایی است. به این ترتیب که کاربر با از کارانداختن برنامه‌های نشان دهنده وب که برای بالا بردن سرعت اسکریپت ها را اجرا می‌کنند می‌تواند از ورود اطلاعات خطرناک جلوگیری کند. همچنین با دریافت اطلاعات از سایتهایی که قابل اطمینان هستند نیز می‌توان جلوی این نوع حمله‌ها را گرفت.

### پر شدن و سرریز شدن بافر

این نوع حمله از طریق ورود آز ادانه و پر شدن بافر برای اجرای یک برنامه کاربردی رخ می‌دهد. این اتفاق در زمان انتقال اطلاعات به داخل بافر رخ می‌دهد. این خطا همچنان ادامه می‌یابد، چون همه برنامه مشکل دارد هم بافر و همینطور این ورود و خروج ادامه پیدا می‌کند. این خرابی باعث می‌شود که برنامه‌های مختلف توسط هکر بتوانند وارد سیستم شده یا حتی هکر آن‌ها را مورد شنود قرار دهد. مثلاً اگر گیرنده از آدرسی استفاده کند که بیشتر از 256 کاراکتر داشته باشد، کاربر با مشکل سرریز بافر مواجه خواهد شد. البته اگر ایمیل بازنگردد مشکل حل می‌شود. در توضیح باید بگوئیم که ماکروسافت یک سرویس مجانی برای مبارزه با این نوع حمله در اختیار همگان گذاشت وقتی که این روش اکتبر 2000 فاش شد.

### شیرینی زهرآلود

وقتی هکری از شیرینی زهرآلود برای هک کردن استفاده می‌کند باید دسترسی مجاز به برنامه کاربردی تحت وب داشته باشد و این قدم اول است. هکربا سیستم آشنا است و به آن اشراف کامل دارد. هکر باید شیرینی زهرآلود را درسیستم خود داشته و آن را به برنامه کاربردی تحت وب ارسال کند.

چون برنامه کاربردی تغییری در سیستم را احساس نمی‌کند. پس در برابر آن کاری انجام نمی‌دهد و از آنجا که به بعد کار شیرینی زهرآلود آغاز می‌شود. بعد از آن برای مثال قیمتی در یک سایت اقتصادی یا یک برنامه کاربرد در یک سیستم اعتباری عوض می‌شود. با این روش هکر می‌تواند به راحتی از اطلاعات بدست آمده سوءاستفاده کند و آن را در جهت سود خود استفاده کند و با کارت کسی دیگر چیزی خریداری کند.

با این توضیحات باید خوانده محترم پروژه ما قانع شده باشد که حفاظت از سیستم برنامه‌های کاربردی، وب سایتها و اطلاعات بانک اطلاعاتی تحت وب بسیار حیاتی و مهم است و برای نیل به این اهداف کارهای مهمی باید صورت گیرد.

## **جلوگیری از هک شدن با روش فکر کردن مثل یک هکر**

با علم به سودمند بودن اینترنت هر روز ابزار ساخت برنامه‌های کاربردی تحت وب قوی‌تر می‌شوند و هر روز نیز امتحانهایی که برای تست امنیت داده‌ها برای برنامه‌های کاربردی به کارمی رود سخت‌تر می‌گردند. در مقیاس سیستم اینترنت در طول روز مقدار کمی معاملات مالی در شبکه اتفاق می افتد که جنبه‌ای سیستماتیک دارد به همین دلیل ایجاد امنیت برای مواردی چون انتخابات اینترنتی و کارهایی که به سطح بالای امنیت اطلاعاتی دارند مهم‌تر می‌نماید.

بهترین راه برای جلوگیری از هک شدن و برنامه ضدهک شدن ساختن فکر کردن مثل یک هکر است چندین بار به سایت خود حمله کنید و راههای معمول ورود هکرها را کنترل کنید و در طر فدگیر در برابر حمله دفاع کنید. کد برنامه خود را تست کنید در یک مرحله به امنیت سیستم خود حمله کنید تلاش کنید یا با بعضی راههای ممکن که همان حفره‌هایی هستند که شما در نظر نگرفتید وارد سیستم شوید.

هیچگاه نماد تضمین کیفیت (QA) کافی نیست، چرا که هر سیستم جدیدی می‌تواند از طرف هکری تهدید شود. آشنایی با زبانهای دیگر ایجاد برنامه‌های کاربردی، همچنین به مسیرهایی که شبکه و برنامه‌های کاربردی از خود دفاع می‌کنند. همه‌ای اینها فاکتورهای لازم برای حمله یک هکر به سایت هست در کل سه سطح برای تخمین زدن درجه امنیت هر سیستم کاربردی قابل بررسی است.

این سطح بندی به‌صورت زیر است:

### تیم توسعه دهنده

1- تیم باید بر سر مقاصد تعیین شده خاص امنیت و بر عکس آن خرابکاری بکوشد.

2- تیم باید بر سر زبان برنامه امنیتی به توافق برسد.

3- تیم می‌بایست در همان ابتدای ایجاد کد محل خاصی را برای برنامه امنیتی اولیه تعیین کند و آن را توسعه دهد.

4- کد آن چند بار تست شود و برای حمله به آن چیزهایی که هکرها می‌خواهند بدست آورند تلاش شود. باید دانست که هکرها متناوباً حمله می‌کنند و تا به مقاصدشان نرسند کنار نمی کشند، پس یک هکر وقتی از هک کردن دست بر می‌دارد که یا کارش با موفقیت انجام شده است یا اینکه متقاعد شود که هیچ راه ممکنی برای ورود به برنامه تحت شبکه‌ای شما وجود ندارد باید توجه داشت که اگر راهی برای ورود پیدا نکردید به این معنا نیست که سیستم امن است و این یعنی هنوز راهی برای ورود به برنامه کاربردی پیدا نکرده‌اید.

5- این بدان معنی نیست که با همکاری همکار شما، برنامه کاربردی شما امن می‌شود، بلکه احتمال خطای شما کمتر می‌شود.

6- کدهای مختلفی را به‌صورت منظم در داخل برنامه‌های کاربردی خود جای دهید تا ظرفیت جلوگیری از هک شدن را متوجه شوید.

7- از نسخه های اصلی کنترل نرم‌افزار استفاده کنید که در داخل سایتهای فروشنده معلوم و مشخص هستند.

8- از کدهای استاندارد و اصلی، تبعیت شود.

9- از مرورگرهای کد استفاده شود تا درهایی که در ابتدا بازمانده است را شناسایی شود.

### تیم کنترل کیفیت (QA)

1- تست به شیوه‌ای که نقاط بحرانی معلوم شوند (همچنین نقاط مرزی)

2- ایجاد بار و تست زیر بار اطلاعات زیاد و استفاده از ابزارهای چون Suiffer

3- حکمه های تعیین شده در برنامه را امتحان می‌کنند تا اتفاقات غیرقابل پیش بینی رویت شوند.

4- انجام سری تست‌های مختلف

5- انجام نفوذ در سطوح مختلف شبکه

6- استفاده کردن از برنامه‌های مرورگر برای پیدا کردن «درهای پشتی» برنامه اگر مجاز بود.

### تیم امنیت اطلاعات

1- امنیت اطلاعات از طریق امنیت موجود در شبکه و سطح کار شبکه (ازنظر وسعت و...) ایجاد می‌شود. به این معنی که این سطح از امنیت بوسیله همکاری برنامه‌ها با app های سطح بالا طراحی و اجرا می‌شوند.

2-ممارست بر سر اطلاع یافتن از جدیدترین انواع ویروسها، کرم‌ها و...

3- تحقیق و بررسی برای پیدا کردن برنامه‌های جدیدترین برای به مبارزه طلبیدن برنامه‌های مخرب

4- داشتن نقشه‌ای برای جلوگیری از حمله در هر محل از شبکه

5- اجرا کردن یک سری برنامه‌های امنیتی بر روی شبکه برای شناسایی تخریب گران جدید

6- اطمینان حاصل کردن از ارتقا یافتن ویروس یاب[[47]](#footnote-47) و محافظ سیستم عامل (OS)

7- ایجاد یک کد خاص عبور تا از سیستم فقط یک نفر مخصوص استفاده کند.

8- ایجاد دیوار آتش و برنامه‌های ضد نفوذگر در سطح برنامه.

9- شناخت کامل تمام برنامه‌های امنیتی جداگانه در سطح شبکه

با داشتن یک شبکه مجهز به ابزارهای امنیتی باید سه سطح مطروحه بسیار مطلوب با هم کار کنند، مثل یک ماشین روغن کاری شده. استفاده از یک سطح تعیین کننده سطح بالای امنیتی سیستم نمی‌باشد. باتجربه‌ای که هکرها دارند امکان حمله و پیدا کردن حفره و نفوذ به آن سوراخ نرم‌افزاری بسیار عادی به نظر می‌رسد که شما با جرای هر سه سطح جلوی این اتفاق را می‌گیرد. ]7[

# فصل چهارم

**درک رابطه خطرها با کد تلفن همراه**

## **مقدمه**

اینترنت چیزهایی بیشتر از داده‌ها را می‌تواند انتقال دهد. اینترنت می‌تواند برای فراهم کردن خیلی از سرویسها، برنامه‌های مخصوصی را انتقال دهد. اگر چه برنامه‌ها برای رسیدن به کاربر به یک مسیر ویژه نیاز دارند.

کد تلفن همراه کدی است که می‌تواند در سرتاسر شبکه حرکت کند و در ماشین مقصد بصورت یک کد اجرائی اجرا شود. مانند اسکریپها در داخل ایمیل و یا کدهایی که در صفحه اینترنت اجرا می‌شوند بنابراین کد تلفن همراه راهی مناسب برای برخی قطعه کدها هست که بر روی پلتفورم های گوناگون اجرا می‌شوند. البته این کدها برای توزیع برنامه‌های کاربردی در سر تا سر شبکه بسیار مناسب و عالی می‌باشند. اینترنت به کاربران اجازه دسترسی به هر نوع داده‌ای را می‌دهد در حالیکه قبل از آن اینچنین نبوده است. آن همچنین اجازه انجام فعالیتهای پرمخاطره را نیز برای کاربران خرابکار فراهم می‌کند کد تلفن همراه یک کد اجرائی هست که با کدهای HTML ادغام شده بر روی ماشین کاربر اجرا می‌شود. این فعل به امنیت این کدها از نگاه کاربران توجه دارد.

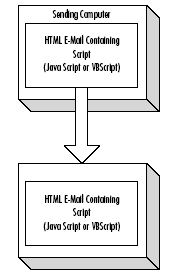
## **تشخیص ضربه حملات کد تلفن همراه**

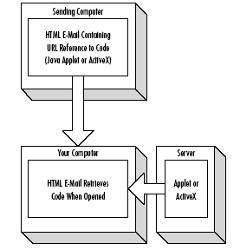
داده‌های HTML قدرت دستیابی به داده‌های روی سیستم را ندارند. اگر شما آن‌ها را با کد تلفن همراه آمیخته کنید عناصربسیار کوچکی برای ارسال بوجود می‌آیند که این عناصر می‌توانند بی صدا، آب زیر کاه بسیار خطرناک باشند. آن‌ها همچنین می‌توانند اطلاعات را از روی سیستم شما بازیابی کنند. البته با فایروال می‌توان تا حدود زیادی جلوی ورودی آن‌ها به سیستم را گرفت.

## **حملات Mail client**

با کد تلفن همراه‌ها مستندات HTML توانایی ورود به کامپیوتر شمارا بصورت ایمیل پیدا می‌کند و بدین صورت یک هکر می‌تواند کارهای خرابکارانة خود را انجام دهد. شما و یا شرکت شما می‌توانند اهداف این حملات خرابکارانه باشند.

گاهی اوقات این کد تلفن همراه‌ها غیر قابل کنترل هستند مخصوصاً زمانی که کاربر مبتدی باشد. دو راه برای کد تلفن همراه‌ها برای رسیدن به کامپیوتر وجود دارد، با این روش (روش اول): کد تلفن همراه‌ها بصورت مستقیم یا پیغامهای ایمیل ادغام می‌شوند همانند شکل (1-4) این شامل زبانهای اسکریپت مانند جاوا اسکریپت و VBscript هست. دومین راه برای کد تلفن همراه‌ها رسیدن به کامپیوترها توسط وب سرور (شکل 4-2) هست یک امیل با مراجعه به کد تلفن همراه موفق به ارسال می‌شود و خیلی از عکسها در HTML به فایلهای که در وب سرور مقیم هستند رجوع پیدا می‌کنند. زمانی که یک ایمیل باز می‌شود عملاً از سرور بازیابی می‌شود.

شکل (5-1)

****شکل (4-2)

## **ماکروها یا اسکریپتهای خرابکار**

شایداولین و مهمترین متعلقات مربوط به یک شرکت الغاء آن شرکت باشد مانند اسناد word و یا word perfect که شامل ماکروهای پرقدرتی هستند و می‌توانند دارای محتویات خطرناکی باشد به عنوان مثال ویروس ملیسا[[48]](#footnote-48) بود که مشکلات زیادی را برای مدیران شبکه بوجود آورده بود.

شناسایی فرم های مشترک کد تلفن همراه‌ها:

کد تلفن همراه به عنوان کدی برای حرکت در سر تا سر شبکه برای اجرای بر روی کامپیوترها تعریف می‌شود. چه بر روی مرورگرها و چه بر روی پیامهای ایمیل چهل نوع اساسی از کد تلفن همراه‌ها وجود دارد.

1. زبانهای ماکرو مانند (VBA)
2. اسکریپت‌های ادغام شدنی مانند جاوا اسکریپت
3. برنامه‌های کاربردی در ویندوز که همراه سیستم عامل است (Java Applets)
4. کنترل‌های اکتیو ایکس کد تلفن همراه‌ها بطریق متفاوتی ضمیمة ایمیل‌ها می‌شوند. آن‌ها معمولاً بصورت ساکت و آرام ضمیمة ایمیل‌ها می‌شوند. تا زمانی که کاربر بوسیله باز کردن آن‌ها و یا ذخیرة آن‌ها بر روی دیسک به آن‌ها رسیدگی کند. اگر آن‌ها از نوع پاینری ویا اسکریپت باشند تا زمانی که کاربر آن‌ها را اجرا نکنند فعال نمی‌شوند. فعالیت آن‌ها به هیچ چیز محدود نمی‌شود. آن‌ها می‌تواند از روی هارد شما بخوانند و بنویسند و حتی اطلاعات شمارا انتقال دهند.

اگر کد تلفن همراه به چیزی اجازة خوانده و نوشتن دهد امنیت به خطر می افتد. اگر چه مهندسان نرم‌افزار دوراندیشیهای لازم را برای این محدودیتها در نظر گرفته‌اند. البته به این طریق تا حدودی قدرت کد تلفن همراه کاهش می‌یابد. این محدودیتهای کد تلفن همراه تا حدودی و البته به زبانی است که آن‌ها را بوجود آورده است.

### زبانهای ماکرو (VBA)

نوع دیگری از کد تلفن همراه‌ها که بسیار خطرناکند از نوع‌های دیگری است که تا بحال شناخته‌ایم وجود دارد از آنجایی که این کدها بین مستندات حرکت می‌کند و این مستندات در سرتا سر شبکه وجود دارند به عنوان کد تلفن همراه شناخته می‌شوند. VBA به کاربران ماکروسافت آفیس[[49]](#footnote-49) اجازة هر گونه عملیاتی را بر روی مستندات می‌دهد. VBA اجازة هر گونه فعل و انفعال را به توابع کتابخانه‌ای و کنترلهای اکتیو ایکس می‌دهد. و بسیاری از برنامه‌ها مانند پاورپوینت, اکسل, ورد می‌توانند از VBA استفاده می‌کنند از آنجایی که آن یک زبان ماکرو قدرتمند محسوب می‌شود و به خوبی توسعه و پیشرفت یافته به همین خاطر دیگر سازندگان نیز این برنامه‌ها را به درستی پذیرفته‌اند.

### مشکلات امنیتی با VBA

ماکروسافت سازندگان VBA را بشدت مورد انتقاد قرار داد و بسیاری از کاربران VBA را سازندة ویروس[[50]](#footnote-50) نام نهاند. به نظر من باید قدرت بیشتری به کاربران برای جلوگیری از حرکت هکرها داده شد. مشکل اصلی در آفیس 97 اتفاق می افتد. مشکل ماکروهایی که چک نمی‌شوند این است که حاوی اسبهای تروجا[[51]](#footnote-51)ن هستند و از این بدتر شامل ویروس ماکرو می‌باشند. یک ماکرو ویروس کدی است که در داخل ماکروهایی که در درون مستندات هستند ذخیره می‌شد. مانند اسناد ورد و زمانی که باز می‌شود ماکرو ویروس اجرا شده و بر روری الگو عادی ذخیره می‌شود. با ارسال این اسناد آلوده شده توسط کاربر برای هر کاربر دیگر این ماکرو ویروس نیز منتقل شده و این آلودگی سر تاس سر شبکه مشهود خواهد شد.

## **ویروس ملیسا**

در مارچ سال 1999 جهان ویروس VBA رادید که چطور بصورت مخفیانه زمانی که یک کاربر یک سند جدید بوجود می‌آورد و توسط کاربر دیگر مورد استفاده قرار می‌گرفت در سر تا سر شبکه پخش می‌شد بنظر خیلی آسان می‌آمد تا بتوانند جلوی آن را بگیرند چرا که ملیسا خیلی آرام در شبکه حرکت می‌کرد و احتمال کلی می‌رود که قبل از آنکه بخواهد در کل شبکه منتشر شود شناخته شده بود. این ویروس خودش را با فایل Templete ادغام کرد. ملیسا توسط VBA در اسناد ورد بوجود آمده بود.

## **حمایت در برابری ویروسهای VBA**

کاربران برای آنکه بتوانند ویروسها را شناسایی کنند باید یک آنتی ویروس خریداری کرده و بر روی کامپیوترهای خودشان نصب کنند. ویروس یاب های مانند MCAfee و برنامه‌های کمکی Norton وجود دارند اگر چه هر کدام از آن‌ها به بهترین وجه ویروس ها را شناسایی کرده و کاربر را مطلع می‌کنند. اگر کاربران فکر می‌کند که اسناد حاوی ماکروهای مفید می‌باشند ممکن است بخواهند آن‌ها را باز کنند. مثلاً اگر آن‌ها یک نوعی را که مخصوص شرکت آن‌ها است را دریافت کنند. آن‌ها احتمالاً ماکروها را فعال می‌کنند ولی اگر ندانند که محتویات آن چیست ومنبع آن از کجاست آن‌ها ماکروها را غیر فعال می‌کنند. اگر یک ویروس ماکرو توسط ویروس یاب پیدا شود بصورت خیلی آسان کدهای آن برای کاربر رویت می‌شود.

در محصولات اکسس, آفیس 97/2000 هنوز قابلیت اطمینان بالایی وجود نداشت و یک دلیل جذب نیز برای آن وجود دارد چرا که اکسس برای نشان دادن فرمها و انجام عملیات برروی آن‌ها به VBA تکیه دارد اگر VBA غیرفعال شود اکسس کارایی چندانی نخواهد داشت. فرم‌ها در اکسس بطور مداوم مورد استفاده قرار می‌گیرند و کدهای VBA را تولید می‌کنند. سندهای اکسس مکان مناسبی برای ویروسهای ماکرو می‌باشند.

## **جاوا اسکریپت**

جاوا اسکریپت یک زبان بسیار سودمند هست که قدرت بالایی را به برنامه نویس برای تولید مستندات HTML می‌دهد. با این زبان برنامه نویس بر روی فیلدها عملیات گوناگونی را انجام دهد و یا تصاویر متحرک بوجود آورد و یا واکنشی را برای حرکت مأوس ایجاد کند. جاوا اسکریپت یک اسکریپت ادغام شدنی هست. یعنی محتوای آن با کدهای HTML به درستی پر شده این زبان اولین بار با نام Netscape Navigator در سال 1995 با نسخة 5/2 معرفی شد. همان طور که در بخش‌های بعدی خواهید دید برخی مشکلات از اپلیت های جاوا اجزاء اکتیو ایکس یا اسکریپت‌های سمت کاربر نظیرجاوا اسکریپت ناشی می‌شود همه این مشکلات روی یک کاربر تأثیر نمی‌گذارد و ممکن است که آن‌ها وسیله‌ای برای هجوم به سیستم و یا سایت شما قرار گیرد. نهایتاً یک راه برای جلوگیری از چنین مشکلاتی کنترل نمودن برنامه‌هایی است که روی سایت شما قابل دسترسی هست در مورد محتویات برنامه‌هایی که در دسترس قرار می‌دهید مراقب باشید.

### امنیت جاوا اسکریپت

جاوا اسکریپت برای اهداف صحیح و روشنی در صفحه وب بوجود آمده اگر کسی با جاوا اسکریپت ایمیل ارسال کند نمی‌تواند گیرنده را همانند outlook مورد حمله قرار دهد. جاوا اسکریپت بسیار قابل اطمینان هست البته در گذشته مشکلاتی برای پیاده سازی آن نت اسکیپ[[52]](#footnote-52) و ماکروسافت وجود داشته است. جاوا اسکریپت قادر است تا با افزونه‌ها فعل و انفعال انجام دهد. افزونه‌ها برنامه‌های کوچکی هستند مانند shock ware که عملیات مرورگرها را افزایش می‌دهند.]2[

## **جاوا اسکریپت و مشکلاتی که پدید می‌آورد**

طراحان وب برای صفحات خود اسکریپت‌ها و اپلیت ها یی را بکار می‌برند، عموماً اپلت های جاوا بطور دیجیتال امضاء می‌شوند یا دارای قالب مجزا می‌باشند. کلمه‌ها می‌توانند طوری یک اپلت را برای اجرا روی یک ماشین برنامه ریزی کنند که اطلاعات را بازیای کند، فایل‌ها را خراب کند و یا تغییر دهد. به یاد داشته باشید که یک اپلت برنامه‌ای است که توانایی این را دارد که روی سیستم شمافعالیت زیان باری را شکل دهد. همان طور که می دانید جاوا یک زبان برنامه نویسی هست که برای تهیه برنامه‌های کاربرای در اینترنت مورد استفاده قرار می‌گیرد.

قرار می‌گیرد. اپلت ها درون صفحات وب جاسازی شده هنگامی که یک کاربر آن‌ها را توسط مرورگر خود بار می ند اجرامی شوند. توسط برنامه نویسی مشابه اپلیت ها، جاوا خصوصیتی مربوط به امنیت را ارائه می‌کند. در خلال کامپایل کد موجود در آنرا به‌منظور خطایای چک می‌کند به این طریق جاوا ناحیه مشخص حافظه را دور از دسترس نگه می‌دارد. هنگامی که بارگذاری شد ماشین مجازی جاوا (JVM) یک مدیر امنیت درون ساز دارد که دسترسی با به حسب سیاستها کنترل می‌کند در ماشین مجازی جاوای نت اسکیپ یک مشکل رخ داده است و آن این است که تحت شرایط خاصی JVM کسی که بارگذای شده است را چک نمی‌کند. از آنجا که تمام کد چک نشده است در نتیجه کد قبل از تأیید نوع جاوا اجرا می‌شود. پس از زمان کوتاهی این مشکل که اینترنت اکسپلورر نیز مشاهده گردید. با توجه به این مشکلات شایع تصور کنید که آن‌ها برای سیستم کاربر تأثیر خواهد گذاشت نه خود سرور وب. همانند روش‌های دیگربرنامه نویسی اینترنت جاوا در سمت کاربر (به جای سروروب) هست. به هر حال اگر یک اپلت[[53]](#footnote-53) برای بهره برداری اطلاعات از یک ماشین کاربر طرحی شده باشد ممکن است کلمات عبور و نام کاربران به دست آورده شود و برای هک کردن سیستم و سایت شما بکار رود. همچنین اگر ماشین کاربر به هر نحوی توسط یک اپلت زیان آور خراب شود کاربر فقط این را می‌داند که بازدید از سایت شما او را دچار چنین مشکلی کرده است این موضوع به اعتبار سایت شما در اذهان عمومی و تصویری که از شرکت شما وجود دارد ضربه خواهد زد. همان طور که می دانیم اپلت هایی که توسط شرکت مایکروسافت ایجاد شده را اکتیو ایکس گویند که توسط یک تگ به نام <OBJECT> در اسناد HTML جاسازی می‌شود. اگر یک کاربر به سند HTML که حاوی کنترل اکتیو ایکس است دسترسی داشته باشد وجود یا عدم وجود آن بر روی کامپیوتر کاربر چک می‌شود. اگر وجود نداشته باشد کنترل اکتیو ایکس برداشت خواهد شد صفحة وب نمایش داده خواهد شد و کد اکتیو ایکس در حافظه بار و اجرا می‌شود.

کد شناسای [[54]](#footnote-54) که توسط شرکت مایکروسافت طراحی شده است به‌منظور تأیید یک کنترل اکتیو ایکس از طریق امضاء کد شده (امضاء دیجیتالی) به کار رفته است. هنگامی که کد شناسای استفاده می‌شود. اکتیو ایکس امضاء توسط شخص ثالثی تأیید شده است. با این کار اطمینان حاصل می‌شود که از زمان ایجاد تاکنون تغییر نکرده است.

جاوا اسکریپت با اکتیو ایکس و جاوا فرق دارد بدین ترتیب که در داخلیک برنامه کامپایل نمی‌شود. با این وجود جاوا اسکریپت دارای برخی تشابهات دستوری و کاربری با جاوا هست. وقتی که یک کاربر به سندی دست می‌یابد که حاوی جاوا اسکریپت است اجرای آن از طریق یک مفسر صورت می‌گیرد این کار کندتر از حالتی است که برنامه به زبانی کامپایل شده باشد که توسط ماشین قابل فهم باشد به همین علت جاوا اسکریپت کندتر از اپلت های جاوا هست.

اگر چه جاوا اسکریپت به علت اینکه یک زبان اسکریپت سازی هست با اکتیو ایکس، جاوا متفاوت است اما هنوز این امکان وجود دارد که یک هکر به‌منظور دستیابی به اطلاعاتی به مورد سیستم شما از یک اسریکپت استفاده کند یا با استفاده از کد به یک سایت یا کامپیوتر کاربر حمله کند.

## **مشکلات امنیتی**

حفره‌های جاوا اسکریپت چندان جدی نیستند. مدل انتزاعی برای جاوا اسکریپت همیشه امن است ولی در گذشته پیاده سازی آن چندان کارا نبود. اصلی‌ترین نقطة ضعف جاوا اسکریپت این بود که آن قادر به خواندن تمامی صفه ها وب بود که می‌تواند برای پایگاه وب مشکلاتی را بوجود آورد همانند portable office.com شخص می‌توانست برای شما ایمیل ارسال کند (با کدهای جاوااسکریپت) به محض آنکه شما ایمیل را خواندید آن می‌توانست خیلی کارهای دیگر را انجام دهد. مانند خواندن دیگر اطلاعات و ارسال ایمیل به شخص دیگر و جلوگیری از خواندن ایمیل توسط شما. این مشکل اولین بار در هات میل بوجودآمد که هات میل سعی کرد این تهدید را با خنثی کردن و با جاوااسکریپت به دیگر سایت‌ها ارسال کند.

## **حملات Web-Based E-mail**

بهترین خطرات جدی جاوااسکریپت از پایگاه وب بوجود آمد. زمانی که کاربران Web-based email را باز می‌کند بطور ذاتی این اجازه را به کدهای جاوا اسکریپت می‌دهد تا مسئولیت هر آنچه صفحه نمایش ظاهر می‌شود را بر عهده بگیرد

## **مهندسی اجتماعی Social Engineering**

همانطور که قبلاً هم اشاره شده مهندسی اجتماعی یکی دیگر از تاکتیک‌هایی هست که یک هکر از آن برای دستبرد زدن به اطلاعات دیگران مانند پسوردشان استفاده می‌کند. این تهدید برای خنثی کردن توسط یکی از نقطه نظرهای تخصصی بسیار کار مشکلی هست. هدف هکر در این مورد کسب اطمینان طرف مقابل هست هکر معمولاً وانمود می‌کند که متعلق به یک شرکت بزرگ می بشاد آن شخص به بازبینی و رسیدگی پسورد نیاز دارد. نحوة دیگر آن کسب اطمینان کاربر برای وانمود کردن به اینکه پسورد کاربر برای آینده نیاز هست.

## **پایین آوردن خطرات امنیتی Java script**

پیشگیری‌های که یک مدیر برای حمایت از کاربرانش در وهلة اول انجام خواهد داد نصب آخرین نسخة یک ویروس یاب بر روی کامپیوترهایشان هست. چیزی که ما به این بخش به آن اشاره خواهیم کرد. بیشتر حفره‌هایی است که رو جاوا اسکریپت به زبان پیاده سازی آن وابسته است. اگر کاربران از پایگاههای وب استفاده می‌کند. مدیر اطمینان خواهد داشت که کاربران سرویس را که سازمان امنیتی را فیلتر می‌کند مورد پذیرش قرار می‌دهند. نت اسکیپ نیز به کاربران اجازه می‌دهد که بتواند جاوا اسکریپت را برای مرورگر و یا برای ایمیل‌هایشان غیرفعال کنند.

## **VBScript**

Microsoft VBScript یکی دیگر از زبانهای ادغام شدنی هست که می‌توان از آن برای مستندات HTML استفاده کرد. VBScript کوتاه شده برای Visual Basic for scripting Edition و به نظر می‌رسد بسیارشبیه به زبان Visual Basic باشد مانند جاوا اسکریپت که شباهتهای زیادی به زبان جاوا دارد. تفاوت اصلی در VBScript این است که آن یک اثر متقابل با کنترلهای اکتیو ایکس دارد که کاربران آن را نصب می‌کنند.

VBScript فقط با Internet Explorer و outlook کار می‌کند بنابراین آن هم مانند جاوا اسکریپت یک وجهه عمومی و مردم پسند در میان کاربران دارد.

### امنیت در VBScript

VBScript توسط شرکت مکروسافت برای امن کردن مرورگر و مستندات HTML طراحی شد. از زمانی که طراحان اینگونه برنامه‌ها بطور صریح زبانهای اسکریپت داروی برنامه‌هایشان اجرا کردند دیگر با مشکلی خاص مواجه نشده‌اند. با VBScript تمامی خطوط بالقوه از روی زبان حذف خواهد شد. لیستی از کارهایی که توسط عملیاتهای Visual Basic انجام می‌شود که شما نمی‌توانید آن‌ها را در VBScript پیدا کنید شامل:

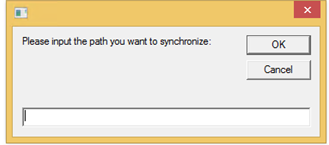
1. فایل ورودی / خروجی [[55]](#footnote-55)
2. تبادل اطلاعات پویا[[56]](#footnote-56)
3. نمونه شی[[57]](#footnote-57)
4. دسترسی مستقیم پایگاه[[58]](#footnote-58)
5. اجرای کد دی ال ال[[59]](#footnote-59)

VBScript فقط یکبار و آن هم زمانی که شما یک ایمیل و یا outlook Express را بازمی کنید اجرا می‌شود. VBScript بطور اصولی دسترسی به داده‌ها را در مستندات HTML محدود می‌کند.

### مشکلات امنیت در VBScript

نقاط ضعفی در VBScript وجود دارد که باعث شده ماکروسافت اصلاحاتی را در آن بوجود آورد مایکروسافت خواستار آن شد که جاوااسکریپت با کنترهالی اکتیو ایکس اثر متقابل داشته باشد. البته مشابه این تغییرات باعث ناامن شدن آن نیز بشود. شما ممکن است فکر کنید حذف خطرناک دستورات Visual Basic مشکلات امنیتی را از بین می‌برد.

چیزهای زیادی وجود دارد که یک هکر از آن می‌تواند استفاده تا زمانی که او به استفاده از کنترلهای اکتیو ایکس محدود نباشد. او می‌تواند راههای زیادی پیدا کند. خوشبختانه آخرین نسخة Outlook Express کنترل‌های امن را از ناامن تشخیص می‌دهد. همان طوری که قبلاً در بحث مهندسی اجتماعی گفته شد VBScript نیز می‌تواند به عنوان یکی دیگر از راهها به عنوان مهندسی اجتماعی برای یک هکر مورد استفاده قرا گیرد آن می‌تواند به‌عنوان یک dialog box برای درخواست اطلاعات کاربر بر روی صفحه نمایش نشان داده شود. شکل (4-3) نمونه‌ای از خطراتی را که با مهندسی اجتماعی بوجود می‌آید را نشان می‌دهد.



شکل (4-3)

### پیشگیری امنیتی VBScript

برای کاربران مشکل خواهد بود که بدانند چه کنترلهایی بر روی سیستمشان توسط حملات VBScript آسیب پذیر خواهد بود. ماکروسافت هم راه مناسبی برای حفاظت کامل از track های کنترل‌های اکتیو ایکس بدست نیاورده یک راه درست این است که اول کاربران باید نسخه‌های کنترلهای خود را بروز رسانی کنند. بروز رسانی بهترین انتخاب برای کاربران است. نسخه‌های آینده اینترنت اکسپلورر، Outlook ماکروسافت به کاربران اجازه می‌دهند که تنظیمات را خودشان انجام دهند و گزینه‌هایی را در اختیار کاربران قرار می‌دهد که به زبانهای اسکریپت اجازه دسترسی به کنترلهای اکتیو ایکس را ندهند.

## **برنامه‌های کاربردی جاوا**

برنامه‌های جاوا نمی‌توانند مقرر داده‌های را روی صفحة HTML ببینند. چرا که آن‌ها بوسیله Sandbox در ارتباط با کارهایی که می‌خواهند انجام دهند محدود می‌شوند. این بدان معنی است که آن‌ها نمی‌توانند در مورد هر چیزی بر روی مستندات HTML اطلاعاتی بدست آورند. تمام کدهای جاوا بر روی یک ماشین مجازی اجرا می‌شوند. آن یک برنامة اجرائی هست که byte-code ها را ترجمه می‌کند. زمانی که برنامه نویس از کامپایلر جاوا (یا Javac) برای کامپایل کردن که منبع استفاده کند کامپایلر Byte-code را بوجود می‌آورد. در یک مقایسه کامپایلر که ماشین را که بر روی سیستم عامل اجرا می‌شود را بوجود می‌آورد ولی byte – code فقط می واند توسط ماشین مجازی ترجمه شود ذاتاً ماشین مجازی فقط یک برنامه اجرایی است که byte-code را ترجمه و به آن اجازه اجرا روی یک رایانه را می‌دهد زمانی که یک کاربر توسط یک اپلت صفحه‌ای را جستجو می‌کند جستجوگر ماشین مجازی نیز شروع بکار می‌کند. نمونه سازهای زیادی وجود دارد که می‌تواند بر روی دیگر سیستم‌ها مانند لینوکس, مکینتاش اجرا شوند. همان کدی که برای ماشین ویندوز فعال می‌شود می‌تواند به همان جذبی نیز بر روی ماشین مکینتاش نیز فعال شود. اپلت ها بطور طبیعی نمی‌توانند داده‌ها را از روی گردانندة سخت کامپیوتر بخوانند یا بنویسند. این بدان معنی است که کاربران بطور کامل در مقابل به خطر افتادن داده‌هایشان ناشی از اجرای اپلتها بر روی سیستمهایشان در امان خواهند بود.

### مشکلات امنیتی با جاوا

بطور کلی برنامة جاوا نمی‌تواند کارهای جاسوسی یا آسیب‌های جدی را به سیستمها وارد کند روزنه‌های زیادی در پیاده سازی ماشین مجازی جاوا (JVM) بوسیلة ماکروسافت و نت اسکیپ وجود دارد اما بعد از تکمیل شدن محصولات آن‌ها بسیار قدرتمند شدند. یک اپلت ممکن است نتواند با دیگر سرورها بر روی اینترنت ارتباط برقرار کند.

## **نگاهی به کنترلهای اکتیو ایکس**

پاسخ ماکروسافت به برنامه‌های جاوا، اکتیو ایکس است. کنترل‌های از دیدگاه کاربران می‌تواند مشابه با برنامه‌های جاوا باشد. اما از لحاظ مدل حفاظتی کاملاً متفاوت است و همچنین جاوا می‌تواند بر روی انواع سیستم عامل مانند ویندوز، لینوکس و مکینتاش اجرا شود. در حالی که اجرای اکتیو ایکس فقط بر روی سیستم عامل اجرا می‌شود که بر روی آن برنامه ذخیره شده باشد بدین معنی که آن‌ها تعهد دارند که فقط در زیرساختهای برنامه‌های ویندوز از شرکت ماکروسافت اجرا شوند. از آنجایی که اکتیو ایکس عمومیت چندانی نزد برنامه نویسان ندارد نمی‌تواند بر روی طیف وسیعی از سیستمها که با اینترنت در ارتباط نه کار کند.

در آغاز اکتیو ایکس فقط در اینترنت اکسپلورر و Outlook کار می‌کرد. آن همچنان نیز با Eudora نیز کار می‌کرد.

برنامه‌های جاوا بر روی سیستم کاربر نصب نمی‌شوند و زمانی که صفحة وب را ترک می‌کند نیز یکباره ناپدید می‌شوند (البته ممکن است برای مدت محدودی در Cash باقی بمانند).

اجرای اکتیو ایکس می‌تواند بطور موقت بر روی سیستم نصب شوند و خیلی اوقات بطور همیشگی یکی از اهداف اجزای اکتیو ایکس برای اجرای بازیها بوسیلة Macromedia هست و بر روی سیستم کاربر نصب می‌شوند مگر تا زمانی که کاربر آن‌ها را حذف کند.

### مشکلات امنیتی با اکتیو ایکس

مدل امنیت اکتیو ایکس تکیه دارد به کاربران با یک تصمیم درست در ارتباط با اینکه کدام برنامه‌ها مورد قبول و کدام برنامه رد می‌شود. برنامه‌های اکتیو ایکس یک عامل بالقوه دارند که می‌توانند مضر باشند اگر مدل امنیتی آن‌ها واضح نباشد. شاید بزرگترین ضعف امنیت اکتیو ایکس این است که هر کنترلی می‌تواند بطور ماهرانه بر روی کامپیوتر فعالیت کند و کاربر متوجه آن نمی‌شود و بطور بی صدا اطلاعات شما از کامپیوتر به سرور و اینترنت منتقل می‌شود.

### اشتباه در انتقال و جایگیری کاراکترها

انواعی از مشکلات وجوددارند که buffer overrun نامیده می‌شوند که به نظر می‌آید خیلی از کنترلهای اکتیو ایکس را آزار می‌دهند. نتیجةی نهایی خطاهای buffer overrun این است که آن بطور آزادانه به کدها اجازه می‌دهد که بر روی کامپیوتر کاربر اجرا شوند. و کاربر ممکن است فکر کند که با استفاده از کدهای کمپانیهای معروفی همچون آدوب و ماکروسافت در امان خواهد بود اما کنترلهایی همچون Acrobat Reader 4.0 دارای این خطاها هستد.

معرفی کنترلهای گیچ کننده‌ای که بطور معمول در Interner Explorer 4.x نصب می‌شوند. می‌تواند برای کاربران بسیار مفید باشد چرا که آن‌ها بطور مستقیم نمی‌تواند به هارددیسک کاربر دسترسی داشته باشند. خطاهای Buffer overrun بطور سهوی اجازة دسترسی به هارددیسک را می‌دهند که بدین صورت نمی‌تواند امن باشند.

### غیر فعال کردن کنترلهای اکتیو ایکس

ویندوز به کنترل اکتیو ایکس اجازه می‌دهد که در زیر ساخت Internet Exploter و Outlook بطور کامل غیر فعال باشد. Killbit می‌تواند فعال شود در ریجیستری ویندوز به این دلیل که کنترل اکتیو ایکس فعال نیست کاربران بیاد CLSID را که به کنترل اکتیو ایکس مربوط می‌شود رادر ریجستری پیدا کنند.

به عقیدة ماکروسافت تصمیم گرفتن اینکه کدام CLSID مربوط می‌شود به کنترل اکتیو ایکس ی که شما می‌خواهید آن را غیرفعال کنید شما ابتدا باید همة کنترل‌های اکتیو ایکس را حذف کنید سپس کنترلی را که می‌خواهید غیرفعال کنید را نصب کنید و سپس "Kill bit" را به Clsid آن اضافه کنید.

## **متعلقات ایمیل**

در ویندوز فایلهای اجرایی متعددی وجود دارد مانند فایلهای باینری قابل اجرا (.exe,.com) فایهای دسته‌ای (.bat) و فایلهای VBScript (.vbs) و فایلهای (.jar) JAR اگر شما یکی از این فایلها را دریافت کنید سریعاً پیامی به عنوان اخطار برای باز کردن و یا ذخیره کردن آن برای شما ظاهر می‌شود. معمولاً شما آنرا باز نمی‌کنید مگر اینکه مطمئن باشید از طرف شخص قابل اطمینانی دریافت کرده باشید.

### حمایت از سیستم شما در مقابل با حملات کد تلفن همراه

دو دیدگاه برای مقابله باتهدیدات امنیتی وجود دارد. اول اینکه از یک تکنیک و دانش خاص برای حمایت از سیستم شما استفاده شود و یا اگر شما نخواهید که خود را برای آموزش این تکنیکها به دردسر بیاندازید می‌توانید از یکی از برنامه‌های کاربردی که بصورت اتوماتیک این امنیت را برای سیستم شما فراهم می‌کند استفاده کنید. این دومین روش هست.

## **برنامه‌های امنیتی**

در حال حاضر یک صنعت برای بوجود آوردن برنامه‌های مبارزه با تهدیدات امنیتی وجود دارد. اگر افراد با انواع ویروسها آشنا هستد. ابزار معمول برای کنترلهای ریجستر regsvr32 هست. این ابزار دارای خط فرمانی است که بسیار محدود است و اطلاعات زیادی دربارة اکتیو ایکس روی سیستم شما به وجود نمی‌آورد.

### کشف کننده‌های حفره‌ها

چندین ویروس یاب در بازار وجود دارند مانند MCAfee ولی شما باید هزینه‌ای برای آن بطور سالیانه بپردازید یک راه حل آزاد به نام BO2K وجود دارد که توسط یک کمپانی سازنده در استرالیا بوجود آمده. BO2K کامپیوتر شمارا اسکن کرده و لیست سرورهای BO2K را نیز پرورش می‌دهد آن همچنین فایلهای افزونه را بخوبی کشف و پیدا می‌کند. می‌توان فایلی را انتخاب و بوسیلة آن اطلاعاتی را بدست آورد.

اغلب هکرها به IP سیستم شما نیازمندهستند. این امکان وجود دارد یک افزونه برای مرور که بطور معمول یک پیغام ایمیل برای هکر با آدرس IP سیستم شما ارسال می‌کند شما می‌توانید عملاً فایل exe مرور را با Ultra Edit باز کنید و آدرس ایمیل هکر را دید.

اگر یک هکر در کارش وارد باشد او ممکن است از مروری ایمیل بدون نام استفاده کنید. در این مورد او برای ردیابی بسیار مشکل و سخت خواهد بود.

### نرم‌افزار فایروال

یکی از اصلی‌ترین مزایای نرم‌افزار فایروال این است که نرم‌افزارهای هک نمی‌توانند به راحتی به فایروال رخنه کنند. فایروال به پورتهای سیستم شما اجازه بلوکه شدن در اینترنت را می‌دهد. Mcafee یک فایروال شخصی را برای کاربران بطور اختصاصی بوجود می‌آورد. با این نرم‌افزار شما می‌توانید تمام برنامه‌ها، پروتکل‌ها و سرویس‌ها را فیلتر کنید. شما همچنین می‌توانید تمام ارتباطات شبکه را مونیتور کنید. اگر برنامه‌ای بخوبی به اینترنت متصل شود شما سریعاً متوجه می‌شوید و می‌توانید اجازه و یا عدم ارتباط آن را صادر کنید.

# فصل پنجم

**ایمن کردن کدهای جاوا**

## **مقدمه**

ایمن نمودن برنامه‌ها و یا سیستم شما مهمتر از طرح ریزی و اجرای یک معماری شبکه ایمن هست. اما قابل توجه ترین قسمتی که اغلب مورد هجوم قرار می‌گیرد، سرور سایت است در حقیقت در طی چند سال گذشته، هک کردن وب، عامل مشترک برای محو و بایگانی شدن برخی سایت‌ها شده است. تهاجمات «برابر سرورهای وب بسیار عادی است و در بسیاری از حالات با ناچیزترین حملات به مخاطره می‌افتد. انتخاب و نصب مناسب نرم‌افزار سرور وب و به دنبال آن به کارگیری تکنیک‌های استحکام آن، می‌بایست در نظر گرفته شود. این فصل، اطلاعات منحصر به فردی در مورد روش‌های امنیت ارائه می‌دهد. در ضمن بعد از طراحی و راه اندازی باید از اسکریتپها و اپلت های ایمن استفاده شود. این عمل برنامه نویسی روال‌های[[60]](#footnote-60) سالم و تحلیل اپلت ها و اسکریپتهای نوشته شده توسط دیگران برای اطمینان از اینکه امنیت را به خطر نخواهد انداخت. اگر در مورد توانایی‌ها و انجام برخی کارهای به خصوص که پروژه ارا با موفقیت روبرو می‌کند اطمینان وجود ندارد، آنگاه بایستی برای انجام کار یک قرارداد خارجی[[61]](#footnote-61) بسته شود. قرارداد خارجی یک قرارداد با حرفه‌ای‌های خارج از شرکت هست تا آن‌ها امنیت را به درستی تأمین نمایند.

## **جلوگیری از مشکلات ناشی از جاوا، جاوا اسکرپت و اکتیو ایکس**

جلوگیری از مشکلات ناشی از اسکریپت‌ها، اپلت ها و اجزا دیگر که در سایت لحاظ شده غیر ممکن نیست، چنانچه قبل از پیش بینی ها و احتیاط‌های لازم انجام شده باشد ابتداء اجزایی را که به‌طور کامل دانش یا اطمینان وجود ندارد لحاظ نشود، اگر اطمینان وجود ندارد که یک اسکرپیت ویژه موجود در یک خط برنامه چه کاری انجام می‌دهد آنرا به یک صفحه اضافه نکنید می‌بایست اپلت ها و اجزاء اکتیو ایکسی به کار برده شود، که کد مبدأ آن در دسترس هست اگر اپلت یا جزء ویژه‌ای را به کار برده شود، اما کد مبدأ آن موجود نباشد اطمینان حاصل شود که توسط منبع معتبری ایجاد شده به عنوان مثال CD های قابل ضبطی ((D-R ها را پیدا که حاوی اجزاء اسکریپت‌ها و اپلت های گوناگون هست به‌منظور اطمینان از نبود هیچ گونه کاستی و عیب در کدها باید آن‌ها چک شود، روش متعارف دیگر این است که صفحه و اجزاء را بدون این که پیوندی به صفحات دیگر داشته باشد بارگذاری شود، این کار باعث می‌شود که کاربران به صفحه‌ای که از آن آگاهی و اطلاع ندارند دسترسی نداشته باشند. روش دیگر استفاده از سرور تست هست، سرور تست کامیوتری است که دقیقاً شبیه به سرور وب پیکربندی شده اما جدا از شبکه قرار دارد توسط پک سرور تست اگر سایت دچار آسیب شود تأثیری روی سایت واقعی نخواهد گذاشت پس عاقلانه است که دسترسی به یک سایت و مشاهده اپلت، اجزاء یا اسکریپت از طریق شناسه کاربر صورت گیرد. اگر همه کاربران سایت را مشاهده نمایند از شناسه کاربر بی نام استفاده شود این کار به‌طور موثری فرد را قادر می‌سازد تا مشکلات را تست نمایید، یک مشکل متداول این است که هکرها از طریق برنامه‌ها و اسکریپت‌هایی که کاربر به آن‌ها اعتماد دارد وارد شوند استفاده از یک کتاب همان برای اجرای یک دستور SSI که احتمال دارد به سایت آسیب برساند اشاره شد با وجود این دیده می شود که برنامه‌های CGI که به زبان Perl نوشته شده می‌تواند به‌منظور اجرای فایل‌های دسته‌ای[[62]](#footnote-62) به کار برده شود زبان‌های اسکریپت سازی می‌تواند برای اجرای فانکنشهای پوسته‌ای[[63]](#footnote-63) به کار رود توسط دستور Cmd.exe که یک اسکریت معتبر هست می‌توانبرنامه‌های دیگری را در ویندوز NT و 2000 اجرا کرد.

علاوه بر ورود کاربر، نیاز خواهید داشت که به برنامه‌ها و اسکریپت‌هایی که ورودی‌ها را از یک کاربر ارسال می‌شود اعتماد نکنید ابزاری مانند Telnet یا برنامه‌های دیگری که بر روی اینترنت موجودی باشند برای شبیه سازی درخواست‌های مرورگر وب به کار می‌رود اگر به ورودی اعتماد شود یک هکر می‌تواند از طریق یک اپلت یا اکتیو ایکس دستورات گوناگونی را به سرور ارسال نماید ممکن است در صفحات وب اطلاعات مهمی یافت شود از آنجا که اسکریپت‌ها می‌تواند به‌طور مستقیم در صفحات جا باز می‌شود توسط مشاهده کد مبدأ HTML می‌توان آن را ملاحظه کرد بیشتر مرورگرهای وب این قابلیت را دارند که به‌منظور آشکار کردن اطلاعات که نمی‌خواهید در دسترس عموم قرار گیرد به کار می‌رود با ملاحظه کد موجود در سند HTML حتی می‌توانید نام کاربران و کلمات عبور را بیابید امکان دارد که اسکریپت‌های درون یک صفحه وب جهت ارسال نام کاربران و کلمات عبور به بانگ اطلاعاتی Access یا SQL به کار برده شود ویندوز NT به چنین اسکریپت‌هایی که شامل نام کاربران و کلمات عبور است جهت ارتباط به این پایگاههای اطلاعاتی نیاز دارد.

برای محافظت خود می‌بایست مطمئن شوید که مجوزها به درستی تنظیم شده و نیز روش‌های دیگر امنیت که از طریق سیستم عاملی که سرور وب روی آن نصب‌شده است قابل دسترسی است به کار برده شده برای مثال سیستم فایل NTFS بر روی ویندوز NT و 2000 فهرست‌های کنترل دسترسی ACL ها را پشتیبانی می‌کنند که می‌تواند به‌منظور کنترل کسی که قادر به اجرای یک اسکریپت است پیکربندی شود، با کنترل دسترسی به صفحاتی که از اسکریپت‌ها استفاده می‌شود بهتر می‌توان خود را در مقابل دسترسی هکرها به این اطلاعات محافظت کرد. به علت احتمال آسیب رسانی اپلت جاوا، جاوا اسکریپت یا اکتیو ایکس به یک شبکه به‌صورت تهدید امنیت یا هجوم به ماشین‌ها بسیاری از شرکت‌ها اپلت ها را فیلتر می‌کنند، فیلتر نمودن اپلت ها، اسکرپیت ها و اکتیو ایکس می‌تواند از طریق پیکربندی دیوار آتش صورت گیرد لذا آن‌ها از یک سند HTML حذف می‌گردند با حذف این موارد از آن چه که نمایش می‌یابد یک صفحه متناوب با آن چه که نویسنده قصد داشته است نمایش می‌یابد. اما در عوض اطلاعاتی که از طریق دیوار آتش عبور داده می‌شود ایمن هستند، در سمت کاربر بسیاری از مرورگرها به‌منظور فیلتر نمودن محتویات می‌توانند پیکربندی شوند یا تغییر تنظیمات یک مرورگر وب از بار شدن چنین برنامه‌های در حافظه کامیوتر کاربر جلوگیری می‌شود کاربر از طریق شبکه شما به اینترنت متصل و محتویات HTML مشاهده می‌شود. اگرچه چاوا اسکریت ها برنامه‌های کامپایل شده‌ای نیستند آن‌ها نیز می‌توانند برای هجوم به کامپیوتر کاربر مورد استفاده قرار گیرند جاوا اسکرپیت کارآمدی مشابه Java را دارد می‌تواند برای دستیابی به اطلاعاتی یا شکل دادن فعالیت‌های ناخواسته روی کامیوتر کاربر برده شود به این دلیل باید مراقب استفاده از اسکرپیت ها در سایت بود.

## **برنامه نویسی اسکریپت‌های ایمن**

اسکریپت‌ها و برنامه‌هایی را دیدیم که در سمت کاربر و روی ماشین کاربر اجرا می‌شوند اسکریپت‌ها و برنامه‌هایی که در سمت سرور و روی سرور وب اجرا می‌شوند به جای این که روی کامپیوتری برای مرور سایت شما استفاده شده برنامه‌ها و اسکریپت‌های سمت سرور عملیات گوناگونی نظیر کار با بانک‌های اطلاعاتی جستجوی سایت بر طبق کلید واژه‌های واردشده و ارائه روش‌های دیگر مبادله اطلاعات بین کاربران را انجام می‌دهند. یک مزیت اسکریت های سمت سرور این است که هر گونه کد مبدأیی از دیدگاه کاربر مخفی می‌ماند در مورد جاوا اسکریت هر گونه اسکریپتی توسط مشاهده که مبدأ و از طریق مرورگر قابل ملاحظه است اما این حالت برای برخی اسکریپت‌ها مصداق ندارد اما اسکریت های سمت ممکن است به‌منظور دسترسی به اطلاعات محرمانه به کار برده شود آخرین کاری که باید انجام داد که چگونه ممکن است اطلاعات موجود در پایگاههای اطلاعاتی مورد دسترسی قرار گیرند یک CGI پیوندهایی بین برنامه‌های کاربردی اینترنت و سرور وب برقرار می‌سازد به عبارت دیگر کاربران از طریق وب می‌توانند به برنامه‌ها دسترسی داشته باشند هنگامی که یک کاربر اسکرپیت یا برنامه CGI را درخواست می‌کند پردازش توسط مرور او آغاز می‌شود درخواست پردازش فرم به سرور وب می‌رسد و اسکرپیت یا برنامه را روی سرور اجرا می‌کند پس از آنکه برنامه ورودی را پردازش نمود سرور وب خروجی اسکریپت یا برنامه را به مرورگر ارسال می‌کند. PERL زبان دیگری برای اسکریپت سازی است که به‌منظور اجرای دستورات و فانکشن های مختلف از مفسر استفاده می‌کند نگارش این زبان شبیه به زبان برنامه نویسی C هست PERL زبان شناخته شده‌ای برای برنامه‌های کاربردی مبتنی بر وب است که به‌طور وسیعی پشتیبانی شده سرور وب آپاچی مثال خوبی از چنین پشتیبانی هست آپاچی دارای افزونه‌هایی است که PERI آن را به نام ASP ارائه نموده ASP اسناد HTML با جاسازی اسکریپت‌ها در آن‌ها هست این اسکرپیت ها می‌توانند به زبان‌های مختلفی نوشته شوند که شامل VB Script، جاوا اسکریپت و نیز شاید شامل دستورات برنامه Active Dataobjact, ADO استفاده گردد متأسفانه استفاده از ASP باعث مشکلاتی نظیر آن چه در اسکریپت سازی در سمت کاربر دیدیم می‌شود جاسازی اسکریپت‌ها در داخل صفحات وب به کاربران بداندیش و مضر اجازه می‌دهد تا ASP را ببیند، نقطه مشترک تمامی این روش‌ها این است که اسکریپت‌ها و برنامه‌ها روی سرور اجرا می‌شوند تهاجمات غالباً به جای آن که روی ماشین کاربری که یک برنامه را استفاده کرده تأثیر بگذارد روی سرور تأثیر خواهد گذاشت کاستی‌ها و شکاف‌ها باعث فاش شدن اسکریپت‌ها یا برنامه و در نتیجه دسترسی به اطلاعات خصوصی یا آسیب به سرور می‌شود تست و بررسی برنامه‌ها قبل از به کارگیری آن‌ها بسیار مهم است با انجام این کار تعدادی از آسیب پذیرها و اشکالات را می‌توان کشف نمود نظیر سرریزهای بافر که در صورت در دسترس بودن یک کد در روی سرور شما مشاهده نخواهد شد برای انجام تست مهم‌ترین کار استفاده از یک آزمایشی هست این سرور بایستی دقیقاً همان پیکربندی‌ها و برنامه‌های کاربردی سرور اصلی را داشته باشد.

طراحی سایت ایمن موارد گوناگونی را در بر می‌گیرد که با انتخاب سرور وب آغاز می‌گردد این کار به طرح ریزی دقیق و صحیح نیاز دارد زمان معقولی را برای تکمیل در نظر باید گرفت طوری که به امنیت آن هجوم نشده و به خطر نیفتد سرور وب از طریق شبکه داخلی دروازه‌ای را به اینترنت باز می‌کند انتخاب سرور وب به نیازهای شرکت بستگی دارد و سپس این نیازها با قابلیت‌ها و توانمندیهای سرور وب مقایسه می‌گردد قابلیت‌های ارائه شده توسط سرور وب به‌منظور استفاده در سایت تجارت الکترونیکی با نیازهای امنیتی و نیازهای تجاری هم خوانی داشته باشد بازنگری دستگاه‌های عامل، دیوارهای آتش و نرم‌افزارهای دیگری که فواید موجود در سرور وب را افزایش می‌دهد امری لازم است. هزینه یک سرور توانایی تهیه و توسعه و میزان برآورد کردن نیازها می‌بایست مدنظر قرار گیرد. اولین عامل انتخاب سرور وب می‌بایست قابلیت‌های امنیت ارائه شده توسط آن و هم چنین سیستم عاملی که سرور وب روی آن نصب می‌شود باشد. پس از نصب سرور وب می‌بایست فرایند پیکربندی و ایجاد المان‌هایی که سایت را بی همتا و ایمن می‌سازد شروع شود قویترین سیستم فایل انتخاب و کمترین مجوزهایی که کاربران برای مشاهده صفحات وب و دسترسی به اطلاعات نیاز دارند به آن‌ها داده شود اسکرپیت هایی که در سمت کاربر و سرور انتخاب خواهند شد را تعیین کرده و مطمئن شوید که از آن‌ها برای هجوم به سایت استفاده نشود جهت دسترسی از طریق سایت یا برداشت از اینترنت توسط کاربران شبکه امضاء کددار می‌تواند مفید واقع شود اگر طراحی و ایجاد نرم‌افزار سرور و محتویات آن در حد مهارتها نیست یا محدودیت زمانی دارد انجام این عملیات را می‌توانید به اشخاص یا شرکتهای دیگری واگذار نمود.

* 1. **مقدمه‌ای بر سیاست امنیت**

نخستین و اساسی‌ترین ابزار امنیت هر سازمانی سیاست امنیت آن هست سیاست امنیت ستون فقرات تمامی عملیات است چون قواعد رفتار تجاری را تعیین می‌کند این قواعد قوانین، پروتکل‌ها، کاربردها، کارکنان و حتی کاربرهایی را که انتظار می‌رود سیستم‌ها از آن‌ها پیروی کنند شکل می‌دهد، ایجاد سیاست امنیت تعهد سنگین است اما با توجه دقیق به جزییات و برخی دوراندیشی‌ها در مورد حالات که ممکن است رخ دهد کاری است قابل کنترل و خطیر سیاست امنیت می‌بایست به عنوان یک سند زنده مطرح شده و دائماً بازبینی و اصلاح شود همان‌طور که درس‌های جدید آموزش داده و یا یک سازمان تأسیس شود.

سیاست امنیت می‌بایست به عنوان ابزاری برای کمک به ایجاد اجرا و پیکربندی ابزارهای فنی نظیر دیوارههای آتش، دستگاه‌های آشکارساز ورود غیر مجاز IDS ها و شبیه آن به کار برده شود. تمامی این راه حل‌های فنّاوری می‌بایست در علمیات خود بازتابی از سیاست امنیت را داشته باشند این ابزار می‌بایستی توسط یک سیاست قابل قبول قوانین را اجرا کرده و از رفتارهای نامناسب جلوگیری نماید.

## **سیاست امنیت چیست؟**

RFC 2196 سیاست امنیت را این طور شرح می‌دهد، قواعد و قوانینی است که اشخاص که به سرمایه‌های اطلاعاتی و فنی شرکت دسترسی دارند می‌بایست به آن‌ها وفادار باشند این تعریف دلالت بر این دارد که شرکت‌ها نحوه به کارگیری فنّاوری خود را بشناسند و در صورتی که روشهای دیگری بکار برده‌اند بشناسند و بدانند که چه اتفاقی خواهد افتاد بهتر است سیاست امنیت را به دید یک ابزار تجاری یک روش برای ایجاد فرایندهای ایمن، و یک فعال کننده برای دست‌یابی به سود، مدنظر قرار گیرد سیاست امنیت می‌بایست به‌منظور کمک به دیگران در اتخاذ تصمیمات ایجاد شود نه ورود به جاده سوددهی، مطمئن‌ترین راه برای ضایع شدن تلاش‌های ایجاد سیاست امنیت افراط در آنهاست یک سیاست امنیت مؤثر، بین هزینه ریسک و هزینه از دست دادن سود تعامل برقرار می‌سازد. چه بسا یک مدیر امنیت با ایده‌های عالی که ارائه نموده است به خاطر عدم درک نیاز به محدود نمودن واقع بینانه اهدافش حداقل در کوتاه مدت راه به جایی نبرده است ماشین سیاسی حرکت کندی دارد. امنیت تجارت الکترونیکی به معنی حفاظت از اطلاعات است اما امنیت اطلاعات مهم‌تر از امنیت کامپیوتر است تنظیم اهداف امنیت سایت برقراری تعادل بین فرهنگ شرکت، کاهش خطر، تفهیم هزینه و سودمندی را می‌طلبد همیشه یک سایت، بسته به سمت و سوی لحظه‌ای تجارت الکترونیکی، نیاز به اصلاح دارد.

## **ارزش در برابر ریسک**

سطح امنیت مطلوب برای هر سازمان تجاری خواه تجارت الکترونیکی یا تجارت عمومی، توسط سرمایه‌هایی که می‌بایست محافظت شود و تحمل شرکت در برابر از دست دادن این سرمایه‌ها مشخص می‌گردد. امنیت مقرون به صرف بیشتر از آن چه که برای تجارت ارزش دارد برای حفاظت از یک ارزش هزینه‌ای ندارد هر چند ارزش آن برای یک تجارت خاص ممکن کمتر یا بیشتر از ارزش بازای واقعی باشد هم چنین بعضی از مدیران تجارت عمومی ممکن است به‌طور کامل ارزش سرمایه‌های غیر قابل لمس نظیر کد مبدأ یا اطلاعات مشترکی را درک نکرده باشند. این که چه چیزی باید محافظت شود از چه تهدیداتی و با چه هزینه‌ای برای یک تاجر بایستی اولویت داشته باشد در غیر این صورت نمی‌توان فهمید که آیا یک راه حل سخت افزاری یا نرم‌افزاری برای امنیت احتیاجات را برآورده می‌کند یا نه یک قسمت قابل توجه از سیاست امنیت شامل نتیجه تحلیل و تثبیت سرمایه‌هایی است که یک شرکت می‌خواهد محافظت کند هزینه مقابله با تهدیدات این ارزش‌ها و سرمایه‌ها و تعاریف قابل قبول برای کاربرد این ارزش‌ها هست.

### سیاست امنیت شامل چه عناصری است

یک سیاست امنیت جامع از چند سیاست منحصر به فرد ساخته شده است هر یک از آن‌ها جنبه‌های یگانه‌ای از فرآیندهای تجاری سایت را مورد هدف قرار می‌دهند این جوانب می‌بایست به‌طور ویژه‌ای در سرتاسر هر ردیف از امنیت ارائه شده برای یک سایت نظیر امنیت پیرامون، امنیت شبکه و امنیت درخواست میزبان مدنظر قرار گیرد چرا که هر ردیف سیاست متفاوتی به کار می‌رود.

تعریف موارد امنیت: شامل مواردی نظیر اطلاعات محرمانه، در مقابل اطلاعات عادی شرح جوابگویی: قوانین و مالکیت روالی را تعریف می‌کند این سیاست هدف تیم یا کمیته امنیت را تعریف کرده و اجرای توقعات بخش‌های مختلف درون یک سازمان را تنظیم می‌کند.

استفاده قابل قبول سیاست:‌ توقعات کنترل‌های دسترسی پیام‌های اخطار و مسئولیتهای استفاده را تنظیم می‌کند پروتکل‌های قابل قبول، مکانیزم های تأیید، جریانات ترافیک و آنچه که ورود یک غیر مجاز را شکل می‌دهد را تعریف می‌کند.

سیاست‌های محرمانگی[[64]](#footnote-64) توقعاتی که برای اختفاء وجود دارد را تعریف می‌کند.

سیاست نظارت: کنترل تغییر و روال‌های مستحکم نمودن سیستم را تشریح می‌کند این سیاست مشخص می‌کند که چگونه مدیریت و نظارت از راه دور بایستی اتفاق بیفتد و چگونه یا وظایف فناوری اطلاعات یک شرکت بیرونی برخورد شود.

سیاست بازرسی و هشدار: ایجاد ملزوماتی که برای اطمینان از نیازهای سایت در نظر گرفته شده شامل ورود کردن مانیتور کردن و آشکارسازی ورود غیر مجاز.

سیاست دسترسی پذیری: ملزوماتی را که برای در دسترس بودن نگهداری ویندوز جواب گویی رویدار و واقعه بازیابی و اصلاح خسارت و ملزوماتی جهت تهیه نسخه پشتیبان روی نوار مغناطیسی و چشم‌پوشی از قسمت‌هایی از لیست اموالی که تحت پوشش قرار گرفته را تعر یف می‌کند.

سیاست خرید: خصوصیات لازم برای خرید سخت افزار را شرح می‌دهد سطح و نوع نرم‌افزار رمزگذاری که می‌بایست پشتیبانی شود روال‌های استفاده از نرم‌افزار غیر مجاز و خصوصیات نگهداری نرم‌افزار در این جا مشخص می‌گردد این سیاست‌های ویژه توسط چگونگی کار آن‌ها با یکدیگر برای تضمین سه قبضه هر ردیف امنیت برای سایت مطرح خواهد بود سه تضمین برای هر ردیف امنیت عبارت است از:

1- رازداری سرمایه‌های اطلاعاتی

2- صحت سرمایه‌های اطلاعاتی

3- در دسترس بودن سرمایه‌های اطلاعاتی

اگرچه چیزی به عنوان یک سیستم کاملاً ایمن وجود ندارد اما انجام ارزیابی‌ها شاید سایت را به خواسته‌ها نزدیکتر نماید خیلی از اوقات در جریان اشتیاق ایجاد یک سایت جدید تعداد کمی از مراحل یا جزییات فراموش می‌گردد این چشم پوشی‌ها یا فراموش کاریهای تصادفی ممکن است راهی را برای یک مهاجم باز نماید.

چه انتظاری از تست امنیت می‌توان داشت این انتظار را می‌توان داشت که تیم برخی سوراخها و حفره‌ها را پیدا کند آن‌ها را اصلاح نماید موارد بیشتری را بیابد و این چرخه دائماً تکرار شود هم چنین می‌توان انتظار داشت که وقتی سایت به روی عموم گشوده شد مردم دیگر آن را برای شما تست کنند تمام هدف این است که شمارا یک قدم به جلوتر ببرد.

پیش بینی انواع مختلف هجوم: برای این که سایت در مقابل یک هجوم آماده باشد می‌بایستی انواع مختلف تهاجمات را شناخته و نحوه کار آن‌ها را بدانید.

هر هجومی سعی دارد تا یک ترکیبی از سه مورد رازداری، صحت و دسترس پذیری که شرح داده شد را واژگون سازد کار شما نگهداری و حفظ این سه مورد است و کار یک مهاجم به خطر انداختن آن‌ها با هجومهایی است که در این فایل شرح داده می‌شود.

هجوم‌های رد سرویس[[65]](#footnote-65)

هجوم‌های نشست اطلاعات[[66]](#footnote-66)

حملات دسترسی به فایل[[67]](#footnote-67)

تهاجمات اطلاعات غلط[[68]](#footnote-68)

حملات دسترسی به فایل / بانک اطلاعاتی ویژه[[69]](#footnote-69)

حملات بالا بردن حق امتیاز[[70]](#footnote-70)

هجوم‌های رد سرویس: قابل فهم ترین نوع هجوم DOS هست هم چنین دفاع در مقابل آن مشکل‌ترین تهاجمات دیگر است یک هجوم DOS هجومی است که در مقابل دسترسی صورت می‌گیرد و عموماً روی صحت و رازداری تأثیر نمی‌گذارد در برخی موارد اگر یک هجوم DOS باعث Crash شود برخی فایلها ممکن است خراب شود هر چند خرابی هر فایلی تحت کنترل هستیم یک مهاجم است اما فقط یک خسارت جنبی هست دو گروه اصلی از هجومهای DOS عبارت است از سیل[[71]](#footnote-71) و هدف گیری شده یک هجوم سیل با پوشاندن شکار خود با یک توده خالص خواه اطلاعات یا ترافیک شبکه، کار می‌کند یک هجوم هدف گیری شده جستجو برای کشف برخی اشکالات یا شرایط ویژه را انجام می‌دهد تا یک دستگاه یا سایت را غیر قابل دسترس کند. یک روش برای انجام حمله سیل به یک شبکه داشتن یک لوله بزرگ‌تر هست چنانچه من یک (45 Mbps) T3 داشته باشم و شما در خانه یک ارتباط دیجیتال (DSL) داشته باشید آنگاه شما از دست خواهید رفت. می‌توان این مشکل را با درخواست از ISP برای مسدود کردن ترافیک من، تقاضا از من برای خروج از شبکه یا انداختن در زندان تخفیف داد، اما این کارها زمان بر است و ضمناً شما در این اثناء نمی‌توانید کار کنید اگر بخواهیم کار خلافی انجام دهیم آدرس‌های مبدأ را جعل می‌کنیم بطوری که نتوانند بسادگی ردیابی شوند چنانچه به ISP شکایت شود می‌توان کاری کرد ترافیک شبیه یک ترافیک عادی به نظر رسد. بنابراین ISP نمی‌تواند بفهمد که کدام ترافیک را فیلتر نماید و کدامیک را نه، یا اینکه می‌توان چندین ماشین یا سایت را برای انجام هجوم سیل به کار برد.

تهاجمات سیل محدود به شبکه‌ها نمی‌شود یک دیسک نیز ممکن است مورد هجوم یک سیل قرار گیرد و تمامی فضای روی دیسک را اشغال کند یا از چیزهایی شبیه بمب خوشه‌ای استفاده کند، برنامه‌ای است که مرتباً از خود کپی‌هایی را روی دیسک سخت ایجاد می‌کند با این کار منابع روی یک ماشین همزمان مصرف شده و آن را کند کرده و نهایتاً باعث سقوط آن خواهد شد تا ‌CPU حافظه و بخشهای پردازشی را مصرف کند این نوع هجوم سیل برخی اوقات به‌منظور حملات ویژه بیشتری به کار برده می‌شود. یک حمله DOS هدف گیری شده نتایجی شبیه به حمله سیل دارد، بدین صورت که در صورت موفقیت آمیز بودن حمله برخی چیزها غیر قابل دسترسی هست.

ساده‌ترین مثال برای یک هجوم هدف گیری شده زمانی است که برخی سرویسهای در حال اجرا روی یک ماشین برای ایجاد Crash به کار رود این کار با برقراری ارتباط با آن و ارسال اطلاعات ناهنجار صورت می‌گیرد.

این دستگاه می‌تواند یک سرور وب سرور DNS سرور MAIL و غیره باشد برخی اوقات این اشکالات در سطح سیستم عامل پدید آید.

به‌طوری عادی یک هجوم سیل DOS در جایی بین هجوم سیل و یک هجوم هدف گیری شده قرار می‌گیرد نظیر یک هجوم سیل SYN این حمله مدام با ارسال بسته‌های SYN از آدرس‌های IP جعلی انجام می‌شود که در سیستم عامل‌های قدیمی‌تر بافرهایی را که منتظر ارتباط جدید بودند پر می‌کند هر ارتباط جدید معمولاً به یک تایمر متصل می‌گردد، بنابراین جریان ثابتی از بسته‌ها، لازم هست اما نه با یک سرعت بالا.

هجوم‌های نشت اطلاعات: کلاس بعدی هجوم، نشست اطلاعات هست یک هجوم نشست اطلاعات حمله‌ای به رازداری هست نشست اطلاعات هنگامی اتفاق می افتد که یک مهاجم اطلاعاتی را بدست آورد که شما نمی‌خواهید یک نشست، اطلاعات کافی برای دسترسی سریع به دستگاه‌های شمارا در اختیار قرار نمی‌دهد اما در عوض ممکن است به یک مهاجم باهوش اطلاعاتی را بدهد که ایده‌ای باشد برای انجام کار یا ممکن است اطلاعات به دست آمده با اطلاعات دیگر ترکیب شود و یک نفوذ ایجاد گردد تمام سیستمها اطلاعاتی را در مورد خود تراوش می‌کنند که قابل پیش گیری نیست بین دستگاه‌های عامل تفاوتهای بسیاری وجود دارد. به عنوان مثال یک مهاجم باهوش می‌تواند تعیین کند که چه سیستم عاملی را به کار گرفته‌اید کار یک مهاجم این است که هر چه بیشتر اطلاعاتی در مورد هدف خودش جمع‌آوری کند تا هجوم خود را طرح ریزی کند. اگر یک مدافع کار خود را به خوبی انجام داده باشد، کمترین اطلاعات را تراوش خواهد کرد و کمترین همکاری را با یک مهاجم خواهد نمود. از طرف دیگر اگر مدافع کار خودش را ضعیف انجام دهد اطلاعاتی را در اختیار یک مهاجم قرار می‌دهد که مستقیماً می‌تواند یک سیستم یا سایت را به مخاطره بیندازد.

### هجوم‌های دسترسی به فایل

همانطور که از نام این نوع هجوم پیداست، هجومی است که یک مهاجم برای دستیابی به فایل‌های روی یک سیستم انجام دهد، این یک هجوم به رازداری و صحت اطلاعات هست زیرگروههایی برای دسترسی به فایل وجود دارد نظیر دسترسی خواندن، دسترسی نوشتن، و مجوزهای حذف کردن دسترسی خواندن فقط روی رازداری تأثیر می‌گذارد، در صورتی که اجازه اصلاحات روی صحت تأثیر خواهد گذاشت به هر حال اگر یک مهاجم روی یک هدف بتواند فایل‌های دل خواه خود را بخواند آن گاه خطرات بیشتری ضمانت می‌شود.

یک مهاجم ممکن است به فایل‌هایی دسترسی پیدا کند که مدافع از آن بی اطلاع است معمولاً این حالت به دلیل پیکربندی اشتباه یا یک سوراخ به وجود می‌آید سرویس‌های زیادی برای ارائه دسترسی به فایل‌ها یا روش‌های مختلف وجود دارد. بنابراین باعث شگفتی نخواهد بود اگر سوراخ‌ها یا پیکربندی‌های نادرستی پدید آید. بیشتر سرویس‌های مبتنی بر فایل نظیر سرورهای پروتکل ارسال فایل FTP و پروتکل ارسال ابر متن HTTP سعی در محدود نمودن فایل‌هایی که کاربر می‌تواند مورد دسترسی قرار دهد دارد یک دایرکتوری ریشه برای برنامه تعریف می‌شود و کاربران قادر به دستیابی فایل‌های خارج از این ساختار دایرکتوری نیستند هر چند اشتباهاتی رخ دهد دستگاه‌های عامل مبتنی بر UNIX و DOS ویندوز از.. برای نشان دادن فهرست پدر یک فهرست جاری استفاده می‌کنند لذا وارد کردن دستور Cd فهرست جاری را یک سطح بالا می‌برد. برخی نرم‌افزارهای سرور این را به حسب نمی‌آورد اجازه می‌دهند تا به عنوان درخواست یک فایل به کار برده شود که به یک مهاجم اجازه داده می‌شود تا پای خود را از گلیمش درازتر نماید.

### تهاجمات اطلاعات غلط

یک هجوم اطلاعات غلط برای گیج کردن یک مدافع طراحی شده هجومی است در برابر صحت اطلاعات، نه صحت خود سیستم‌ها بلکه اطلاعات مدافع در مورد سیستم‌ها این هجومی است به صحت اطلاعات تفاوت بین هجومی که یک فایل گزارش را حذف یا ویرایش می‌کند و حمله غلط این است که در یک حمله اطلاعات غلط، اطلاعات اصلی هنوز موجود هست فقط چیزهایی حذف شده است یک مثال ساده فرض کنید شما فایل گزارشی دارید که حاوی اطلاعاتی در مورد تلاشهای ناموفق ورود است یک مهاجم ناشی با نوشتن یک اسکرپیت سعی می‌کند که با کلمه عبور guess و نام کاربر ewinter بارها بارها ورود کند خواهید دید که در گزارشات صدها تلاش ناموفق برای ورود با کاربر ewinter وجود دارد که شما خواهید دانست با چه شناسه‌ای واردشده و چه اتفاقی افتاده است شما با شخصی که شناسه متعلق به اوست صحبت کنید تا ببیند چه اطلاعای راجع به آن دارد چنانچه شما برای هر یک از کاربران خود صدها ورودی در گزارش خود داشته باشید در کل هزاران خط با کلمات میهمان وارد می‌شوند اما اگر ورودی‌های گزارش ثابت نگه داشته شوند نخواهید دانست که چه کسی واردشده و چه موقع یک مهاجم موفق به ورود شده است. یک هجوم اطلاعات غلط یک اسکن nmap هست که یک ترافیک اضافی روی میزبان و در کنار بسته‌های واقعی که اسکن را انجام می‌دهد تولید می‌کند اطلاعات واقعی آنجا هستند اما می‌بایست آن‌ها را جدا کنید.

### هجوم‌های دسترسی به فایل / بانک اطلاعاتی ویژه

این نوع از هجوم تقریباً شبیه به هجوم دسترسی به فایل هست تنها تفاوت آن این است که هجوم به یک سیستم فایل رسمی صورت نمی‌گیرد شبیه یک هجوم دسترسی به فایل حملات ممکن است به رازداری و صحت صورت گیرد که بستگی به سطح دسترسی به دست آمده دارد، مثال‌هایی از انواع فایل‌های ویژه هر ترتیبی از بانک اطلاعاتی یا روش دسترسی به آن نظیر Sybase-Oracle یا MySQL هست و مشابه آن رجیستری ویندوز: این چنین فایل‌های ویژه معمولاً در بالای یک سیستم فایل به سر می‌برد هر چند کل مجموعه اطلاعات ممکن است فقط در یک فایل تنظیم قرار داده شود. اگر به زیر ساخت سیستم فایل دسترسی پیدا شود به خطر انداختن فایل‌های ویژه امکان پذیر خواهد بود توجه داشته باشید که دسترسی به اصل یک فایل از یک بانک اطلاعاتی یا فایل شبیه به آن باعث خرابی آن خواهد شد اگر فایل فعال باشد.

برنامه‌های بانک اطلاعاتی و رجیستری ویندوز ایندکسهای اطلاعاتی که می‌بایست هماهنگ با اطلاعات نگه داشته شود را دنبال می‌کند و ممکن است که همان وقتی که شما سعی در نوشتن در یک فایل همیشه آن‌ها را نیز همین کار را انجام دهند ذخیره موقت[[72]](#footnote-72) نیز به وقوع می‌پیوندد به این ترتیب که حتی اگر شما محل نوشتن در فایل را به درستی نظارت کنید ممکن است یک عمل کپی کردن در حافظه باشد ارائه نسخه نامربوط در این حالت ممکن است کپی نیز رونویسی شود و این هنگامی است که Cache تخلیه گردد دسترسی خواندن، اغلب بسیار کاربردی هست و این در صورتی است که قادر باشید قالب و فرمت فایل را به‌طور مناسب تغییر نمایید اگرچه ممکن است برخورد زیادی یا سختی تلاش برای نوشتن یک کلمه عبور در یک فایل بانک اطلاعاتی یا تغییر مستقیم در فایل داشته باشید کارکنان بسیار عجیبی در یک سایت یا بانک اطلاعات زندگی می‌کنند که در مورد سایت‌های تجارت الکترونیکی صادق است ممکن است یک اشتباه بزرگ و متداول برنامه نویسی که توسع دهندگان مرتکب می‌شوند زمانی است که توسعه یک سایت وب به‌طور نامناسب خاتمه یابد یا اطلاعات تهیه شده برای کار فیلتر گردد این کار برای مهاجم راهی باز خواهد نمود تا دستورات SQL خود را به یک بانک اطلاعات بفرستد اغلب یک مهاجم می‌تواند از راه دور مجموعه صحیحی از دستورات را به یک سرور SQL بخوراند.

چرا مهاجمین توانایی تهدید سایت ها را دارند و چگونه آن‌ها شناسایی می شوند، یک مهاجم نوعی تهدید است تهدیدات دیگر شامل قطع برق، از دست دادن ارتباط و هر چیزی که مانع انجام ایمن تجارت است، دو نوع اصلی از تهدیدات، هجوم به تسهیلات و هجوم هدف گیری شده هست، هجوم به تسهیلات هنگامی پدیدار می‌شود که یک مهاجم سعی در پیاده کردن روشهای جدید روی هر ماشینی در جهان که شامل شما نیز می‌شود دارد. بنابراین آن‌ها سرتاسر اینترنت را برای پیدا کردن ماشین‌های آسیب پذیر اسکن می‌کنند که شما جزء آن هستید در اکثر اوقات این نوع اسکن‌ها برای حفره‌های شناخته شده و قدیمی‌تر به کار می‌رود اگر حداقل توجه و مراقبت را نسبت به ملحقات داشته باشید تا حدی از گزند این نوع هجوم در امان خواهید بود. مهاجمی که شخص را نشانه گیری کرده باشد خطرناکتر است آن‌ها مسر هستند و عموماً در مورد این که چه نوع هجوم یا هجومهایی را انجام دهند هوشمندانه‌تر عمل می‌کنند.

کار ما این است که مواظب این مهاجمین باشیم و نوع حمله‌های صورت گرفته را تعیین کرد که کار ساده‌ای نیست با اطلاعات بسیار محدودی داریم و می‌کوشیم تا مقاصد مهاجمی که هزاران کیلومتر دورتر است کشف نماییم. یک هجوم به تسهیلات معمولاً به دنبال مجموعه محدودی از آسیب پذیری ها می‌گردد کرمها مثال خوبی از این نوع می‌باشند کرم Ramen پورت‌های 111 (Portmapper) 21 (FTP) و 512 (Lpd/lprng) مربوط به میزبانها را اسکن می‌کند و دارای RPC که (Remote Procedure Call) هست از Statd, و (Wuftpd) که روی لینوکس 6.2 Red Hat و Lprng که با Rea Hat 7.0 کار می‌کند بهره ببرد یک مهاجم یا یک (کرم) به این روش شمارا تست می‌کند در صورتی که جواب نگیرد IP بعدی را چک خواهد نمود، شخص برای او جالب نیست تنها ماشین یا ماشینهایی که او می‌تواند از آن‌ها بهره ببرد مهم است مهاجمی که شمارا هدف قرار داده سعی در رخنه یا سرور شمارا دارد و به دنبال ضعف‌هایی است که در نظر نگرفته شده هم چنین مهاجمی که سایت را نشانه رفته معمولاً برخی عملیات شناسایی را انجام می‌دهد که شامل اسکن کردن پورت انگشت نگاری سیستم عامل، تلاش برای سنجش سطح دفاع و تصرف برخی از فایل‌های نمونه است. با بررسی گزارشات دیوار آتش و IDS به اختلاف بین کسانی که حقه بازی و فریب کاری می‌کنند پی خواهید برد ما امیدواریم که یک مهاجم از طریق مجموعه آدرسهای IP ثابت وارد شود اما همیشه این طور نیست باید همیشه متوجه پورت‌هایی که به‌طور متداول برای بهره گیری جدید اسکن می‌شود، باشید این نوع اطلاعات را می‌توان با خواندن فهرست‌های نامه نگاری به دست آورد و لیستی از چیزهایی که برای آن اسکن می‌شوید خصوصاً اختلال[[73]](#footnote-73) تهیه نمود.

## **فهرست منابع**

[1] David Thiel, iOS Application Security, No Starch Press, February 2016,296

[2] Johnny Long, Bill Gardner, Justin Brown, Google Hacking for Penetration Testers, 3rd Edition, Elsevier / Syngress, November 2015,234

[3] Kevin Beaver, Hacking For Dummies, 5th Edition, Wiley / For Dummies, December 2015,408

[4] Kevin Cardwell, Henry Dalziel, Essential Skills for Hackers, Elsevier / Syngress, December 2015, 48

[5] Oriyano, CEH v9, 3rd Edition, Wiley / Sybex, April 2016,648

[6] Owen Yamauchi, Hack and HHVM, O'Reilly Media, September 2015,284

[7] Raymond Blockmon, CEH v9, Wiley / Sybex, April 2016,192

[8] 599eme Man, "Xss & Iframe Phishing", exploit-db, 2016, 8.

[9] behindthehills, "xss2phishing", exploit-db, 3.

[10] John, "DNS-Based Phishing Attack in Public Hotspots", exploit-db, 2016, 4.

[11] Markus Jakobsson, Filippo Menczer, "Web Forms and Untraceable DDoS Attacks", exploit-db, 2016, 24.

[12] Rockey Killer, "Phishing - The Art of fooling End Users", exploit-db, 2016, 9.

## **Abstract**

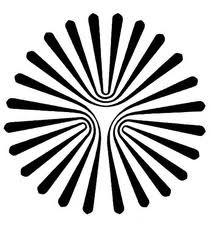
Nowadays with increasing computer clients and Digitization of large volumes of information such as images and videos, Bank transactions, communications, Organization archives and..., There are Prepared many targets for hackers, Therefore, knowledge of hacking techniques, vulnerabilities and security in computer networks and the Internet is very important.

Information and computer security in today's world is an important part of Computer Engineering, and it’s possible by identifying ways to hack, Identifying security holes, and tools used by hackers. Due to the increasing Changes of computer systems, their upgrade, fixing the security holes, the Hackers update their tools and methods too, so Computer engineers need to update their knowledge in order to confront them.

In this project we are getting to know different kinds of attacks from the hackers, different kinds of bugs and ways to identify the hackers.

The contents of this project is regulated in six seasons. First chapter has been an introduction to hacking, basic definitions, Trojans and other definition, that cause better understanding of later chapters. In the second chapter the definition of security, some aggressive and expert reviews on them, firewall and how to bypass it and prevent identify open ports will be discussed. The third chapter covered topology, hack, hacker-stimulating agents, viruses, DDOS, worms and keyboard readers. Chapter Four are evaluated scripting code such as JavaScript in terms of security and hacking and review how they are hacking. The fifth chapter is devoted to the conclusions and recommendations in security.

Key words: Hack - security - prevention of infiltration - infiltration – Sniffing information - the malware

Payam Noor University

**Hacking on computer networks / internet**

A Project Report

Presented to:

Department of Information Technology and Communication

Faculty of Engineering

Payam Noor University of Damavand

In Partial Fulfillment of the Requirement for the degree of

Bachelor of Science in

**Software Engineering**

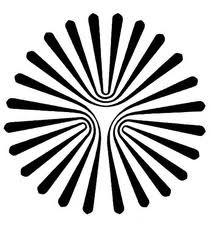
Advisor:

**MRS. Mahboobe Kamyab**

By:

**Saeed Azari**

May 2016

 Payam Noor University

**Hacking on computer networks / internet**

A Project Report

Presented to:

Department of Information Technology and Communication

Faculty of Engineering

Payam Noor University of Damavand

In Partial Fulfillment of the Requirement for the degree of

Bachelor of Science in

**Software Engineering**

Advisor:

**MRS. Mahboobe Kamyab**

By:

**Saeed Azari**

May 2016

1. yahoo messenger [↑](#footnote-ref-1)
2. Hotmail [↑](#footnote-ref-2)
3. Server [↑](#footnote-ref-3)
4. Backspace [↑](#footnote-ref-4)
5. MSN messenger [↑](#footnote-ref-5)
6. ICQ [↑](#footnote-ref-6)
7. Crack [↑](#footnote-ref-7)
8. Cracker [↑](#footnote-ref-8)
9. mailbox [↑](#footnote-ref-9)
10. Phishing [↑](#footnote-ref-10)
11. spiders [↑](#footnote-ref-11)
12. Trash [↑](#footnote-ref-12)
13. spyware [↑](#footnote-ref-13)
14. Denial-of-Service [↑](#footnote-ref-14)
15. Java [↑](#footnote-ref-15)
16. JavaScript [↑](#footnote-ref-16)
17. ActiveX [↑](#footnote-ref-17)
18. redirector [↑](#footnote-ref-18)
19. Boarder Guard [↑](#footnote-ref-19)
20. body guard [↑](#footnote-ref-20)
21. strong authentication [↑](#footnote-ref-21)
22. Secure Socket Layer [↑](#footnote-ref-22)
23. Hub [↑](#footnote-ref-23)
24. Switch [↑](#footnote-ref-24)
25. Router [↑](#footnote-ref-25)
26. Reapter [↑](#footnote-ref-26)
27. Bridge [↑](#footnote-ref-27)
28. Proxy\_Server [↑](#footnote-ref-28)
29. Back door [↑](#footnote-ref-29)
30. Soci Engieneering [↑](#footnote-ref-30)
31. Packets [↑](#footnote-ref-31)
32. Zombies [↑](#footnote-ref-32)
33. Stateful inspection [↑](#footnote-ref-33)
34. Scanner [↑](#footnote-ref-34)
35. Soopshots [↑](#footnote-ref-35)
36. Unix [↑](#footnote-ref-36)
37. platform [↑](#footnote-ref-37)
38. Signatur [↑](#footnote-ref-38)
39. Anonymous [↑](#footnote-ref-39)
40. Windows challenge response [↑](#footnote-ref-40)
41. Apache [↑](#footnote-ref-41)
42. Merriam Webster [↑](#footnote-ref-42)
43. CNN [↑](#footnote-ref-43)
44. Broadcast [↑](#footnote-ref-44)
45. Note Pad [↑](#footnote-ref-45)
46. اطلاعات بیشتر در https://en.wikipedia.org/wiki/ILOVEYOU [↑](#footnote-ref-46)
47. Antivirus [↑](#footnote-ref-47)
48. Melissa [↑](#footnote-ref-48)
49. Microsoft office [↑](#footnote-ref-49)
50. virus builder Accessory [↑](#footnote-ref-50)
51. Trojan hourse [↑](#footnote-ref-51)
52. Netscape [↑](#footnote-ref-52)
53. اصطلاح اپلت (برنامک) در سال ۱۹۹۳ توسط applescript معرفی شد. کلمه برنامک می‌تواند برای شرح برنامه‌هایی استفاده شود که به‌تنهایی و بدون لینک به شبکه قابل استفاده هستند. از قبیل بسته‌های کامل که با سیستم‌عامل ارائه می‌شوند برای مثال ماشین‌حساب یا یک ویرایشگر متن. [↑](#footnote-ref-53)
54. Authenticode [↑](#footnote-ref-54)
55. File I/O [↑](#footnote-ref-55)
56. Dynamic Data Exchange (DDE) [↑](#footnote-ref-56)
57. Object instantiation [↑](#footnote-ref-57)
58. Direct Database Access [↑](#footnote-ref-58)
59. Execution of Dll code [↑](#footnote-ref-59)
60. Procedures [↑](#footnote-ref-60)
61. Outsourcing [↑](#footnote-ref-61)
62. Batch Files [↑](#footnote-ref-62)
63. Shell functions [↑](#footnote-ref-63)
64. Privacy Policy [↑](#footnote-ref-64)
65. Denial of Service [↑](#footnote-ref-65)
66. Information Leakage [↑](#footnote-ref-66)
67. File Access [↑](#footnote-ref-67)
68. Misinformation [↑](#footnote-ref-68)
69. Special File/ Data base Access [↑](#footnote-ref-69)
70. Evelation of privilege [↑](#footnote-ref-70)
71. Flood [↑](#footnote-ref-71)
72. Caching [↑](#footnote-ref-72)
73. Noise [↑](#footnote-ref-73)