





مؤسسه آموزش عالی علوم و فناوری سپاهان

گروه فناوری اطلاعات

گزارش پروژه دوره کارشناسی فناوری اطلاعات

با عنوان :

ارزیابی امنیتی حملات ممکن به شهر الکترونیکی

استاد راهنما :

آقای مهندس حمید صاحب خرد

دانشجو :

محمد مهدی درفشی

بهار ۱۳۸۹

چکیده:

ابتدا شرح مختصری از حملات کامپیوتری صورت می پذیرد و موارد کاربرد هر کدام مورد بررسی قرار می گیرد سپس با در نظر گرفتن واحدهای موجود در یک شهر الکترونیکی از قبیل دبیرستان مجازی، دانشگاه مجازی، بیمارستان مجازی و ... حملاتی را که ممکن است به آنها صورت گیرد را مورد بررسی قرار می دهیم و سپس راه های جلوگیری از آنها نیز توضیح داده می شود. بنابراین می توان با اطلاع داشتن از انواع حملات و راه های جلوگیری از آنها، امنیت یک شهر الکترونیکی را افزایش داد.

تشکر و قدر دانی :

لازم می دانم که از زحمات استاد محترم،سرور گرامی ،جناب آقای مهندس صاحب خرد که با صبری وصف ناپذیر در طی چهار ترمی که با ایشان دروس مختلفی را داشته ام، این حقیر و سایر دانشجویان را با علوم مربوط به فناوری اطلاعات آشنا ساخته اند؛ نهایت تشکر و قدردانی را به عمل آورم و دست بوس ایشان به جهت زحمات و صبری که در راه آموزش بنده متحمل شده ام باشم.

پر واضح است که هر شاگرد خوبی که استعداد تبدیل شدن به استاد خوبی را دارد،ابتدا استاد خوبی داشته که در راه آموزش او از هیچ چیزی دریغ نکرده است لذا مهندس صاحب خرد نیز با قبول زحمت مطالعه ی پایان نامه ی بنده،منت را بر این شاگرد کوچک خود تمام کرده و یاد و نامشان تا ابد در حافظه ی بنده باقی است.از خداوند برای ایشان و سایر اساتیدی که در طول دوره ی کارشناسی زحمتی در جهت آموزش بنده متقبل شده اند طلب توفیق روز افزون و پیشرفت این بزرگواران را از درگاه خداوند خواستارم.

فهرست مطالب

	آشنایی با شهر الکترونیکی
۱	مقدمات
۲	اهداف شهر الکترونیکی
۲	راهبردهای شهر الکترونیکی
	- بیمارستان الکترونیکی
۵	تعریف
۷	اهداف پزشکی از راه دور
۷	کاربرد اصلی پزشکی از راه دور
۸	انواع پزشکی از راه دور
۹	جراحی از راه دور
۱۰	اولین جراحی از راه دور فرانکفورت در جهان
۱۱	روش Robotic
۱۲	اولین بیمارستان مجازی در جهان
	- دانشگاه الکترونیکی (مجازی)
۱۳	آموزش الکترونیکی چیست
	- بانکداری الکترونیک
۱۷	بانکداری الکترونیکی چیست و چالش‌های پیش روی بانکداری الکترونیک در ایران
۱۷	جایگاه تجارت الکترونیک
۱۷	تعریف تجارت الکترونیک
۱۸	تعریف بانکداری الکترونیک
۲۰	سرویس‌های بانک الکترونیک
۲۰	شاخه‌های بانکداری الکترونیک
۲۱	مزایای بانکداری الکترونیک
۲۳	پول الکترونیکی یا پول دیجیتال
۲۵	پول الکترونیکی و ویژگی‌های آن
۲۷	پیامدهای اقتصادی گسترش استفاده از پول الکترونیکی

روش‌های نفوذ

	- حملاتی که وبسایت ما را مورد هدف قرار می‌دهد
۳۰	تزریق دستورات SQL
۳۱	SQL Injection چیست؟
۳۲	چگونگی تشخیص
	راه‌های مقابله
۳۳	به روز باشید
۳۴	رمزنگاری

۳۶	مثال های عملی
۳۸	نتیجه گیری
	XSS
۳۹	آشنایی با XSS
۴۰	چگونه XSS رخ می دهد؟
۴۹	محافظت وبسایت از XSS
۵۰	چگونه از خودمان در برابر حملات XSS محافظت کنیم ؟
	- حملاتی که برنامه های تحت سیستم عامل را مورد هدف قرار می دهد
	ویروس ها
۵۱	مقدمه
۵۲	تاریخچه
۵۳	تقسیم بندی ریزتری از ساختمان ویروس ها و حوضه فعالیت آنها
۵۳	ویروسها چگونه پخش می شوند
۵۴	نحوه مخفی شدن ویروسها و نحوه اطلاع ما از وجود ویروس
۵۷	پیشگیری از ویروس
۵۸	علت ایجاد ویروس های کامپیوتری
۵۹	نتیجه گیری
	تروجان ها
۶۰	مقدمه ای در باره ی تروجان ها
۶۰	تاریخچه
۶۱	معرفی و مقابله با تروجان
۶۴	تهدیدهای آتی
۶۷	نتیجه گیری
	کرم ها
۶۸	مقدمه
۶۹	تاریخچه اولین Worm
۷۰	نحوه تکثیر به چه صورت است
۷۲	آنالیز یک کرم
۷۲	آسیب پذیری چیست
۷۳	معمول ترین خطاهای برنامه نویسی که منجر به آسیب پذیری ها می شوند
۷۵	تاریخچه آسیب پذیری ها
۷۶	عملیات یک کرم در سیستم عامل
۷۸	Local and remote
۷۹	Port scanning
۷۹	آلوده سازی
۸۱	نمونه ای از آسیب پذیری های موجود در زبان C/C++

۸۳	نمونه ای از آسیب پذیری در win XP sp2
۸۴	نحوه ی تشخیص سیستم عامل توسط کرم
۸۶	نتیجه گیری
۸۷	- حملاتی که شبکه ی ما را مورد هدف قرار می دهد
۸۷	نقش عوامل انسانی در امنیت شبکه های کامپیوتری
۹۷	لیست تمامی سرویس های فعال بر روی پورت های ویندوزی و لینوکسی
۱۲۵	انواع حملات در شبکه های کامپیوتری
۱۲۵	مقدمه
۱۲۶	وظیفه یک سرویس دهنده
۱۲۷	سرویس های حیاتی و مورد نیاز
۱۲۸	مشخص نمودن پروتکل های مورد نیاز
۱۲۹	مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری
۱۳۰	حملات (Attacks)
۱۳۱	حملات از نوع DOS
۱۳۴	حملات از نوع Back Door
۱۳۶	Spoofing
۱۳۶	Man in the Middle
۱۳۶	Replay
۱۳۶	TCP/IP Hijacking
۱۳۶	DOS Denial of Service و DDOS Distributed Denial of Service
۱۳۷	DNS Poisoning
۱۳۷	Social Engineering
۱۳۷	Birthday
۱۳۷	Brute force
۱۳۷	Dictionary
۱۳۸	Software Exploitation
۱۳۸	War Dialing
۱۳۸	SYN flood
۱۳۸	Smurfing
۱۳۸	Sniffing
۱۳۸	Ping of Death
۱۳۹	پویش پورت
۱۳۹	حملات قطعه قطعه کردن (Fragmentation Attack)
۱۳۹	Buffer Overflow Exploits (سرریزی بافر)
۱۴۰	دستکاری پارامترهای cgi-bin
۱۴۰	دستکاری فیلد های مخفی در فرمهای شما

۱۴۰	نمایش دایرکتوری ها
۱۴۱	دستکاری Cookies/Session
۱۴۱	نفوذ به وسیله پسورد ها و ACL های ضعیف
۱۴۲	Cross-site Scripting (XSS)
۱۴۲	تزریق دستورات به سرور
۱۴۳	تزریق SQL (SQL Injection)
۱۴۳	جمع آوری داده حساس توسط عدم کنترل خطاها
۱۴۳	ضعف های موجود در پیکربندی سرور
۱۴۴	Zero-Day Exploits

مشکلات رایج

	- عیب نسبی روش های رمزنگاری اطلاعات
۱۴۵	مقدمه
۱۴۵	MD5 چیست؟
۱۴۶	روش های رایج کرک کردن هش های MD5

تأمین امنیت فیزیکی

۱۵۰	- نقش عوامل ساختمانی در امنیت مراکز داده
۱۵۰	مقدمه
۱۵۳	اقدامات ضروری برای ایجاد یک Data Center
۱۵۳	عوامل مورد بررسی در مکانیابی
۱۵۴	عوامل مورد بررسی در طراحی معماری
۱۵۵	- تهدیدات مراکز داده در زمان بحران
۱۵۵	بمب الکترو مغناطیسی (EMP)
۱۵۶	- استحکامات و سازه های امن
۱۵۷	مشخصات اجرایی
۱۶۰	حداقل ضوابط مقاومت در برابر آتش
۱۶۱	- بررسی سیستم های تأسیسات الکتریکی مرکز داده
۱۶۵	- بررسی سیستم های تأسیسات مکانیکی مراکز داده

۱۷۳	منابع
-----	-------

پیوست ها

۱۷۶	پیوست یک : مقایسه ی اجمالی لینوکس و ویندوز :: پیش به سوی Open Source
۱۸۱	پیوست دو : امنیت در نرم افزارها ، گذشته ، حال و آینده

مقدمه :

شهر الکترونیکی، واژه ای که امروزه آن را زیاد می شویم ولی به اندازه ی وسعتش در مورد آن فکر نکرده ایم. همان طور که از این کلمه آشکار است، این شهر از نهاد ها و واحد های بسیاری تشکیل شده است که وقتی ما می توانیم آن را شهر الکترونیکی خطاب کنیم که همه ی واحد های درون آن اعم از بانک، بیمارستان، پلیس و ... به صورت الکترونیکی فعالیت کنند و بخش زیادی از الکترونیکی فعالیت کردن شامل تعامل به صورت الکترونیکی با مردم (ارباب رجوع) است که یک سازمان الکترونیکی باید بتواند به درستی آن را انجام دهد.

در دنیای فناوری اطلاعات؛ تمامی دستاوردهای موجود بدون داشتن امنیت لازم هیچ ارزشی ندارد. پس امنیت حرف اول را می زند زیرا یک سیستم هر چقدر هم که سریع و بهینه باشد و به ما در پیاده سازی بخش های شهر الکترونیکی کمک کند ولی ایمن نباشد هیچ ارزشی ندارد زیرا هیچ کسی مایل نیست که با استفاده از برنامه ای یا سیستمی، اطلاعاتش در دسترس دیگران قرار گیرد. گرچه رسیدن به امنیت هیچ گاه صد درصد نیست ولی با روش هایی می توان این درصد را به صد نزدیک تر کرد.