





موسسه آموزش عالی علوم و فناوری سپاهان

گروه فناوری اطلاعات

گزارش پژوهه 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 کامپیوترا صورت می پذیرد و موارد کاربرد هر کدام مورد بررسی قرار می گیرد سپس با در نظر گرفتن واحد های موجود در یک شهر الکترونیکی از قبیل دیبرستان 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 آن ها نیز توضیح داده می شود.بنابراین می توان با اطلاع داشتن از انواع حملات و راه های جلوگیری از آن ها،امنیت یک شهر الکترونیکی را افزایش داد.

تشکر و قدر دانی :

لازم می دانم که از زحمات استاد محترم،سرور گرامی ،جناب آفای 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 بندۀ 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 مطالعه‌ی پایان نامه‌ی بندۀ،منت را برابر این شاگرد کوچک خود تمام کرده و یاد و نامشان تا ابد در حافظه‌ی بندۀ باقی است.از خداوند برای ایشان و سایر اساتیدی که در طول دوره‌ی کارشناسی زحمتی در جهت آموزش بندۀ مقبول 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 پژوهشکی از راه دور
۷	کاربرد اصلی پژوهشکی از راه دور
۸	انواع پژوهشکی از راه دور
۹	جراحی از راه دور
۱۰	اولین جراحی از راه دور فرآیناده در جهان
۱۱	روش Robotic
۱۲	اولین بیمارستان مجازی در جهان
۱۳	- دانشگاه الکترونیکی (مجازی)
	آموزش الکترونیکی چیست
	- بانکداری الکترونیک
۱۷	بانک داری الکترونیکی چیست و چالش های پیش روی بانکداری الکترونیک در ایران
۱۷	جایگاه تجارت الکترونیک
۱۷	تعريف تجارت الکترونیک
۱۸	تعريف بانکداری الکترونیک
۲۰	سرویس های بانک الکترونیک
۲۰	شاخه های بانکداری الکترونیک
۲۱	مزایای بانکداری الکترونیک
۲۳	پول الکترونیکی یا پول دیجیتالی
۲۵	پول الکترونیکی و ویژگی های آن
۲۷	پیامدهای اقتصادی گسترش استفاده از پول الکترونیکی
	روش های نفوذ
	- حملاتی که وبسایت ما را مورد هدف قرار می دهد
۳۰	Tzotzic دستورات SQL
۳۱	SQL Injection چیست؟
۳۲	چگونگی تشخیص
	راه های مقابله
۳۳	به روز باشید
۳۴	رمز نگاری

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

۸۳	نمونه ای از آسیب پذیری در win XP sp2
۸۴	نحوه‌ی تشخیص سیستم عامل توسط کرم
۸۶	نتیجه‌گیری
۸۷	حملاتی که شبکه‌ی ما را مورد هدف قرار می‌دهد -
۸۷	نقش عوامل انسانی در امنیت شبکه‌های کامپیوتری
۹۷	لیست تمامی سرویس‌های فعال بر روی پورت‌های ویندوزی و لینوکسی
۱۲۵	انواع حملات در شبکه‌های کامپیوتری
۱۲۵	مقدمه
۱۲۶	وظیفه یک سرویس دهنده
۱۲۷	سرویس‌های حیاتی و موردنیاز
۱۲۸	مشخص نمودن پروتکل‌های مورد نیاز
۱۲۹	مزایای غیرفعال نمودن پروتکل‌ها و سرویس‌های 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	(DDOS) Distributed Denial of Service و (DOS) 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	پوشش پورت
۱۳۹	حملات قطعه قطعه کردن (Fragmentation Attack)
۱۳۹	Buffer Overflow Exploits (سریزی بافر)
۱۴۰	دستکاری پارامترهای cgi-bin
۱۴۰	دستکاری فیلد‌های مخفی در فرم‌های شما

۱۴۰	نمایش دایرکتوری ها
۱۴۱	Dستکاری 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 خطها
۱۴۳	ضعف های موجود در پیکربندی سرور
۱۴۴	Zero-Day Exploits

مشکلات رایج

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

تامین امنیت فیزیکی

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

۱۷۳	منابع
-----	-------

پیوست ها

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

شهر الکترونیکی، واژه ای که امروزه آن را زیاد می شویم ولی به اندازه‌ی وسعتش در مورد آن فکر نکرده‌ایم. همان طور که از این کلمه آشکار است، این شهر از نهادها و واحدهای بسیاری تشکیل شده است که وقتی ما می توانیم آن را شهر الکترونیکی خطاب کنیم که همه‌ی واحدهای 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 بخش‌های شهر الکترونیکی کمک کند ولی این نباشد هیچ ارزشی ندارد زیرا هیچ کسی مایل نیست که با استفاده از برنامه‌ای یا سیستمی، اطلاعاتش در دسترس دیگران قرار گیرد. گرچه رسیدن به امنیت هیچ گاه صد درصد نیست ولی با روش‌هایی می توان این درصد را به صد نزدیک تر کرد.