###### 28

###### آزاد.jpeg

###### دانشگاه آزاد اسلامي

###### واحد تهران مرکز

**موضوع:**

**امنیت در اینترنت با نگاهي به هكرها و شيوه عملكردشان**

**فهرست مطالب**

**فصل اول :نگاهي به هكرها و شيوه عملكردشان**

**مقدمه**

هكر به چه معناست

اهداف هكر

روشهاي نفوذ هكرها

اصول ابتدايي براي گريز از كرك شدن

استفاده از FAKE PAGE ها

مهندسي اجتماعي چيست؟

ترو جان ها

تكنيكهاي انتخاب كلمه عبور

استاندارد 17799ISO

فيشينگ Phishing چيست؟

مشخصات مشترك بين فيشينگ و ايميل

قوانين مواجهه با عمليات فيشينگ

روشهاي معمول حمله به كامپيوترها

برنامه هاي اسب تراوا

اسكريتيهاي Cross-site

ايميلهاي جعلي

پسوردهاي مخفي فايل

حملات Pharming چيست؟

بررسي زيناي واقعي

ديواره آتش Fire walls

**فصل دوم : به كارگيري اصول امنيت**

**مقدمه**

امنيت به عنوان يك زيربنا

امنيت فراتر از يك كلمه رمز

اول خطرات سطح بالا و مهمتر را برطرف نماييد.

امنيت به عنوان يك محدوديت

تهاجم DDOS چيست؟

تهاجمات مصرف منبع

كالبد شكافي يك تهاجم سيل SYN

كالبد شكافي يك تهاجم DDOS

ابزارهاي مهاجمين براي انجام خدمات DDOS

روشهاي اساسي حفاظت

فيلترسازي ورودي و خروجي

محكم كردن پپكربنديهاي ديوار آتش

اجراي يك مرور كننده (Scanner) آسيب پذيري

مقايسه قابليت هاي امنيت سرور وب

تصديق (Authentication)

كلمات عبور

گواهي نامه ها و امضاهاي ديجيتالي

به كارگيري برنامه هاي كاربردي CGI

IIS

پورت ها، سرويس ها و اجزاء بلا استفاده را غير فعال كنيد.

اسكريپت ها و فايل هاي غير لازم را پاك كنيد

هك كردن كلمه عبور و ابزار تجزيه و تحليل

**فصل سوم: متدولوژي هك كردن**

* مقدمه

درك سطوح و شرايط

* خلاصه ي تاريخچه ي هك كردن

1. سيستم هك كردن تلفن
2. سيستم هك كردن كامپيوتر

* عوامل تحريك هكرها چيست؟

1. عوامل غير اخلاقي محرك هكرهاي بدانديش
2. كاركردن با حرفه اي ها عرصه ي امنيت داده ها
3. كم كردن مشكلاتي با به خدمت گرفتن سيستم امنيتي

* شناخت انواع حملات در سيستم هاي موجود
* Dos/ DDos
* ويروسهاي هك كننده
* اسب تروآ
* كرمها
* برنامه هاي ولگرد
* دزدي كردن

1. دزدان كارتهاي اعتباري
2. دزدان موجوديها (هويت)
3. در خلال و راه زنان اطلاعات

* درك شيوه ي سيستم پيشگيري كننده امنيتي برنامه هاي كاربردي و تهديدات آن

1. اخلالهاي پنهان
2. پارامترهاي جعلي و پنهان
3. برش ابتدايي
4. پر شدن و سرريز بافر
5. شيريني زهرآلود

- جلوگيري از هك شدن با روش فكر كردن مثل يك هك كننده

**فصل چهارم : چگونه از تبديل شدن به يك برنامه نويس سطح پايين جلوگيري كنيم.**

**مقدمه**

برنامه نويسان ايجاد كننده‌ي كدهاي بي ارزش كيستند؟

از قانون تبعيت كنيم.

وقتي برنامه نويسي مي كنيم خلاقيت داشته باشيم

اجازه‌ي فكر كردن به خود بدهيد.

برنامه هاي ماژولار درست تر كار مي كند.

ساخت كد در فضاي تهي

ساخت برنامه هاي معين و قابل اجرا و ايجاد امنيت داده ها

در آخر بدانيد برنامه ي كه من قابل اجراست!

بجنبيد و برنامه هايتان را امن و قابل اجرا كنيد.

**فصل پنجم درك رابطه خطرها با mibile code**

مقدمه

تشخيص ضربه حملات Mobile code

ماكروها و اسكريپتهاي خرابكار

زبانهاي ماكرو (VBA)

مشكلات امنيتي با VBA

ويروس melisa

حملات در برابر ويروسهاي WBA

Javascript

امنيت در Javascript

جاوااسكريپت و مشكلتي كه پديد مي آورند

مشكلات امنيتي

حملات web-bused Email

بازنگري مهندسي اجتماعي (Social engineering)

پايين آوردن خطرات امنيتي Javascript

VBscrpt

امنيت در VBscrpt

مشكلات امنيت در VBscrpt

پيشگيريهاي امنيتي VBscrpt

برنامه هاي كاربري جاوا

مشكلات امنيتي در java

نگاهي به كنترلهاي Activex

مشكلات امنيتي با Activex

اشتباه در انتقال و جايگزيني كاراكترها

غيرفعال كردن كنترلهاي Activex

متعلقات ايميل

برنامه هاي امنيتي

كشف كنننده هاي حفره ها

نرم افزار فايروار

**فصل ششم ايمن كردن كدهاي جاوا**

**مقدمه**

جلوگيري از مشكلات ناشي از جاوا ، جاوا اسكريپت و Active x

برنامه نويسي اسكريپ هاي ايمن

سياست امنيت چيست

ارزش در برابر ريسك

سياست امنيت مي بايست شامل چه عناصر باشد

هجومهاي دسترسي به فايل

تهاجمات اطلاعات غلط

هجوم هاي دسترسي به فايل / بانك اطلاعاتي ويژه

**مقدمه**

امنيت در دنياي واقعي ما امري اجتناب ناپذير است و همگي‌مان به نوعي سعي داريم تا امنيت را در محيط پيرامونمان ايجاد كنيم. همانطور كه شما براي ساختمان خود چندين كليد تعبيه مي كنيد، از ابزارهاي امنيتي براي كنترل ورود و خروج استفاده مي كنيد و حتي در سطح ابتدايي از حدود افراد ناشناس به حيطه ي منزل خود جلوگيري مي‌كنيد، نشان مي دهد كه شما به امنيت محيط زندگي خود اهميت مي دهيد. در دنياي واقعي تضمين امنيت امري مهم، مشكل و سخت مي باشد. همچنين هزينه ي بالاي اين ضمانت نيز قابل توجه است. براي مثال بسياري از پروژه ها با هزينه اي معلوم ساخته مي شود ولي براي اخذ مدرك و جهاني شدن بايد هزينه اي معادل چند ده برابر هزينه ي ساخت پروژه خرج شود تا صحت و امنيت سيستم مورد تأييد قرار گيرد. در دنياي پيچيده ي مجازي اينترنت امنيت نمودي ديگر دارد، اين تفاوت مي تواند بيان كننده ي پيچيدگي خاص اين سطح از امنيت دارد. براي مثال اگر شما سايتي در اينترنت به صورت فعال داشته باشيد و هزينه ي زيادي براي طراحي و پياده سازي برنامه ي كاربردي خود خرج كرده باشيد، بسيار متعجب خواهيد شد اگر ببينيد كه سايت شما مورد حمله قرار گرفته و تقريباً تخريب شده است. اين حمله بسيار سخت و غير قابل درك است. اين امر در مورد سايت هاي تجاري و يا بانك هاي اعتباري الكترونيكي بسيار خطرناك است. چرا كه با حمله‌اي به اين سيستم احتمال خاش شدن اطلاعات حساب هزاران نقد وجود دارد. پس اين سطح از امنيت بسيار مهم و حياتي مي نمايد و اگر شما نتوانيد تصوير قابل قبول و مطمئني از سايت خود ايجاد كنيد آنگاه يا تمامي مشتريان خود را از دست خواهيد داد و تجارت الكترونيك شما نابودي شود يا اينكه اطلاعات مشتريان فاش شده تبعات قانوني اين اقدام، اعم از شكايات مشتريان دامن شما و شركت شما را مي‌گيرد. به همين علت ايجاد يك ساختار ايمن سخت افزاري و نرم افزاري و فيزيكي تجهيزات شما يكي از واجبات ساخت يك برنامه‌ي كاربردي موثر در سطح شبكه است. اين پروژه كه در پيش روي داريد شما را با انواع تهاجمات و حملات به سايت هاي مختلف و طرق نفوذ به برنامه‌هاي كاربردي آشنا مي كند. به صورت خلاصه با انواع ابزارهاي خاص حمله اعم از ويروس ها، كرم ها، برنامه هاي ولگرد، تكنيك اسب تروا آشنا مي كند. در ادامه به بررسي چگونگي حملات معروف در طول تاريخ شبكه مي پردازيم، دزدان كارتهاي اعتباري را از حيث عملكرد با بقيه ي هكرها مقايسه مي كنيم و تكنيك هاي جلوگيري از هك شدن را آموزش مي دهيم.

در انتها مي توانيد با مروري هر چند اجمالي بر چند برنامه ي كاربردي با دنياي واقعي برنامه نويسي شبكه آشنا شويد.

اين مرور به شما كمك مي كند تا ديدتان را در مورد امنيت (Security) و قابليت اجرايي (Functionality) تصحيح كنيد و بتوانيد برنامه ي خود را ايمن كنيد. به كمك اين قسمت از پروژه اهميت تست امنيت داده را خواهيد فهميد و آن را در ابتداي اهداف خود خواهيد گنجانيد. نكته ي جالب در فصول بعد بيان اصول امنيت داده، فهميد و آن را در ابتداي اهداف خود خواهيد گنجانيد. نكته ي جالب در فصول بعد بيان اصول امنيت داده، تحليل امنيت، و به طور كلي دانستن معناي واقعي امنيت داده مي باشد. حملات به برنامه هاي خاص از راه دور نيز جزء فصول مطرح شده مي باشد. در اين بخش به تحليل Script هاي از خانواده ي زبانهاي معروفي چون java و Perl و ... نيز مي‌پردازيم. بيان مفهوم Active X نيز از قلم ها خارج نشده است و تحليل سياست‌هاي كلي تعيين امن و ناامن بودن برنامه اي نيز از اهداف انتهايي اين پروژه است. در ضمن يادآور مي شويم كه در طرح و بررسي اين پروژه از منابع ديگري نيز استفاده شده است. مي توان از وبلاگ هاي مختلف كه يادداشتهاي گاهاً، موثر و با ارزش كه نويسان حرفه اي را نيز در بر مي گرفته نام برد. همچنين سايتهايي كه اطلاعاتي هر چند جزئي و مقدماتي نيز در اختيار ما گذارده اند نيز جزء منابع خاص ما مي باشند. در كل در اين حوزه اطلاعات سطح شبكه‌ي جهاني اينترنت بسيار محدود مي باشد و به جز چند سايت برجسته كه حتي هزينه هايي را نيز طلب مي كردند، ديگر سايت خاصي با اطلاعات مناسب براي تنظيم و تهيه‌ي يك پروژه‌ي علمي و كاملاً حرفه اي، وجود نداشت و به همين علت منبع اصلي ما در اين پروژه كتاب تعيين شده‌ي Hack Proofing مي باشد كه جزء ارزنده ترين كتب در اين سطح مي‌باشد. در خاتمه اين پروژه را به تمامي انديشمندان عرصه‌ي علوم كامپيوتر و جامعه‌ي علمي كشور و تمامي كساني كه به فنون اينترنت و كامپيوتر علاقه مند هستند تقديم مي كنيم باشد كه قدمي هر چند كوچك در ارتقاي آگاهي علمي و فني دانشجويان برداشته باشيم. همچنين همانطور كه هيچ موجودي در جهان هستي خالي از خطا و اشتباه نيست ما نيز از اين قاعده‌ي جهان شمول مبرّا و مجزا نيستيم، اگر اشتباه و قصوري در طرز نگارش و مطالب علمي مشاهده كرديد از اينكه به آدرس Email تهيه كنندگان تماس بگيريد بسيار خشنود مي‌شويم و در تصحيح خطاي خود تلاش خواهيم كرد. باشد كه هيچگاه چراغ پر فروغ علم و ادب در سرزمين پارس خاموش نشود و هر روز با گذر از ايام پرده هاي نابخردي و ناداني يكي يكي از پس هم كنار رفته و ما را به سمت روشنايي مطلق باري تعالي هدايت نمايد.

در آخر از استاد محترم و ساعي خود جناب مهندس خاكي كمال تشكر و قدرداني را داشته و براي توفيق روزافزون اشيان دعا مي‌كنيم. همچنين از تمامي اساتيد محترم دانشگاه كه در رسانيدن ما به سرمنزل مقصود علم و آگاهي از هيچ تلاشي دريغ نكردند كمال تشكر را داريم.