به نام خدا

اصطلاحات هک

ارتش سایبری امام مهدی (عج)

تحولی در فضای مجازی برای امام زمان (عج)

ایدی اینستاگرام:

IRAN_CYBER_ARMY

ایدی لاین :

UPV5449Z

به نام خدا

ارتش سایبری امام مهدی (عج) وابسته به بسیج دانشجویی دانشگاه علم و صنعت ایران تقدیم میکند.

این جزوه حاوی مطالب مفیدی و کاملی برای آموزش هک به صورت مبتدی بوده و با یاد گرفتن این اصطلاحات میتوانید از دیگر اموزش هایی که در پیج قرار خواهد گرفت استفاده نمایید ان شا الله.

IP :

ای پی :

ببینید دوستان هر یک از ما در دنیای واقعی یک اسمی داریم . مثلا من اسمم امیر هست و شما اسم مخصوص به خودتون دارین تا بتونین شناسایی بشین. و برای این کار در نیای مجازی و اینترنت برای شما یک ای پی در نظر گرفتن که مخفف Internet Protcolهست.

و دو نوع داره که یک نوع ۴ (ورژن ۴) و نوع ۶ (ورژن ۶).

برای مشاهده ای پی خودتون کافیه در گوگل عبارت " my ip " رو جستجو کنید. این ای پی در هر بار اتصال شما به اینترنت تغییر میکنه.(در بعضی موارد هکر نیاز

داره بـرای حفـظ دسترسـی از هـدف ای پـی ثـابتی داشـته باشـه کـه بـا روجـوع بـه سیسـتم ارائه دهنده اینترنت میتونه ای پی استاتیک یا ثابت با پرداخت پول دریافت کنه).

و یـا اینکـه بـرای مشـاهده لیسـت کـاملی از IPv6 , IPv4 میتونیـد در cmd ویـنـدزو عبارت , " ipconfig " و در ترمینال لینوکس عبارت " ifconfig " رو اجرا کنید.

Port :

پورت :

پـورت هـا درگـاه هـایی هسـتند بـرای انتقـال اطلاعـات. هـر وبسـایت کـه داریـن میبینیـد توسـط پـورت بـه سیسـتم شـما اورده شـده و شـما میتونیـد محتویـات ایـن صـفحه رو بخونیـد. پـورت هـا در دونـوع فیزیکـی و مجـازی هسـتند. پـورت هـای فیزیکـی مثـل , USB HDMIکـه میتونیـد در کنـار لـب تـاپ یـا پشـت کـیس کـامپیوتر خودتـون انـواع مختلفـی از اونـا رو ببنییـد ولـی پـورت هـای مجـازی رو نمیشـه دیـد و هکـر از هـر دو نـوع ایـن پـورت های برای دزدیدن اطلاعات استفاده میکنه .

server :

سرور :

بـه کـامپیوتری کـه بـه شـما سـرویس بـده مـیگن سـرور. هـر وبسـایتی کـه شـما بهـش سـر میزنیـد توسـط یـک سـرور پشـتیبانی میشـه کـه اگـه یـه سـایت رو بشـه هـک کـرد میشـه بـه تمـامی سـایت هـایی کـه روی اون سـرور هسـت نفـوذ کـرد و بـه ایـن کـار symlink گفتـه میشه.

client :

کلایت :

سیسـتم هـایی کـه از سـرور خـدمات دریافـت میکـنن رو کلاینـت مـیگن. شـما یـک کلایـت هستید .

Deface

:دیفیس :

تغییر چهره دادن یک وبسایت یا یک سیستم شخصی رو دیفیس میگن. بعضی از هکر ها زمانی که به وبساتی نفوذ کنن برای اثبات هک خودشون میتونند اون وبسایت رو دیفیس کرده و در سایت های بین المللی هک اونا رو ثبت کنن. پس از این نوع دیفیس سایت توسط مدیر اصلی قابل بازگردانی هست. ولی در بعضی از موارد که با تخلیه اطلاعاتی مواجه بشه اگه بک اپی از سایتش نداشته باشه نمیتونه سایتو برگردونه.

bug :

باگ :

اشکال، هر جایی اشکالی رخ بده بهش باگ گفته میشه. شاید شما در طی برنامه نویسی به باگ های زیادی برخورد کرده باشید و تونسته باشید این باگ ها رو رفع کرده باشید. اگه برنامه نویسی که سایت رو مینوسه در مراحل امنیتی سوتی داده باشه و هکر بتونه از اون سوتی استفاده ناصحیح کنه بهش باگ گفته میشه.

انواع باگ ها رو در ادامه به طور نسبتا کامل با هم بحث خواهیم کرد.

Admin Page :

ادمین پیج :

جایی که ادمین میتونه وارد پنل مدیریتی سایت یا سرور بشه. این صفحه خیلی حساس و قابل ملاحضه هست. اگه پیدا بشه باهاش میشه خیلی کار ها کرد که به این روش ها و روش پیدا کردن این صفحات هم میپردازیم.

Dork :

دورک :

یک سری از ادرس های خصوصی وبسایت ها توسط گوگل نگه داری میشن که اگه بشه به یعضی از اونا دسترسی پیدا کرد میشه بدون هیچ محدودتی به کل سرور دسترسی پیدا کرد یا میشه از این ادرس ها باگ یعضی سایت ها رو تشخیص داد. کاربرد بیشتر دورک ها در مثال دومی (باگ) هست. اگه توسط این دورک ها باگی از سایتی پیدا شد به این روش گوگل هکینگ گفته میشه.

Data Base :

دیتابیس :

جایی که اطلاعات هر سایتی درون اونها ذخیره میشه. اطلاعاتی از قبیل رمزهای کاربران، یوزرنیم های کاربران،(اگه بانک باشه خودتون حدس بزنید :دی).

هکرها سعی بر این دارند که به دیتابیس نفوذ کرده و از اطلاعات لذیذی که در دیتابیس ذخیره شدن تغذیه کنن.

Target :

تارگت :

به هر چیزی که بخوایم هک کنیم تارگت گفته میشه. تارگت میتونه یک صفحه فیس بوک یا یک ایمیل یا یک دیتابیس باشه.

bypass :

بای پس :

وقتی در حین مراحل انجام کار به گره میخوریم یعنی مدیر سایت یه کارای امنیتی کرده که روش های ما جواب نمیده باید از خلاقیت خودمون استفاده کنیم و اون مرحله رو دور بزنیم. از این اصطلاح در موارد زیادی استفاده میشه. به طور مثال اگه به سیستمی نفوذ کنید و انتی ویروس رو دور بزنید به این کار شما بای پس گفته میشه که خیلی خوب سعی میکنیم بهش بپردازیم ان شا الله.

shell :

شل :

زمانی که از طریق باگ هایی که در پایین بهشون اشاره میکنیم وارد یه سایت شدین به قسمت اپلود اون سایت رفته و یه شل مخصوص خودمون اپلود میکنیم. بعد با استفاده از این فایل شل که روی سایت اپلود کردیم میتونیم به قسمت های دیگر سایت به راحتی دسترسی پیدا کنیم و یه جور یه پنل کار مدیریتی برای هکر به حساب میاد.

symlink :

سیمی لینک :

وقتی با استفاده از باگ ها به سایتی نفوذ کردیم و شل رو اپلود کردیم در این مرحله میتونیم با استفاده از شل یه سری کارهایی بکنیم که به دیگر سایت های روی سرور مورد نظر هم دسترسی پیدا کنیم.

Client Haching :

هک سیستم شخصی :

اگه شما با استفاده از روش هایی که در آینده بهتون میگم به سیستم شخصی نفوذ کنین به این کار هک سیستم شخصی گفته می شود.

keylogger :

کی لاگر :

این نوع برنامه ها برای ضبط کلید های زده شده توسط کاربر کاربرد داره و هر کلیدی که توسط کاربر زده شده رو ذخیره میکنه و برای هکر ارسال میکنه.

Fake Page :

فیک پیج :

این نوع صفحات که صفحات تقلبی اسم دارند برای دزدیدن اطلاعات کاربر هنگامی که برای کار خود به سایت مرجعی رجوع میکنه استفاده میشه. به طور مثال وقتی شما بخواین وارد حساب بانکی خودتون بشین از سایت بانک باید وارد حساب بشین و اگه هکر بیاد یک صفحه تقلبی بسازه و ظاهرش مث صفحه بانک باشه ولی اطلاعاتی که میگیره و به هکر بفرسته فیک پیج هست و خیلی خطرناک هست.

در ادامه به روش های جلوگیری از افتادن در دام فیک پیج ها در پست های بعدی خواهیم پرداخت.

root :

روت :

کاربر یا مدیر کل یه سیستم کامپیوتری روت نامیده میشه. مثلا همون خانمی که توی سایت داشنکده پشت اون میزه تنها نشسته روت سایت به حساب میاد و کنترل کل سیستم رو به عهده داره. سعی میکنیم درون یه سرور روت بشیم تا کارهای خاصی رو انجام بدیم.

معرفی انواع باگ ها :

SQL Injection :

یکـی از خطرنـاک تـرین و فراگیرتـرین بـاگ هـای شـناخته شـده در سـطح بـین المللـی هسـت کـه بـه زودی هـای زود هـم پچ(غیرفعـال) نخواهـد شـد. هنگـامی کـه برنامـه نـویس بـرای ارتباط سایت خود به دیتابیس خود سوتی بدهد این باگ رخ خواهد داد.

XSS	:	Cross	Site	Scripting
RFU	:	Remote	File	Upload
RFI	:	Remote	File	Include
DNN	:	Dot	Net	Nuke
LFI	:	Local	File	Include

CSRF : Cross Site Request Forgery

Brute Force :

صـفحه وبـی را در نظـر بگیریـد کـه دو بـاکس بـرای گـرفتن نـام کـاربری و رمـز عبـور دارد و در صـورت درسـت بـودن ایـن دو مـورد میتـوان وارد آن صـفحه شـد. اگـر شـما برنامـه را بنویسـید یـا داشـته باشـید کـه تعـداد زیـادی نـام کـاربری و رمـز عبـور را پشـت سـر هـم روی ایـن صـفحه امتحـان کـرده تـا رمـز عبـور و نـام کـاربری اصـلی را پیـدا کنـد بـه ایـن روت بـورت

فـورس گفتـه میشـود. ایـن روش کـاربر هـای بسـیار زیـادی دارد از جملـه در ادمـین پـیج هـا، حساب های یاهو ، فیس بوک،و... ایمیل ها و...

Scanner :

کسـی کـه یـک سیسـتم را مـورد بررسـی قـرار میدهـد تـا بـاگ هـا یـا خطاهـایی کـه باعـث میشـود بتـوان از ایـن بـاگ هـا اسـتفاده کـرد را اسـکنر میگوینـد. اسـکنرها یـا انسـان هسـتند یـا نـرم افـزار. البتـه انسـان هـا بـا نـرم افـزار هـا موفـق بـه ایـن کـار مـی شـوند. نـرم افـزار هـای مختلفی برای هک وجود داد که در آینده به آنها خواهیم پرداخت.

Exploit : اکسـپلویت : نـوعی کـد مخـرب کـه توسـط هکـر هـا نوشـته مـی شـود بـرای سـوء اسـتفاده از حفـره هـای امنیتـی . معمـولا ایـن کـد هـا بـا C++ یـا perl , Python و php نوشته می شوند که در معرفی متااسپلویت به آنها بیشتر خواهیم پرداخت.

از اکسپلویت ها در سیستم های عامل ، وب سرور ها، شبکه ها و .... استفاده می شود.

dDos :

مخفـف کلمـه denial of service یـا تکـذیب سـرویس میباشـند. هنگـامی کـه سـرور توانـای پـردازش یـک درخواسـت از طـرف هـر کلاینـت را دارد ، اگـر در یـک لحظـه ۴۰ میلیـون درخواسـت بـه سـمت سـرور بـرود چـه بـه روز سـرور خواهـد آمـد؟ بـه ایـن کـار dDos گفته می شود.

Back Track :

سیسـتم عامـل محبـوب هکـر هـا کـه اپـدیت شـده بـه . Kali Linux ایـن سیسـتم عامـل تحـت لینـوکس مـی باشـد و هـر نـوع ابـزاری بـرای هـک هـر نـوع سیسـتم نـرم افـزاری را بـرای شما فراهم آورده است.

به بک ترک و کالی بسیاز حرفه ای خواهیم پرداخت.

Metasploit :

این نرم افزار که به چاقوی سویسی معروف است شما را قادر میکند که هر چیزی را که فکر میکنید هک کنید. این نرم افزار ابزار های زیادی را فراهم کرده که البته کار با ان نیز بسیار ساده در عین حال هوشمندانه و قدرتمند است. فیلم اموزش کار با این ابزار در وبلاگ نیز موجود است. برای مشاهده مطلب اینجا را کلیک کنید.

CMS : Content Manage System :

سیستم مدیریت محتوا . برای مدیریت محتوای یک وبسایت به کار میرود که انواع بسیار مختلفی دارد که شما نیز میتوانید این سیستم را برای خود طراحی کنید. از معروف ترین سی ام اس ها وردپرس، جوملا، وبیولیتن و .... است.

این بود اصطلاحات ابتدایی و پشرفته ای که نیاز به راه افتادن در مسیر هک و هکر شدن نیاز دارید.

ان شا الله از تابستان به لطف الهی و عنایت امام زمان(عج) اموزش های نفوذ رو شروع خواهیم کرد.

برای دریافت اموزش های دیگر به پیج ما در لاین مراجعه نمایید. ایدی پیج در صفحه اول این کتاب موجود است.

برای سلامتی و تعجیل در فرج امام مهدی(عج) صلواتی با توجه کامل ارسال نمایید.

ارتش سایبری امام مهدی(عج).

خرداد ۹۴.

و من الله التوفیق

خداحافظ