جامع صورت به سایت هک آموزش

آشیانه امنیتی گروه

آشنا مقدماتی صورت به ها سایت به نفوذ ی نحوه با را شما ما مقاله این در
به دستیابی برای شما و میشود تقسیم مختلفی جلسات و ها بخش به مقاله . میکنیم
.کنید دانلود آنجا از و شوید آشیانه سایت وارد میتوانید ها مقاله سایر

نویسنده :
SolD!3r

به نام خدا

جلسه ی اول.

در این جلسه سعی بر این داریم که شما رو با اصطلاحات هکینگ آشنا کنیم . خب شروع میکنیم :

1 . تارگت : در لغت به معنای هدف و واحد است . بر فرض مثال شما زمانی سایتی برای نفوذ در نظر دارید . به اصطلاح به این هدف شما تارگت گفته میشود.

2. باگ : باگ ها یا حفرات امنیتی یا خرابی های امنیتی گفته میشود . این خرابی ها از اشکالات و سهلنگاری های برنامه نویسان

وب و صفحات وب است. که فرد نفوذ گر این این خرابی ها به نفع خود برای هر نوع هدفی استفاده میکند. زمیمه ی نفوذ به باگ

همین باگ ها و خرابی ها هستند.

3. دیفیس : در کل به معنای تغیر ظاهری سایت یا یک صفحه است. برای درک بهتر زمانی که شما تارگت مورد نظر رو هک

میکنید برای اثبات هک خود یا هر چیزه دیگه صفه های سایت (میتونه صفحه اول یا صفحات دیگه) رو تغیر میدید . به اصطلاح

به این عمل شما میگن دیفیس کردن. یعنی شما سایت رو دیفیس یا همون هک کردید.

4. : بایپس : به معنای دور زدن یا همان میانبر است . گاهی اوقات در زمانی که شما در حال هک کردن تارگتی هستید برخی از

دستورات اجرا نمیشن حالا میتونه به خاطر ابزارهای امنیتی سایت باشد یا هر چیز دیگه. حال ما برای ادامه دادن به کار خود با

مشکل مواجح میشیم پس میایم به کمک انواع روش ها این دستورات رو یه جوری وارد و ابزارها رو دور میزنیم. به این کار ما

بایپس کردن میگن.

5. اکسپلویت : کدهای مخربی هستند که بنا به نیاز نفوذگر نوشته میشوند (البته همشون مخرب نیستند).

6. فیک پیج : بعضی از هکرها صفحه ایی مانند صفحه ی ورود به سایت طراحی میکنند. این صفحه ها مانند بقیه ی صفحات

اینترنتی هستند ولی فرق اینها در کد نویسیشونه . که اکثرا کد نویسی ها به صورتی است که وقتی قربانی یوزرنیم و پسورد

خود را وارد این صفحه میکند یوزرنیم و پسورد برای هکر ارسال میشود. البته این نوع حمله بیشتر برای هک ایمیل ها و اکانت

های مختلف استفاده میشود . ولی از این روش هم میشه برای هک سایت استفاده کرد.

7. دورک ها : دورک ها سری کدهایی هستند که فرد برای جستوی سریع و دقیق تردر موتور های جستجو گر از آن استفاده میکند.

8. : گوگل هکینگ : ساده ترین تعریفی که به ذهنم رسید : استفاده از گوگل جهت هک را گوگل هکینگ میگویند.

9. هش ها : هش ها یه جور الگوریتم و روش های کد گذاری و رمزگذاری متن هاست. که مدل هایی از جمله :

MD5 – SHA – MySQL – Wordpress …..

10. کرک : در کل به معنای شکست و نفوذ است . که این نفوذ میتونه به برنامه ها باشه و این شکستن میتونه شکستن پسوردها و متن

های رمزنگاری شده باشه.

11. پچ : به معنای جایگزین و درست کردن چیزی گفته میشه مثل پیچ کردن باگ ها ....

12 . هگز : یک نوع الگوریتم رمزنگاری است.

13 . پورت : یه سری درگاه های اتصال و انتقال میاشد.

14. اف تی پی : اف تی پی یا پورت 21 که مخفف است یعنی پروتکل انتقال فایل. این پورت برای انتقال فایل به کار میره

و این انتقال در دوجهت آپلود و دانلود انجام میشه. خب زیاد وارد این بحث نیمیشم تا همین تعریف بسند میکنه.

با تشکر :

SolD!3r

پایان جلسه ی اول.