گروه کاربران لینوکس اصفهان تقدیم میکند ...

ارائه کننده : مهرداد عباسی

با تشکر از:

کلیه اعضای گروه کاربران لینوکس اصفهان

عنوان سمینار :

آیا لینوکس امن است!؟

عناوین سمینار :

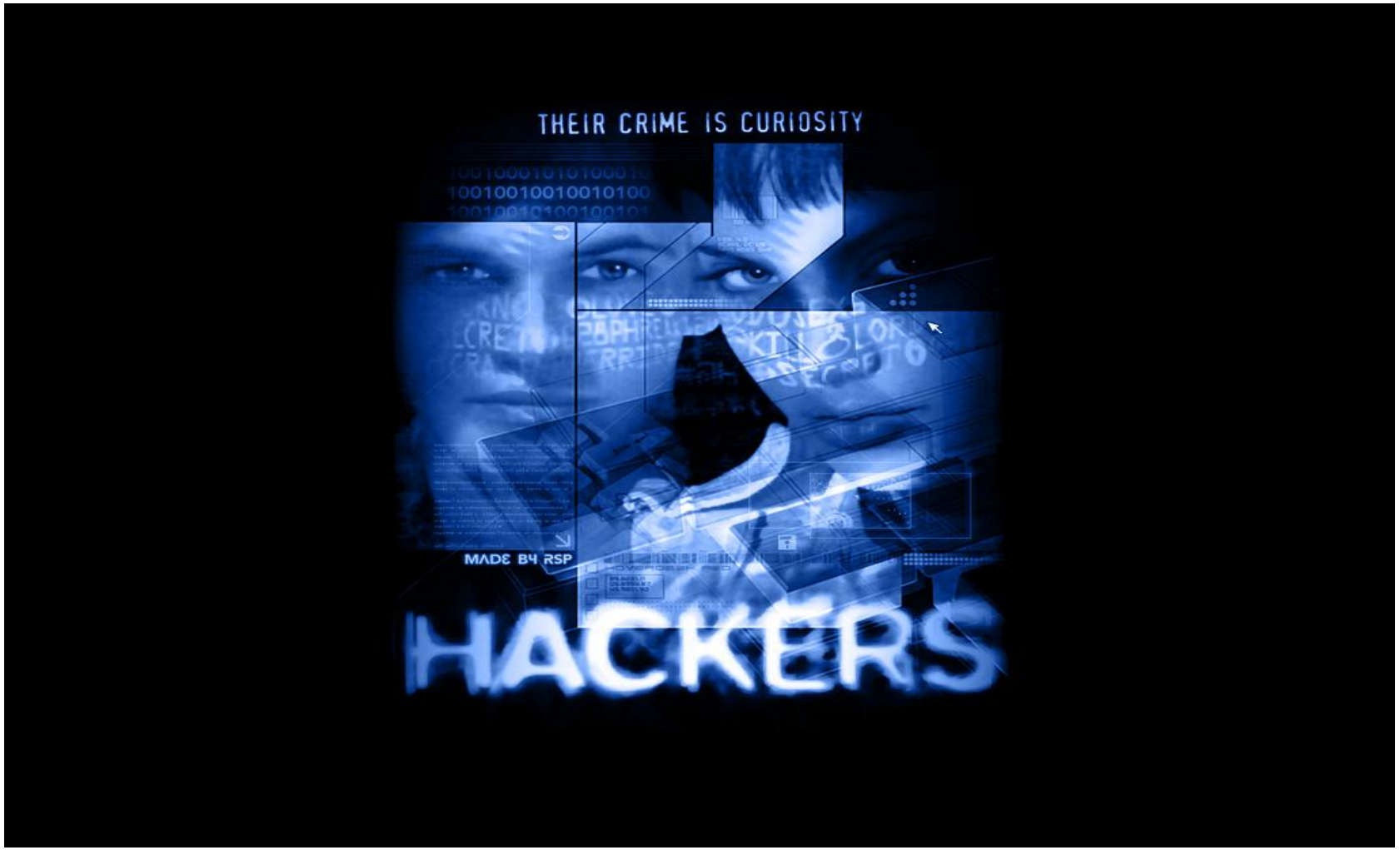
۰ از افسانه تا واقعیت هک و امنیت

۱ اصطلاحات فنی و علمی برای کاربران آماتور

۲ مروری کوتاه بر امنیت اطلاعات کامپیوتری

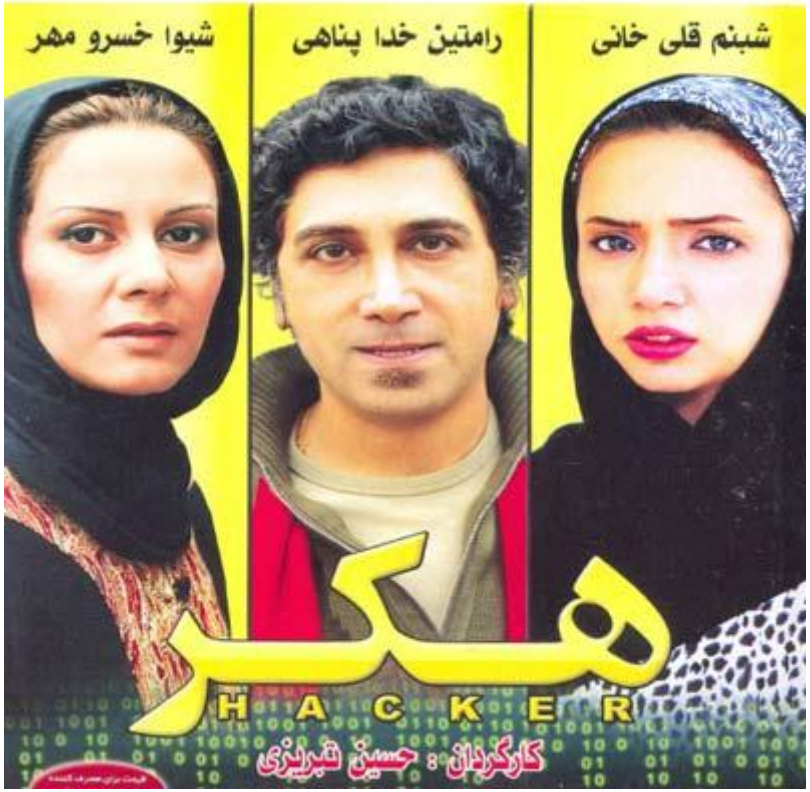
۳ امنیت سیستم عامل

از افسانه تا واقعیت هک و امنیت




THE
MATRIX


0.000742435
LIVE FREE OR
DIE HARD
WHAT IF YOU'RE HURT AND ALONE AND YOU
DIAL 911 AND NO ONE ANSWERS


شبنم قلی خانی
رامتین خدا پناهی
شیوا خسرو مهر
هکر
HACKER
کارگردان: حسین تبریزی

واقعیت		افسانه	
هک	**امنیت**	**هک**	**امنیت**
هیچ سیستمی به ذات امن نیست	امنیت هیچ گاه ۱۰۰٪ نیست ! امنیت نسبی است	هرسروری به راحتی هک میشود	۱۰۰٪ امن
سرور و سایت شما ممکن است هک شود	هر سروری ممکن است هک شود !	ما هر سرور و سایتی را هک میکنیم	سرور ما هک نشدنی است
بدون شرح !	بدون شرح !	من بزرگترین هکر دنیا هستم	من بزرگترین امنیت کار دنیا هستم
منکر سواد نیستیم ولی نه در این حد !!!	بدون شرح !	آشیانه دومین تیم بزرگ هک جهان است	سرور های آشیانه هک نشدنی است
بدون شرح !	بدون شرح !	بدون شرح !	بدون شرح !

اصطلاحات فنی و علمی برای کاربران آماتور

Hacker:

فردی که کاملا به تکنولوژی کامپیوتر وبرنامه نویسی واقف است وبا ورود غیرمجاز به سیستم ها ازطریق کدهای مخرب که بر روی سیستم عامل اجرا میکند، اقدام به سرقت اطلاعات یا تغییر یا حذف آنها میکند (Black Hat) ویا صرفا هدف از نفوذ تنها برای نشان دادن آسیب پذیری سیستم میباشد . (White Hat) اینکار میتواند بصورت انفرادی یا گروهی انجام شود

Server:

کامپیوتر سرویس دهنده

Port:

پورت دروازه ارسال یا دریافت اطلاعات میباشد.

Bug:

عمدتا به نوعی خطا در دستورات یا منطق یک بر نامه گفته میشود که باعث میشود برنامه به درستی عمل نکرده و یا نتایج نادرست تولید کند. باگها ممکن است کم اهمیت و جزیی باشند و ممکن است بسیار مخرب باشند. (یکی از راههای نفوذ وجود باگ در سیستم می باشد).

Hoax Malware Worm Spyware-Adware

به بدافزارهایی گفته میشود برای مقاصدی چون تکثیر در سیستم ها بصورت ویروس یا برنامه های به ظاهر بی ضرر که قابلیت های مضر را مخفی میکنند.

-Trojan-Backdoor:

بدافزاری که بصورت یک برنامه کاربردی یا خدماتی ویا بصورت یک بازی ویا ...ارائه میشود ولی در نهان، اقدام به خرابکاری وارسال اطلاعات حساس میکند.

مثال Lootseek.av :ویا Galapoper.a و...

Rootkits

RootKitها برنامه هایی هستند که از نظر ساختار کاری بسیار شبیه Trojan ها و Backdoor ها هستند ولی با این تفاوت که شناسایی RootKit بسیار مشکلتر از درب های پشتی است زیرا RootKit ها علاوه بر اینکه به عنوان یک برنامه کاربردی خارجی مثل شنونده Netcat بر روی سیستم اجرا می شوند بلکه جایگزین برنامه های اجرایی مهم سیستم عامل و در گاهی مواقع جایگزین خود هسته کرنل می شوند و به هکرها این اجازه را می دهند که از طریق درب پشتی و پنهان شدن در عمق سیستم عامل به آن نفوذ کنند و مدت زیادی با خیال راحت با نصب ردیابها (Sniffer) و دیگر برنامه های مانیتورینگ بر روی سیستم اطلاعاتی را که نیاز دارند بدست آورند. در دنیای هکرها دو نوع RootKit اصلی وجود دارد که هر کدام تعریف جداگانه ای دارند.

RootKitسنتی

RootKitسطح هست

Exploit:

اکسپلویتها کدهایی هستند که هکر برای سوءاستفاده از باگهای کشف شده درسیستم عاملها ویا نرم افزارهای مختلف وبیشتر به زبانهای برنامه نویسی C و Perl می نویسد.

هکربسته به نوع زبان برنامه نویسی که استفاده میکند، اکسپلویت نوشته شده را با استفاده از کمپایلرهای مخصوص به آن زبان به حالت اجرایی تبدیل میکند وعلیه آن باگ در سرویس هدف بکار میگیرد.

درواقع با اکسپلویت کد، هکر میتواند سطح دسترسی خود را از حالت محدود به سطح بالاتر نظیر سطح دسترسی Administrator ارتقاء دهد ودستورات مخرب خود را اجرا نماید.

مثلا باگ Vista Nt Raise Hard Error در فایل csrss.exe که یکی از مهم ترین فایلهای Microsoft client/server Runtime است ومربوط به پردازش Nt Raise Hard Error میباشد وباعث بارگذاری فایلهای dll در فایل csrss.exe میشود.

برای این باگ ۲ اکسپلویت کد نوشته شده که میتوان در آدرس زیر آن را مشاهده نمود:

http://www.securityfocus.com/archive/1/455365

این باگ واکسپلویتهای آن در اوایل ۲۰۰۷ درشبکه های زیرزمینی به قیمت $50.000خرید وفروش میشد وجالب اینکه این سیستم عامل از طرف ماکروسافت بعنوان یک سیستم عامل ایمن معرفی شده بود...

Privilage Escalation:

در این روش هکر با اکسپلویت کد نوشته شده برای باگ موجود در سیستم هدف، سطح دسترسی خود رااز یک کاربر معمولی به بالاترین سطح دسترسی در آن سیستم عامل یا آن

Applicationخاص به صورت غیر مجاز ارتقاء میدهد.

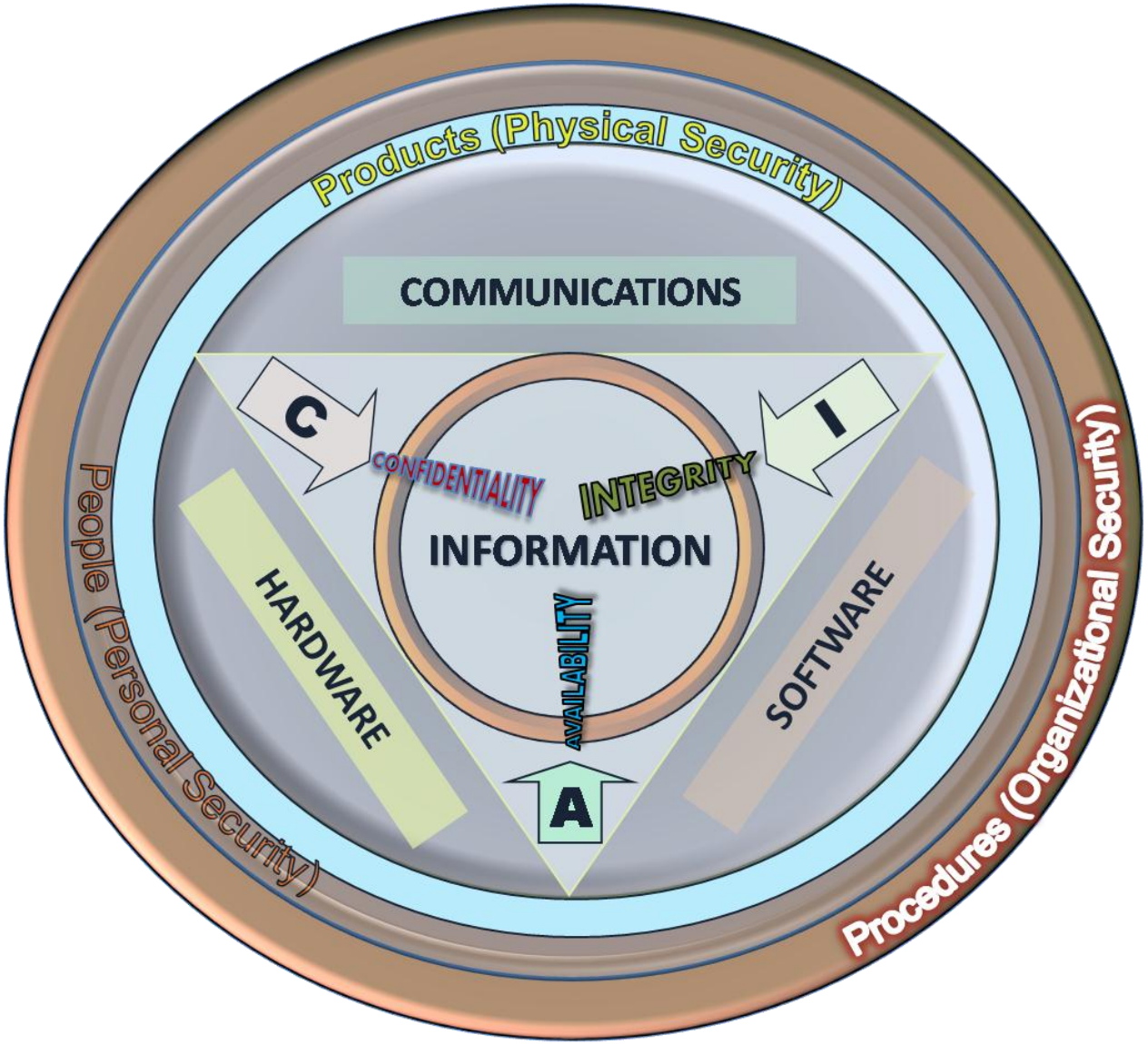
مروری کوتاه بر امنیت اطلاعات کامپیوتری

امنیت اطلاعات یعنی حفاظت از اطلاعات و سیستم های اطلاعاتی از فعالیت غیرمجاز. این فعالیت ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری

Confidentiality محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز.

Integrity یکپارچه بودن یعنی جلوگیری از تغییر داده ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات.

Availability اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند.


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
AVAILABILITY
A
People (Personal Security)
Procedures (Organizational Security)

سرویس های امنیتی

۱ – محرمانه ماندن اطاعات

۲ – احراز هویت

۳ – سلامت داده

۴ – کنترل دسترسی

۵ –در دسترس بودن

نگاهی بر امنیت سیستم عامل

امنیت نرم افزار منبع باز

بیشتر مردم می توانند امکان بازرسی کد منبع برای پیدا کردن و رفع آسیب پذیری داشته باشند

..