به نام آنکه جان را فطرت آموخت

تست نفوذ پذیری

AUTHOR : Peyman shahkar (Desperado)

Peyman.shahkar@Gmail.com
Peyman_shahkar

Virangar Under Gr0und Security Team

تقدیم به تیم امنیتی ویرانگر

تقدیم به تنها معنی بخش زندگی ام

تست نفوذ پذیری چیست؟

تست نفوذ پذیری فرآیند ارزیابی امنیتی شبکه یا سیستم های رایانه ای ، بوسیله شبیه سازی یک حمله که توسط هکر انجام می شود ، است. که معمولا با یکی از دو روش BlackBox ,White Box اجرا می شود. بعنوان مثال اگر تمرکز روی منابع رایانه باشد، مثال هایی که می تواند به تست نفوذ پذیری موفق منجر شود شامل دسترسی به اسناد محرمانه و لیست های قیمت ، پایگاهای داده و اطلاعات حفاظت شده دیگر است.

مهمترین تفاوت بین هکر و شخصی که تست نفوذپذیری انجام می دهد این است که، تست نفوذپذیری با مجوز و قراردادی که با سازمان یا شرکت امضاء شده است انجام می شود و در نهایت منجر به یک گزارش خواهد شد.هدف از تست نفوذ پذیری با لابردن امنیت داده ها توسط تست امنیتی می باشد. اطلاعات و ضعف های امنیتی که در نفوذ پذیری

مشخص می شود محرمانه تلقی شده و نباید تا برطرف شدن کامل افشاء شود. ولی در مورد هکر این رویه و روال وجود ندارد.

چرا تست نفوذپذیری انجام میشود؟

تست نفوذ پذیری در سازمان به دلایل زیر انجام می شود:

· یافتن حفره های امنیتی سیستم های مورد استفاده پیش از آنکه دیگران این حفره ها را مشخص کنند.

هکر ها از هر موقعیت زمانی و حفره ای امنیتی، برای نفوذ استفاده می کنند. تعدادی از آنها به –day exploit ها (کدهایی ،برای استفاده از ضعف های امنیتی که هنوز در دسترس عموم قرار نگرفته و اصطلاحا Publish نشده اند.) دسترسی دارند و اغلب از حملات مشخص و قابل جلوگیری استفاده می کنند.تست نفوذ پذیری ، امنیت شبکه را از دیدگاه هکر مورد بررسی قرار می دهد ضعف های امنیتی که در تست نفوذ پذیری مشخص می شود، برای جلوگیری از دسترسی هکرها پوشش داده شده و بر طرف می شوند.

ارائه گزارشاتی از مشکلات به مدیریت سازمان

گروه امنیت در سازمان به نقاط ضعف سیستم آشنایی کافی دارند و تست نفوذ پذیری می تواند این نقاط ضعف را در غالب گزارش و بعنوان شخص ثالثی که از نتایج این تست سودی نخواهد برد، به مدیریت ارشد سازمان ارائه کرده و تصمیم گیری های امنیتی سازمان را سرعت بخشد.

بازرسی تنظیمات امنیتی

اگر گروه امنیت، کار امن سازی سیستم های سازمان را انجام دهد، تست نفوذپذیری می تواند گزارشی را در مورد نحوه عملکرد این گروه ارائه دهد.تست نفوذ پذیری، امنیت شبکه را بیشتر نمی کند، بلکه فاصله بین دانش و چگونگی پیاده سازی را مشخص می کند.

دوره های امنیتی برای کارشناسان بخش شبکه

آموزش به کارشناسان شبکه و امنیت سازمان، قابلیت پاسخگویی به حملاتی که اتفاق می افتند را ایجاد می کند.به عنوان مثال، در صورتی که در فاز تست نفوذ پذیری ، بدون اطلاع کسی نفوذ انجام شود، حاکی از عدم آموزش بررسی و کنترل سیستم ها توسط کارکنان است. نمونه ای از این آموزشها ، شناخت فعالیت ها و ترافیک های مشکوک و مخرب خواهد بود.

ارزیابی امنیتی تکنولوژی جدید

بهترین زمان برای تست تکنولوژی جدید، قبل از تولید آن است. تست نفوذ پذیری روی تکنولوژی ها، نرم افزار ها و .. جدید قبل از ارائه شدن در بازار تجاری، اغلب می تواند صرفه زمانی و اقتصادی را به دنبال داشته باشد.

ابزارهای تست نفوذ پذیری:

ابزارهای فراوانی برای تست نفوذ پذیری استفاده می شوند.این ابزار ها در دو گروه اصلی شناسایی (Reconnaissance) و exploitation دسته بندی می شوند.اگر چه تست نفوذ پذیری اکثرا با ابزارهای exploitation انجام می شود ولی در حالت کلی، در فاز شناسایی،

ابزارهایی که برای تشخیص پیرامون هدف هستند، استفاده می شود.بعد از شناسایی هدف ، استفاده از ابزارهای نفوذ صورت می گیرد ابزارهایی از این گروه شامل:

GFI LANguard

ISS Internet Scanner

Sara

Nmap

می باشند.

Nmap:Network Mapper

ابزاری جهت شناسایی و ممیزی است که به صورت رایگان ارائه شده است. طراحی این ابزار به صورتی است که می تواند به سرعت شبکه های بزرگ را پویش کند و به صورت متنی و گرافیکی استفاده می شود.

Flexible:

تکنولوژی های پیشرفته ای در جهت شناخت شبکه مقصد دارد. این شناخت شامل مشخص کردن سیستم های امنیتی مورد استفاده مانند فایروال، روتر و موانع دیگری است که در شبکه مقصد استفاده شده است، می باشد.پویش کامل انواع پورتها(TCP/UDP)، تشخیص سیستم عامل و نسخه آن و ping sweeps و موارد دیگر می باشد. برای اطلاعات بیشتر به آدرس زیر مراجعه نمایید: documentation page.

POWERFUL

قابلیت پویش شبکه های که دارای صدها هزار رایانه هستند را دارد.

Portable

سازگاری با بیشتر سیستم عامل ها مانند Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga.

Easy:

قابلیت های فراوان این محصول کاربران زیادی را به خود اختصاص داده است. در کنار این قابلیت ها استفاده به صورت گرافیک و یا متنی نیز وجود دارد. ساده ترین حالت برای مشخص کردن پورتهای باز مقصد به صورت زیر می باشد: nmap -v -A targethost

Free:

مهمترین هدف از تولید این ابزار، کمک به بالا بردن امنیت شبکه اینترنت و اینکه مدیران شبکه، بازرسان (Auditors) و حتی هکر ها بتوانند توسط این ابزار شبکه را پویش و نقاط ضعف را مشخص کنند.

Nmap ابزاری عمومی برای پویش می باشد. پویش پورت ها اولین قابلیت این ابزار است که عموما به عنوان بخشی از فازشناسایی تست نفوذپذیری و یا حمله مورد استفاده قرار میگیرد. هکر ها معمولا پویش پورت ها را به صورت محدود انجام می دهند و به دلیل ترافیک زیادی که پویش تمامی پورت ها ایجاد می کند، بندرت دست به پویش تمامی پورت های مقصد می زند.

(excess traffic)

در مواردی که تمامی پورت ها مورد پویش قرار می گیرند، ترافیک زیادی ایجاد می شود و بیشتر IDS ها و سیستم های مانیتورینگ این نوع پویش را تشخیص می دهند و قوانین لازم را اعمال می کنند.

از قابلیت های دیگر این ابزار تشخیص سیستم عامل مقصد می باشد. بخش شبکه ای پیاده سازی شده در هر سیستم عامل، جوابهای متفاوتی را به بسته های دریافتی می دهد. از این رو این ابزار می تواند سیستم عامل مقصد را تشخیص دهد. تشخیص سیستم عامل کاملا دقیق نیست ولی به حمله کننده کمک می کند تا روش و استراتژی حمله خود را، مخصوصا زمانی که اطلاعات زیادی دریافت کرده است، مشخص کند. مثال زیر تشخیص سیستم عامل هدف را نشان میدهد، پس از مشخص شدن هدف، هکر به جمع آوری و استفاده از ابزارها و ضعف های امنیتی که برای سیستم عامل ویندوز ۲۰۰۳ ارائه شده است می پردازد.

nmap –v –O 192.168.0.0/16 10.0.0.0/8

tcp open IIS/۱۰۲۷

tcp open ppp/۳۰۰۰

tcp open globalcatLDAP/۳۲۶۸

tcp open http-proxy/۸۰۸۰

Device type: general purpose

Running: Microsoft Windows NT/2K/XP|2003/.NET

OS details: Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2

منبع : sgnec