فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۵ (پاییز ۱۳۹۴): صص ۱۱۹ – ۱۴۴

ارائه یک روش سنجش نفوذپذیری در امنیت شبکه مبتنی بر ابزارهای متن باز

محمد رشیدنژاد[۱]
جمشید نصرت‌آبادی[۲]
حجت‌اله قدیری[۳]

تاریخ دریافت: ۱۳۹۴/۰۳/۲۳
تاریخ پذیرش: ۱۳۹۴/۰۶/۰۴

چکیده

با رشد و فراگیر شدن بستر شبکه در حوزه فناوری اطلاعات و ارتباطات و نقش مستقیمی که در ایجاد، نگهداری و توسعه کسب‌وکارها ایفا می‌نماید، بحث‌های امنیتی شبکه اهمیت ویژه‌ای می‌یابند. یکی از راه‌هایی که بتوان از پایداری و صحت امنیت شبکه اطلاع پیدا کرد، سنجش نفوذپذیری است. در سنجش نفوذپذیری با شبیه‌سازی حملات هکرها، اقدام به ارزیابی و شناسایی آسیب‌پذیری‌های رایانه‌ها، شبکه‌ها و سامانه‌ها می‌گردد. این مقاله با روش پیمایش و با هدف شناخت فرآیند سنجش نفوذپذیری و ابزارهای به کار رفته در هر مرحله از آن و ارائه یک روش بومی مبتنی بر ابزارهای متن باز با قابلیت استفاده و کارایی این ابزارها انجام‌شده است. در این تحقیق ابتدا به شناخت کاملی از سنجش نفوذپذیری و مفاهیم آن پرداخته‌شده، سپس با مطالعه عمیق و بررسی همه‌جانبه استانداردها و متدولوژی‌های مختلف سنجش نفوذپذیری، یک متدولوژی مناسب برای سنجش نفوذپذیری شبکه‌ها ارائه گردیده است. هم‌چنین ابزارها و تکنیک‌های مؤثر برای مراحل پنج‌گانه اصلی جمع‌آوری، پویش، دست‌یابی، حفظ دست‌یابی و پاک کردن رد پا مبتنی بر این روش نیز ارائه گردید. جامعه آماری شامل ۲۰ شبکه سازمانی (هر شبکه دارای ۵۰ تا ۸۰۰ رایانه) توسط محققان انتخاب گردید و عملیات سنجش نفوذپذیری را با پنج ابزار پیشنهادی برای مراحل پنج‌گانه اصلی روی شبکه‌ها انجام دادند و با توجه به خروجی هر یک از ابزارها، سطح موفقیت آن بر اساس مقیاس لیکرت سنجیده شد. نتایج نشان داد شاخص‌های میانگین موفقیت این روش ۳,۳۷ و انحراف معیار آن ۱,۱۱ است. که قابل‌قبول بودن و توانمندی این روش را تأیید می‌کند و می‌توان بر اساس روش پیشنهادی از این ابزارها برای سنجش نفوذپذیری شبکه‌ها استفاده نمود.

کلید واژه‌ها: *آسیب‌پذیری ،پویش ، سنجش نفوذ، شبیه‌سازی حمله، شناسایی*

۱- کارشناس ارشد مهندسی فناوری اطلاعات دانشگاه تربیت مدرس security.org@gmail.com
۲- کارشناس ارشد مدیریت فناوری اطلاعات دانشگاه پیام نور تهران nosratabadi61@yahoo.com
۳- دکترای علوم دفاعی هیات علمی دانشگاه علوم و فنون فارابی تهران mrc.security@scitco.ir

مقدمه

سنجش نفوذپذیری فرآیندی است که برای شبیه‌سازی حملات یک هکر یا یک گروه هکری جهت ارزیابی آسیب‌پذیری‌های یک کامپیوتر یا یک مجموعه کامپیوتر (شبکه) صورت می‌گیرد، این فرآیند بسته به گستردگی شبکه متغیر و می‌تواند شامل سنجش و ارزیابی تمام ضعف‌های امنیتی سرویس‌ها، عیب‌های فنی یا آسیب‌پذیری‌های مختلف باشد. پس از بررسی و استخراج اطلاعات، این اطلاعات همراه با گزارشی در اختیار مدیر سیستم قرار می‌گیرد تا به‌موقع برای رفع عیوب احتمالی، اقدام‌های لازم صورت گیرد. مهم‌ترین تفاوت بین هکر و شخصی که سنجش نفوذپذیری انجام می‌دهد این است که، سنجش نفوذپذیری با مجوز و قراردادی که با سازمان یا شرکت امضاءشده است انجام می‌شود و درنهایت منجر به یک گزارش خواهد شد. هدف از سنجش نفوذپذیری، بالا بردن امنیت داده‌ها توسط تست امنیتی می‌باشد. اطلاعات و ضعف‌های امنیتی که در نفوذپذیری مشخص می‌شود محرمانه تلقی شده و نباید تا برطرف شدن کامل افشاء شود.

فرآیند سنجش نفوذپذیری شامل یک فرآیند پنج مرحله‌ای است که شامل شناسایی، پویش، دسترسی به هدف، حفظ دسترسی و پاک کردن ردپا و درنهایت گزارش دهی به همراه راه‌کارهای امنیتی است (Graves, 2010).

در حال حاضر شرکت‌ها و مؤسسات مختلفی ازجمله EC-Council دوره‌هایی را که بر روی تکنیک‌ها و تکنولوژی‌های هک از دیدگاه حمله تکیه دارد، ارائه می‌کنند .در این دوره‌ها، مخاطبان با چک لیست‌های امنیتی آشنا شده و توانایی بررسی سیستم‌های امنیتی موجود را کسب می‌نمایند و قادر به شناسایی آسیب‌پذیری‌های سیستم و تعیین وضعیت امنیتی یک سازمان با استفاده از تست‌های نفوذ هستند .هم‌چنین با استفاده از حمله به سیستم‌ها، روش‌های دفاعی نیز موردبررسی قرار خواهند گرفت. ازجمله دوره هکر شرافتمند (CEH) یکی از این قبیل دوره‌ها است که بر پنج مرحله تکیه دارد (Graves, 2010). هم‌چنین تحقیقات مختلفی در این زمینه انجام‌شده است که نتیجه آن منجر به روش‌های بهینه، تاکتیک‌ها و تکنیک‌های مشخصی برای سنجش نفوذپذیری شبکه‌های رایانه‌ای با سیم و بی‌سیم، نرم‌افزارها و وب‌سایت‌ها شده است.

در این تحقیق سعی می‌گردد تا با مرور تحقیقات پیشین در این زمینه، انجام تحقیقات میدانی و بررسی استانداردها، به روش‌ها و یک پیمایش جامع در خصوص سنجش نفوذپذیری، فرآیند، تاکتیک و تکنیک، روش‌ها و ابزارهای مرتبط با آن و نحوه گزارش دهی، چارچوب مشخصی را برای این حوزه شناسایی و در

انتها یک مکانیزم مشخص بومی از فرآیند سنجش نفوذپذیری تا گزارش دهی بر اساس ابزارهای متن باز ارائه دهیم. سپس روش پیشنهادی را با ابزارهای متن باز ارائه‌شده بر روی ۲۰ شبکه رایانه‌ای که هر شبکه بین ۵۰ تا ۸۰۰ رایانه دارد، ارزیابی نموده که نتایج حاصل از این ارزیابی قابلیت اطمینان و اعتبار روش پیشنهادی را نشان می‌دهد.

بیان مسئله

مدیران شبکه همیشه موارد امنیتی را در شبکه‌های سازمانی برقرار می‌نمایند اما در راستای کنترل امنیت و پایداری شبکه‌ها اقدام اساسی صورت نمی‌پذیرد. سنجش نفوذپذیری یکی از اقدامات مهم در راستای کنترل امنیت و پایداری شبکه است. سنجش نفوذهایی که معمولاً انجام می‌گیرد به دلیل استفاده از ابزارهای حرفه‌ای، گران‌قیمت و متن باز نبودن و عدم انعطاف‌پذیری آن‌ها این فرآیند بسیار پرهزینه و زمان‌بر است و به دلیل استفاده از ابزارهای ضعیف و ناکارآمد و به‌کارگیری نامناسب ابزارها غالباً موفقیت چندانی در شناسایی آسیب‌پذیری‌ها و برطرف کردن آن‌ها حاصل نمی‌گردد. هم‌چنین به دلیل تنوع روش‌ها و متدولوژی‌های سنجش نفوذ، تصمیم‌گیری برای انتخاب یک روش متناسب با محیط سازمانی با مشکل مواجه می‌شود. از طرفی در فرآیند سنجش نفوذ، انتخاب ابزار مناسب که بتواند خروجی درست و بهینه‌ای را در هر گام به وجود آورده و برای گام بعدی یک ورودی مناسب تلقی گردد و هم‌چنین یکپارچگی را در تمامی گام‌های فرآیند حفظ نماید به عنوان یک مسئله مهم مطرح می‌گردد.

اهمیت و ضرورت تحقیق

سنجش نفوذپذیری با شناسایی آسیب‌پذیری‌ها و نقاط ضعف شبکه و ارتقا سطح امنیتی شبکه می‌تواند از اهمیت بالایی در حوزه پدافند غیرعامل برخوردار بوده و نقش مؤثری در این راستا ایفا نماید. هم‌چنین سنجش نفوذپذیری برای سازمان‌ها یک ضرورت است چراکه با توجه به فراگیر شدن شبکه‌ها در سازمان‌ها و استفاده از برنامه‌ها و فناوری‌های نوین و حتی غیربومی در این حوزه، شناخت کامل فرآیند سنجش نفوذپذیری به منظور کنترل امنیت اطلاعات در سطح سازمان یک الزام محسوب می‌گردد. سنجش نفوذپذیری به سازمان‌ها دریافتن حفره‌های امنیتی سیستم‌های مورداستفاده پیش از استفاده هکرها و دیگران از این حفره‌ها، ارائه گزارش‌هایی از مشکلات به مدیریت سازمان، بازرسی تنظیمات امنیتی و

دوره‌های امنیتی برای کارشناسان بخش شبکه و ارزیابی امنیتی تکنولوژی جدید و ارتقای سطح امنیت اطلاعات سازمان کمک می‌کند (Yeo, 2013).

تحقیقات مختلفی در زمینه سنجش نفوذپذیری انجام‌شده است که منجر به روش‌های بهینه، تاکتیک‌ها و تکنیک‌های مشخصی برای سنجش نفوذپذیری شبکه‌های رایانه‌ای با سیم و بی‌سیم، نرم‌افزارها و وب‌سایت‌ها شده است اما این روش‌ها و استانداردها به صورت کلی، جامع و با نگاه کسب‌وکار بوده و یک رویکرد کلان را برای مجریان عملیات سنجش نفوذ به وجود می‌آورد. ازاین‌رو نیاز است که یک روش بومی با ابزارهای جدید و کارآمد و مراحل صحیح به‌کارگیری آن‌ها منطبق باسیاست‌های سازمانی، تجهیزات و بسترهای موجود طراحی و تدوین گردد.

سؤال و هدف تحقیق

سؤال‌های اصلی تحقیق:

۱- چگونه می‌توان با بررسی روش‌های نفوذپذیری به یک روش سنجش نفوذپذیری بومی مبتنی بر متن باز دست یافت؟

۲- روش سنجش نفوذپذیری مبتنی بر ابزارهای متن باز از چه میزان کارایی و اثربخشی برخوردار است؟

هم‌چنین هدف از این تحقیق دست‌یابی به یک متدولوژی بومی و قابل‌اطمینان مبتنی بر ابزارهای متن باز برای سنجش نفوذپذیری می‌باشد.

پیشینه

تاکنون تحقیقات مختلفی در زمینه سنجش نفوذپذیری انجام‌شده است که نتیجه آن منجر به روش‌های بهینه، تاکتیک‌ها و تکنیک‌های مشخصی برای سنجش نفوذپذیری شبکه‌های رایانه‌ای با سیم و بی‌سیم، نرم‌افزارها و وب‌سایت‌ها شده است که از آن جمله می‌توان به استانداردهای OSSTMM، ISAFF، OWASP، NIST و PTES و هم‌چنین دوره CEH اشاره نمود (Haubris & Pauli, 2013). از طرفی روش‌های متداولی توسط محققان مختلف ازجمله هابریز و پاولی در سال ۲۰۱۳، مک کلور و همکاران در سال ۲۰۰۹ و گراوس در سال ۲۰۱۰ و هم‌چنین نوری در سال ۱۳۸۹ طرح‌ریزی و ارائه‌شده است که در ادامه به آن‌ها اشاره می‌شود.

روش‌های متداول سنجش نفوذ

اغلب سنجش‌های نفوذ به دو شکل طبقه‌بندی می‌شوند:

۱- از نظر میزان اطلاعاتی که در اختیار تست نفوذکننده قرار می‌گیرد.

۲- از نظر مکانی که سنجش نفوذ ازآنجا انجام می‌شود.

سه نوع مختلف از سنجش نفوذ بر اساس اطلاعاتی که در اختیار تست نفوذکننده قرار می‌گیرد، توسط مجریان انجام می‌شود؛ جعبه سفید، جعبه سیاه و جعبه خاکستری (Graves, 2010). در تست جعبه سفید، متقاضی سنجش کاملی را در اختیار تست کننده قرار داده و تست کننده با شبکه هدف همکاری کامل دارد.

در تست جعبه سیاه تنها چند نفر از مدیران شبکه اطلاع دارند که تست در حال انجام است و هیچ‌گونه اطلاعاتی در اختیار تیم تست نفوذ قرار داده نمی‌شود.

در تست جعبه خاکستری ترکیبی از این دو تست و یک طرح تست سفارشی می‌باشد که اطلاعات نسبی از شبکه در اختیار تیم قرار داده می‌شود.

هم‌چنین دو نوع سنجش نفوذ بر اساس محل سنجش شامل سنجش داخلی و خارجی مطرح است که در آن تست نفوذکننده شبکه و سامانه‌ها را بر اساس سناریو و توافقات از پیش تعیین‌شده، شبکه را از داخل شبکه یا از خارج آن و از طریق اینترنت ارزیابی می‌کند. تاکتیک‌ها و روش‌های مختلفی نیز توسط تیم‌های تست نفوذ طراحی، استفاده و ارائه‌شده است.

در یک تاکتیک ارائه‌شده برای سنجش نفوذ، سه دسته اصلی شامل اطلاعات، تیم و ابزار را معرفی می‌کند که زیرمجموعه اطلاعات به چهار مرحله تقسیم می‌شود و شامل؛ جمع‌آوری اطلاعات، شناسایی سیستم‌عامل (OS)، اسکن پورت و شناسایی خدمات و سرویس است. در دسته‌بندی تیم و ابزار هر عضو تیم باید مسئولیت خود را انجام دهد و آن‌ها باید ابزارها را هم کامل بشناسند (Haubris & Pauli, 2013).

نوع دیگر روش سنجش نفوذ شامل روش جمع‌آوری اطلاعات مستقل می‌باشد که از چهار مرحله تشکیل‌شده است؛ فاز اول بررسی خدمات شبکه شامل رکوردهای DNS (نام دامنه سیستم) و دیگر اطلاعات فنی است و برای این‌که وب‌سایت‌ها در شبکه درست عمل کنند به آن نیاز دارند. فاز دوم شناسایی سیستم‌عامل است. برای انجام این مرحله شناسایی آن‌ها توصیه می‌کنند که از ابزار NMAP استفاده کنید سپس مرحله اسکن پورت می‌باشد که روش‌های گوناگون اسکن (SYN,FIN,XMAS) را به کار می‌برد. مرحله آخر شناسایی سرویس است که در آن هدف جمع‌آوری اطلاعات در خصوص نوع

سرویس، نوع برنامه‌های کاربردی و سطح وصله‌های امنیتی سرویس‌ها و نـرم‌افزارهـای سـازمان مـوردنظر است (Haubris & Pauli, 2013).

دو نوع از حملات برای سنجش نفوذ توصیه مـی‌شـود: نـوع اول حملـه غیرفعـال مـی‌باشـد کـه بـرای جمع‌آوری است و در طی این حمله نفوذکننده مستقیماً به سیستم یا شبکه هـدف تجـاوز نمـی‌کنـد و آن را تحت تأثیر قرار نمی‌دهد. شکل دیگر، حمله نفوذی است که در آن نفوذکننده بـه سیسـتم یـا شـبکه هـدف تجاوز می‌کند (McClure, Scambray, & Kurtz, 2009).

یک مرحله اساسی برای این‌که بتوانیم با هک شرافتمندانه یا سنجش نفوذ شروع کنیم شامل گام‌هـای زیر است (Graves, 2010):

- بررسی ردپاها
- اسکن کردن
- شناسایی

برای انجام این مرحله باید یک لیست کوچک از سایت‌هـایی کـه بـرای مرحلـه جمـع‌آوری اطلاعـات استفاده می‌شوند تهیه کرد. هم‌چنین یک لیست کوچک برای مرحله شناسایی و اسکن نیاز است.

یک روش سنجش نفوذ که خیلی مورداستفاده قرار می‌گیرد و موردتوجه ارزیاب‌های امنیتی است، روشی است که در شش گام زیر ارائه‌شده است (Haubris & Pauli, 2013):

- جمع‌آوری اطلاعات
- تحلیل آسیب‌پذیری
- تعریف اهداف ثانویه
- نفوذ/ حمله
- تحلیل نتایج
- تحلیل نهایی / مستندسازی

از روش‌های رایج در سنجش نفوذ که توسط گروه صا افتا در ایران ارائه‌شده، فرآینـدی اسـت کـه یـک نفوذ گر اخلاقی مشابه با یک نفوذ گر مخرب دنبال می‌کند. گام‌های پیش رو برای دسـت‌یـابی و نگـه‌داری مداخل ورودی به یک سیستم رایانه‌ای بدون ارتباط با منظور نفوذ گرها مشابه می‌باشند. پنج مرحلـه‌ای کـه نفوذ گرها معمولاً در جریان نفوذ به یک سیستم دنبال می‌کنند شامل مراحل زیر است (نوری, ۱۳۸۹)

- شناسایی
- پویش
- حصول دسترسی
- نگه‌داری دسترسی
- رد گم کردن

صرف‌نظر از این‌که از کدام استاندارد پیروی می‌شود باید یک روش و تاکتیک درست انتخاب شود تا اثربخشی و کارایی لازم را متناسب با محیط ارزیابی و سنجش داشته باشد.

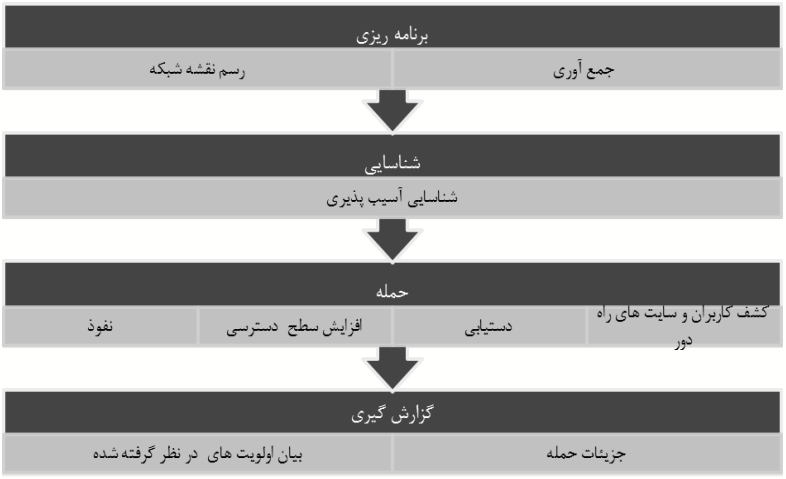
استانداردهای سنجش نفوذ فعلی

هدف از استانداردهای سنجش نفوذ این است که یک طرح اولیه به ما بدهد از این‌که سنجش نفوذ چیست و در خصوص مراحلی که باید از آن‌ها پیروی کنیم یک طرح جامع و کامل به ما بدهد. استانداردهای گوناگونی وجود دارند که هر کدام جوانب مثبت و منفی دارند و انتخاب هر کدام از آن‌ها بر اساس اهداف و محیط تستی است که می‌خواهید انجام دهید.

استانداردهای فعلی

در حال حاضر استانداردهای زیادی شامل OSSTMM، ISSAF، NIST و OWASP و PTES وجود دارند که می‌توانند دنبال شوند.

روش OSSTMM به دنبال ایجاد یک شیوه استاندارد برای انجام یک آزمون امنیتی کامل است که شامل مراحلی است که باید گام به گام انجام شود (herzog & Barceló, 2010). در نقشه امنیت معرفی‌شده برای این استاندارد پنج بخش امنیت اطلاعات، امنیت کارکنان، امنیت ارتباطات، امنیت بی‌سیم و امنیت فیزیکی وجود دارد. فرآیند آن شامل ۴ مرحله برنامه‌ریزی (جمع‌آوری و رسم نقشه شبکه)، شناسایی (شناسایی آسیب‌پذیری)، حمله (کشف کاربران و سایت‌های راه دور، دست‌یابی، افزایش سطح دسترسی و نفوذ) و گزارش‌گیری (جزئیات حمله و اولویت‌ها و نتایج) است. شکل ۱ فرآیند OSSTMM را نشان می‌دهد.



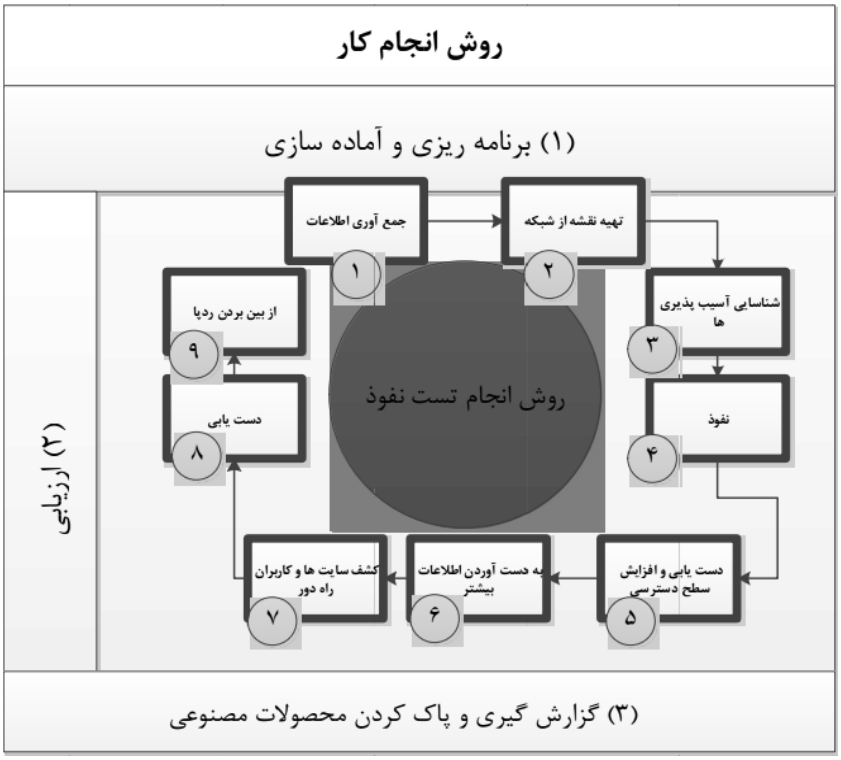
شکل ۱: فرآیند OSSTMM

روش ISSAF یک روش انجام سنجش نفوذپذیری است که به منظور ارزیابی کنترل‌های موجود در شبکه، سیستم و برنامه‌های کاربردی موجود در شبکه طراحی‌شده است. روش ISSAF شامل سه مرحله و نه گام ارزیابی است (Rathore, et al., 2006).

این سه مرحله کلی عبارت‌اند از:

- برنامه‌ریزی و آماده سازی
- ارزیابی
- گزارش‌گیری، پاک‌سازی و خراب کردن محصولات مصنوعی

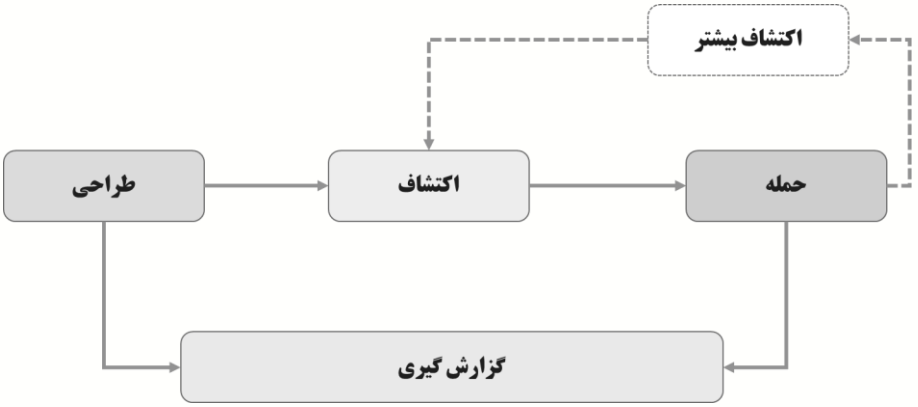
شکل ۲ مراحل انجام روش ISSAF را نشان می‌دهد.



شکل ۲: مراحل انجام سنجش نفوذپذیری به روش ISSAF

NIST برای انجام سنجش نفوذپذیری مراحل دیگری را ذکر کرده است که شامل چهار مرحله طراحی، اکتشاف، حمله و گزارش‌گیری است (Scarfone, Souppaya, Cody, & Orebaugh, 2008).

در شکل ۳ این مراحل و ترتیب آن‌ها نشان داده شده است.

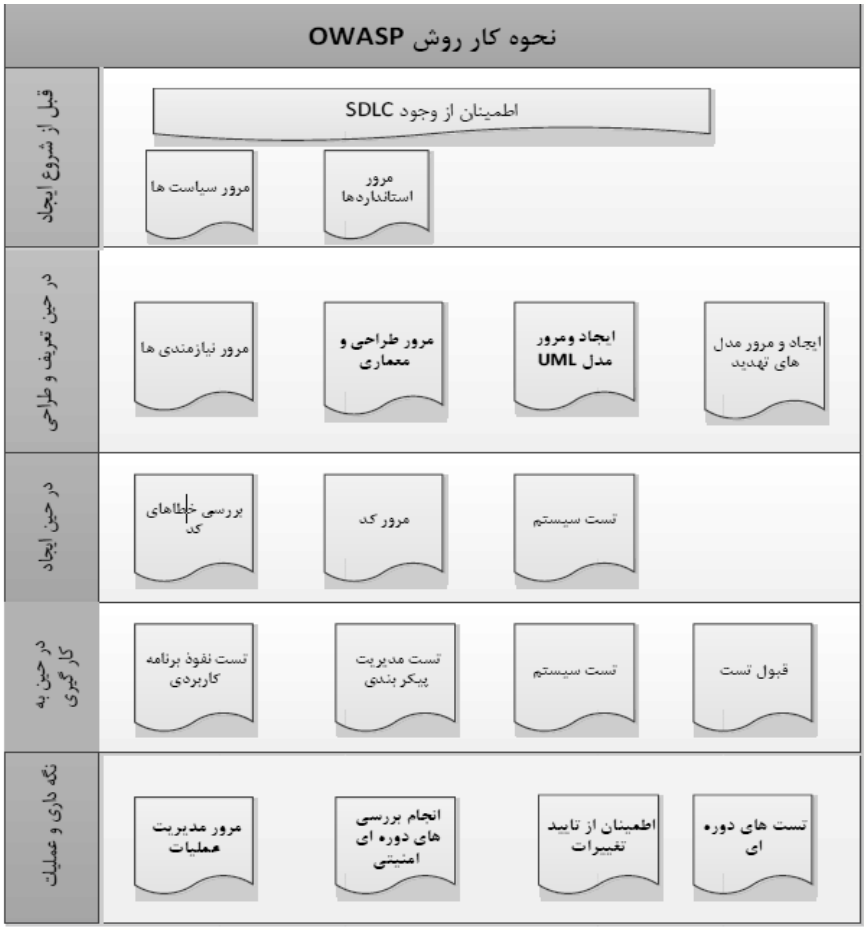


شکل ۳: مراحل روش NIST

OWASP سنجش نفوذپذیری برنامه‌های وب است که از تست جعبه سیاه استفاده می‌کند. به عبارت دیگر ارزیاب هیچ اطلاعی در مورد برنامه کاربردی مورد تست ندارد (Muller & Meucci, 2014). OWASP نام انجمنی است که سازمان‌ها را قادر می‌سازد تا برنامه‌های کاربردی قابل‌اعتماد را خرید و نگه‌داری کنند. هدف آن ایمن‌سازی نرم‌افزارهای موجود است. چارچوب کاری OWASP دارای فعالیت‌هایی است که باید در مواقع زیر انجام گیرد:

- قبل از شروع ایجاد
- در حین تعریف و طراحی
- در حین ایجاد
- در حین به‌کارگیری
- نگه‌داری و عملیات

شکل ۴ جزئیات روش OWASP را تشریح می‌کند.



شکل ٤: نحوه کار روش OWASP

PTES یک استاندارد نسبتاً جدیدی است که توسعه آن در سال ۲۰۱۰ شروع‌شده است (Haubris & Pauli, 2013). یکی از ویژگی‌های خاص این استاندارد این است که در مناطق خاصی از فرآیند تست که کارشناسان صنعت روی آن تمرکز دارند توسعه‌یافته است. مراحلی که در PTES تحت پوشش قرار دارند به شرح زیر است:

- اقدامات پیش تعامل
- جمع‌آوری اطلاعات
- مدل‌سازی تهدید

- تحلیل آسیب‌پذیری
- بهره‌برداری
- پس از بهره‌برداری
- گزارش

در جدول ۱ مقایسه‌ای بین استانداردها و تکنیک‌های اشاره‌شده، صورت گرفته است.

جدول ۱- مقایسه‌ای بین استانداردها و تکنیک‌های سنجش نفوذ

استاندارد سنجش نفوذ	ویژگی‌ها	مزایا	معایب
OSSTMM	• فرآیند ۴ مرحله‌ای • ۹ فعالیت برای تکمیل فرآیند • بررسی و تست در پنج حوزه ○ امنیت فیزیکی ○ امنیت ارتباطات ○ امنیت نیروی انسانی ○ امنیت ارتباطات بی‌سیم ○ امنیت داده‌ها و اطلاعات شبکه	• متدولوژی متن باز • استفاده از معیارهای قابل‌محاسبه • ایجاد فهرستی از مواردی که باید تست شوند • پوشش کامل در حوزه شبکه و ارتباطات	• پوشش کم در حوزه برنامه‌های کاربردی • جزییات زیاد برای تست و طولانی شدن زمان تست
ISSAF	• فرآیند ۳ مرحله‌ای • ۹ گام برای تکمیل فرآیند • بررسی و تست شبکه، سیستم و برنامه‌های کاربردی	• برقراری ارتباط مؤثر بین ابزار و عملیات تست • اجرای تست با گام‌های مشخص	• بیان روش‌ها و اقدامات با جزییات و موظف بودن ارزیاب به پیروی از آن و کاهش خلاقیت ارزیاب در اجرای فرآیند
NIST	• فرآیند ۴ مرحله‌ای • بررسی و تست شبکه و سیستم	• تکرار مراحل جمع‌آوری اطلاعات و نصب ابزارها که منجر به کشف اطلاعات بیشتر و دست‌یابی به سیستم‌های بیشتر می‌شود • سادگی و کاهش جزییات	• تست تکنیکی و ساده برای سازمان‌ها به‌طوری که تنها به عنوان بخشی از ارزیابی و سنجش کلی مورداستفاده قرار گیرد.
OWASP	• فرآیند ۵ مرحله‌ای • بررسی و تست برنامه‌های کاربردی تحت وب	• تمرکز کامل در حوزه برنامه‌های کاربردی تحت وب در چرخه حیات و توسعه نرم‌افزارها • جزییات کامل برای تست به صورت جعبه سیاه و خاکستری • مبتنی بر آسیب‌پذیری‌های معمول برنامه‌های تحت وب • ارائه روش‌های کاربردی و گام به گام برای تست نرم‌افزار و ارائه گزارش جامع برای تست	• پوشش تنها در حوزه نرم‌افزاری و عدم پوشش شبکه، سیستم و... • پوشش کم سایر نرم‌افزارها مانند سیستمی، غیر وب و ...

PTES	• فرآیند ۷ مرحله‌ای • بررسی و تست برنامه‌های کاربردی تحت وب و شبکه	• ایجاد یک راهنمای خط مبنا برای تست امنیتی • توجه ویژه به مدل‌سازی تهدید • معرفی ابزارهای مورداستفاده	• در حال تکمیل در برخی حوزه‌ها • پوشش محدود در حوزه نرم‌افزاری و شبکه • معرفی تعداد زیادی از ابزارها و عدم ارائه یک روش کاربردی

بر اساس استانداردها و تاکتیک‌های ارائه‌شده، گام‌های اساسی مشترک در این روش‌ها را تشریح می‌کنیم.

مرحله قبل از تعامل گام مهمی است، زیرا نفوذکننده اطلاعات موردنیاز خود از قبیل دامنه آزمون، چه اهداف خاصی مدنظر است و قوانین مورداستفاده در تست و ارزیابی را برای انجام سنجش نفوذ به دست می‌آورد. در برخی استانداردها به عنوان برنامه‌ریزی یا آماده سازی تعریف‌شده است. تست نفوذکننده با اطلاعات بیشتری که در این مرحله به دست می‌آورد گزارش مفیدتری به سازمان خواهد داد. نکته کلیدی موردبحث در مرحله پیش تعامل این است که کدام قسمت از سازمان باارزش‌تر و دارای اطلاعات مهم‌تری است. هنگامی‌که این مناطق شناسایی شد، ارزیاب در مورد این‌که آن‌ها به چه دسترسی نیاز دارند و اهداف آن‌ها چه چیزی خواهد بود، ایده بهتری می‌تواند بدهد. این هم‌چنین مرحله‌ای است که ارزیاب با نظر سازمان تعیین می‌کند آن‌ها در تست کلاه سفید، سیاه یا خاکستری باشند.

هدف از مرحله جمع‌آوری اطلاعات این است که تا آنجا که ممکن است اطلاعات بیشتری در خصوص هدف خود به دست آوریم. این اطلاعات شامل اطلاعات اساسی خود سازمان، سیستم‌های مورداستفاده و یکسری اطلاعات بیشتر در خصوص خود کارمندان باشد. در این مرحله ابزارهای اتوماتیک نباید تنها ابزارهایی باشند که مورداستفاده قرار می‌گیرند بلکه باید بررسی‌های دیگر به عنوان مکمل در این خصوص انجام بگیرد. اغلب اطلاعات به‌دست‌آمده در مرحله اتوماتیک یک ورودی اولیه برای مراحل بررسی و تست به صورت دستی است. بر اساس اطلاعات به‌دست‌آمده در طی این مرحله مدل‌سازی تهدید انجام می‌شود زیرا باید مشخص شود شرکت به چه شکلی تولید درآمد می‌کند و چگونه روزبه‌روز کسب‌وکار را انجام می‌دهد. بخش مهم در این قسمت این است که مشخص شود تهدیدات بزرگ از کجا وارد خواهند شد و یک نقشه تهدید برای دارایی‌های اولیه و ثانویه طراحی می‌شود.

تحلیل آسیب‌پذیری مرحله‌ای است برای یافتن این‌که چه آسیب‌پذیری‌های نرم‌افزاری /خدماتی وجود دارد و این‌که حمله کننده چه روش‌های دیگری برای رسیدن به هدف می‌تواند استفاده کند. این شامل دو مرحله دستی و اتوماتیک می‌باشد. روشی که در این مرحله از تحلیل صورت می‌گیرد می‌تواند با نحوه

عملکرد OpenVAS متفاوت باشد و بر اساس اطلاعات به‌دست‌آمده در مرحله اسکن همه روش‌های اسکن برای راه‌اندازی یک سرور را انجام دهد تا بتواند مشابه آن شبکه را راه‌اندازی نماید و بتواند در تست آسیب‌پذیری به صورت دستی از آن‌ها استفاده نماید.

بعد از این‌که نفوذکننده اطلاعات را به دست آورد مرحله تحلیل آغاز می‌شود. در این مرحله آن‌ها همه اطلاعات قبلی را مورداستفاده قرار می‌دهند تا معین کنند که چه روش حمله‌ای بهتر جواب می‌دهد. هم‌چنین شامل استفاده از اکسپلویت های خاص و دور زدن آنتی ویروس و نرم‌افزارهای امنیتی نیز می‌شود. با استفاده از اطلاعات به‌دست‌آمده در مرحله تحلیل آسیب‌پذیری و اکسپلویت های دیگر شبکه را توسعه می‌دهیم برای این‌که بتوانیم به اطلاعات سیستم‌های مورد هدف دسترس پیدا کنیم.

انواع حملات رایج و کاربردی در مرحله نفوذ و دسترسی به هدف شامل حملات زیر است:

- مهندسی اجتماعی
- حمله کشف کلمات عبور و عبور از مکانیزم احراز هویت
- شنود اطلاعات مبادله شده و کشف اطلاعات حساس
- حمله به پایگاه داده‌ها
- حمله به برنامه‌های کاربردی سازمانی و عمومی
- حمله به سرورها
- حمله به باگ های سیستم‌عامل‌ها
- حملات سرریز بافر
- حمله به وب سرور مانند دزدیدن جلسه، تزریق کد، اعتبارسنجی ورودی‌ها
- حمله به تجهیزات شبکه مانند سوییچ، روتر و عبور از شبکه‌های مجازی
- عبور از مکانیزم های امنیتی شبکه‌های بی‌سیم
- استفاده از کدهای مخرب مانند تروجان و درب‌های پشتی
- حملات از کار انداختن سرویس

در مرحله بعد از بهره‌برداری، هدف اصلی نگه‌داشتن دسترسی و شناسایی بیشتر شبکه می‌باشد. وقتی این کار انجام شد یک کار گسترده‌ای برای تداوم حفظ دسترسی انجام‌شده است. بعد از این‌که تست انجام شد مرحله گزارش آغاز می‌شود که باید شامل بخش‌های گزارش فنی و خلاصه اجرایی باشد. گزارش فنی می‌بایست شامل همه اطلاعاتی باشد که شما در طی مرحله سنجش نفوذ و بقیه مراحل به دست می‌آورید.

روش، نوع تحقیق، جامعه آماری و تجزیه و تحلیل داده‌ای

با مطالعه دقیق و عمیق استانداردها و متدولوژی‌های مختلف برای فرآیند سنجش نفوذپذیری، این فرآیند به‌طور کامل شناخته شد و در بررسی استانداردها به آن اشاره گردید. با توجه به تجارب محققان در حوزه سنجش نفوذپذیری و بررسی متدهای مختلف، یک متدولوژی برای محیط‌هایی که دارای شرایط خاص حاکمیتی و سیاست‌های ویژه و سخت‌گیرانه‌ای هستند مانند محیط‌های سازمانی و نظامی ارائه شد که این متدولوژی برای محیط‌های غیر سازمانی یا محیط‌های بااهمیت کم‌تر نیز کاربردی است.

روش بومی سنجش نفوذپذیری

روش بومی ارائه‌شده تلفیقی از روش‌ها، تکنیک‌ها و استانداردهای موجود (Haubris & Pauli, 2013) و (Young, 2014) و تجارب چندین ساله محققان در حوزه ارزیابی امنیتی و سنجش نفوذ و هم‌چنین نتایج حاصل از تحقیقات نظری و سازمانی است.

جدول ۲ تمامی مراحل موجود در انجام سنجش نفوذپذیری بومی را به صورت قدم به قدم با ذکر جزئیات برای بهره‌برداری در محیط شبکه سازمانی بیان می‌کند.

جدول ۲- تمامی مراحل موجود در روش سنجش نفوذپذیری پیشنهادی

گام	عنوان	توضیح
۱	مجوز بالاترین مقام سازمانی	مجوز و تأییدیه مقامات سازمانی مهم‌ترین مرحله قبل از انجام سنجش نفوذپذیری است. بدون این کار، تمامی حمله‌هایی که در جریان تست در مقابل هدف انجام می‌شود، غیرقانونی به نظر می‌رسد. دستور باید توسط بالاترین مقام سازمان ابلاغ گردد.
۲	هماهنگی با مبادی ذی‌ربط	به منظور انجام تست باید با مبادی ذی‌ربط ازجمله مراجع امنیتی و حفاظتی هماهنگی کامل صورت گرفته و مدیران نسبت به فرآیند انجام کار و نحوه دسترسی به اطلاعات، شناخت آسیب‌ها و ... مطلع گردند. هم‌چنین باید مشخص شود به مجری سنجش نفوذپذیری چه مقدار اطلاعات باید داده شود و همین طور روش موردنظر برای اجرای تست بیان می‌شود. این مرحله برای محیط‌هایی که دارای شرایط خاص حاکمیتی و سیاست‌های ویژه و سخت‌گیرانه‌ای هستند مانند محیط‌های سازمانی و نظامی الزامی است.
۳	طرح حمله	این مرحله توسط گروه مجری تست انجام می‌شود که شامل اقدام‌های زیر است: • انتخاب گروه مجری سنجش نفوذپذیری • جمع‌آوری ابزارها • طرح روش حمله

۴	جمع‌آوری اطلاعات	این مرحله شناسایی هدف یا Footprinting نامیده می‌شود. در این مرحله تمامی اطلاعات موردنیاز در مورد سازمان هدف یا یگان مربوطه مورد ارزیابی جمع‌آوری می‌شود. از این اطلاعات در مراحل بعدی استفاده می‌شود.
۵	پویش[1]	مرحله پویش شامل جست‌وجو و بررسی سیستم‌ها، سرویس‌ها و برنامه‌هایی است که در سیستم تحت تست اجرا می‌شوند. در این مرحله سیستم‌های فعال شناسایی و نقشه شبکه ترسیم می‌شود. هم‌چنین آسیب‌پذیری‌های هدف و سامانه‌های مورد تست شناسایی می‌شوند. شناخت آسیب‌پذیری‌ها از مهم‌ترین مراحل کار است.
۶	دست‌یابی	این مرحله باعث می‌شود که گروه مجری نشان دهد آیا اکسپلویت یا روش حمله‌ای برای آسیب‌پذیری‌ها و تهدیدات قابل بهره‌برداری است یا خیر؟ این مرحله به منظور اثبات ادعا به کار می‌رود. برای دست‌یابی روش‌هایی وجود دارند که عبارت‌اند از: • دست‌یابی از طریق اینترنت و سایت‌های مرتبط با سازمان • دست‌یابی از طریق اکسپلویت • مهندسی اجتماعی • دست‌یابی بی‌سیم • انکار سرویس[2] • حمله پست الکترونیکی (هرزنامه) • تروجان‌ها
۷	نگه‌داری دست‌یابی	بعد از این‌که گروه مجری موفق به دسترسی شدند، نیاز به برگشت دوباره به داخل سیستم برای اجرای تست بیشتری دارند. این مرحله شامل نصب برنامه دروازه پشتی برای برگشت مجدد به داخل سیستم برای اجرای تست بیشتر است. در این قسمت نیز میزان امنیت سیستم هدف در مقابل‌نصب برنامه‌های دروازه پشتی۳ نیز سنجیده می‌شود. در برخی تست‌ها به دلیل زمان محدود یا عدم امکان دست‌یابی مجدد به سامانه این کار صورت نمی‌گیرد.
۸	از بین بردن رد پا	در این مرحله مجری سنجش نفوذپذیری همان‌طور که یک مهاجم ردپای خود را از بین می‌برد، به پاک کردن آثار حمله‌های انجام‌شده می‌پردازد.
۹	تهیه گزارش	در این مرحله مجری تست نفوذ، تمامی اکتشاف‌های خود را به صورت مستند در گزارشی جمع‌آوری می‌کند. این گزارش به سازمان مورد تست تحویل داده می‌شود. این مرحله ازجمله قسمت‌های مهم انجام عملیات سنجش نفوذپذیری است زیرا نتیجه تمامی تلاش‌های انجام‌شده در طی اجرای فرآیند تست، در این مستند باید جمع‌آوری شود.
۱۰	طرح برنامه برای زمان انجام تست‌های بعدی	بعد از این‌که گروه مجری تست، کار خود را به اتمام رساند و نتایج کار خود را به سازمان یا یگان مورد ارزیابی تحویل داد، باید برای انجام تست‌های بعدی زمان تعیین کند تا مطمئن شود سیستم هدف در مقابل آسیب‌پذیری‌هایی که در آینده اتفاق می‌افتد، مقاوم است. این کار با هماهنگی مبادی ذی‌ربط به صورت دوره‌ای یا غیرمترقبه طرح‌ریزی می‌شود.

1. Scanning (Enumeration)
2. Denial OF Service
3. Back Door

روش پیشنهادی در ۱۰ مرحله قابل‌برنامه‌ریزی و اجراست و نکته مهم این است کـه مراحـل پـنج‌گانـه اصلی فقط مبتنی بر ابزار است.

ابزارهای متن باز سنجش نفوذ

به منظور انجام سنجش نفوذپذیری بر اساس روش پیشنهادی روی مراحل پنج‌گانه اصلی نیـاز اسـت از تکنیک‌ها و ابزارهای خاص آن نیز استفاده گردد. معمولاً انجام فرآینـد سـنجش نفـوذ بـه دلیـل اسـتفاده از ابزارهای حرفه‌ای، گران‌قیمت و متن باز نبودن و عدم انعطاف‌پذیری آن‌ها بسیار پرهزینه و زمان‌بـر اسـت و به دلیل استفاده از ابزارهای غیرقابل تغییر و به‌کارگیری نامناسب آن‌ها غالباً موفقیـت چنـدانی در شناسـایی آسیب‌پذیری‌ها حاصل نمی‌گردد. در زیر تعدادی از مهم‌ترین ابزارهای متن باز و حرفه‌ای این حـوزه معرفـی می‌گردند که در گام‌های مختلف سنجش نفوذ کاربرد وسیعی دارند. ابزارهای سـنجش نفـوذ از نظـر پلتفـرم اجرایی به چند نوع تقسیم می‌شوند:

- مبتنی بر سیستم‌عامل ویندوز
- مبتنی بر سیستم‌عامل لینوکس
- مبتنی بر سیستم‌عامل مک
- مبتنی بر سایر سیستم‌عامل‌ها ازجمله FreeBSD، اندروید و ...

که ابزارهای مبتنی بر سه دسته اول رایج و اکثر نرم‌افزارهای سنجش نفوذ روی ایـن سیسـتم‌عامـل‌هـا ابزارهای خود را منتشر کرده‌اند.

ابزارهای سنجش نفوذ هم به صورت رایگان و هم به صورت سفارشی و غالباً با هزینه‌های بـالا عرضـه می‌گردند. هم‌چنین برخی از این ابزارها برای استفاده آسان و کاربردی ارزیابی‌کنندگان به صـورت مـتن بـاز طراحی‌شده‌اند که از محبوبیت بالایی برخوردار هستند.

نکته مهم در انتخاب این ابزارها ویژگی انعطاف‌پذیری، نصب روی چندین پلتفرم، قدرت بالا و پایـداری نرم‌افزار برای تست‌های طولانی و به‌کارگیری حافظه و پردازنده بالا، کاربری راحت و ساده، متن بـاز بـودن به منظور اعمال تغییرات ارزیاب، دارای راهنمای کاربری حرفـه‌ای و مناسـب، پشـتیبانی قـوی و مسـتمر و رایگان بودن آن است.

در زمینه سنجش نفوذپذیری، ابزارهای بسیار زیادی وجود دارد ویکی از بهترین سایت‌هـای مرجـع کـه ابزارهای جدید را به ما معرفی می‌کند سایت WWW.SECTOOLS.ORG می‌باشد (sectools, 2014).

پنج ابزار بسیار مهم متن باز با ویژگی‌های ذکرشده که در این تحقیق به آن‌ها پرداخته می‌شود شامل Kali Linux، Nmap، OpenVAS، Metasploit و Wireshark است.

استفاده از یک سیستم‌عامل سفارشی به منظور انجام سنجش نفوذپذیری بسیار ساده‌تر از تهیه و نصب ابزارهای موردنیاز این آزمون است. Kali linux با فراهم کردن یک محیط کاربرپسند، تمامی ابزارهای موردنیاز را نیز در دسته‌بندی‌های مناسب قرار داده است و در انجام یک آزمون نفوذ، می‌تواند کمک شایانی به‌صرفه جویی زمان و هم‌چنین جامعیت آن بنماید (Faircloth, 2011).

هدف از سیستم‌عامل Kali و نسل‌های قبلی آن از قبیل سیستم‌عامل BackTrack ، غلبه بر چالش‌هایی نظیر یک‌پارچه‌سازی مجموعه ابزارها جهت انجام مراحل مختلف آزمون نفوذ (مراحل شناخت، شناسایی آسیب‌پذیری‌ها، تسخیر سیستم، پاک کردن ردپا و نگه‌داری دسترسی) و نیز همگام‌سازی برای انجام مراحل مختلف نفوذ، مدیریت تیم و ابزارهایی برای ارائه خروجی‌های مناسب است. Kali Linux مجموعه ابزارهایی برای انجام مراحل مختلف سنجش نفوذ و بازرسی قانونی و تحلیل بد افزار دارد. مجموعه ابزارهای تعبیه‌شده در سیستم‌عامل Kali ، تمامی لایه‌های مرتبط با فرآیند سنجش نفوذ (شامل منابع انسانی، برنامه‌های کاربردی، سرویس‌ها، سیستم‌عامل، شبکه و پایگاه داده) را پوشش می‌دهد.

نرم‌افزار Nmap جهت اسکن کردن شبکه‌های بسیار بزرگ به معنی واقعی کلمه، یعنی صدها هزار رایانه در شبکه‌ها و اینترنت، استفاده می‌شود (Haubris & Pauli, 2013) و در مرحله شناسایی و پویش بسیار کاربردی است. Nmap مخفف Network Mapper می‌باشد و یک نرم‌افزار کاربردی برای پویشی شبکه یا ممیزی امنیتی شبکه به شمار می‌آید. این نرم‌افزار طوری طراحی‌شده که شبکه‌های بزرگ را به سرعت اسکن کند، اگرچه می‌تواند بر روی سیستم‌های تنها نیز به خوبی کار کند. Nmap از IP packet های خام به صورت منحصربه‌فرد استفاده می‌کند تا تعیین کند چه رایانه‌هایی (hosts) بر روی شبکه در دسترس می‌باشند، چه سرویس‌هایی (ports) ارائه می‌کنند، چه سیستم‌عامل‌هایی (به همراه نسخه سیستم‌عامل) بر روی آن‌ها در حال اجرا می‌باشد، چه نوع packet filter ها / فایروال‌هایی مورداستفاده قرار گرفته و چندین پارامتر دیگر. Nmap بر روی اکثر رایانه‌ها، هم گرافیکی و هم کنسول‌ها قابل‌استفاده است. Nmap یک نرم‌افزار مجانی است که به همراه کدهای آن تحت واژه GNU GPL در دسترس می‌باشد.

Wireshark یک آنالیزگر بسته‌های شبکه در شبکه و اینترنت است (T. Simpson, Backman, & E. Corley, 2011). یک آنالیزگر بسته، پکت‌هایی را که در شبکه رد و بدل می‌شوند به دام انداخته و آن‌ها را مورد پردازش قرار می‌دهد و در صورت امکان جزئیات آن را نمایش می‌دهد. درواقع این نرم‌افزار به‌طور

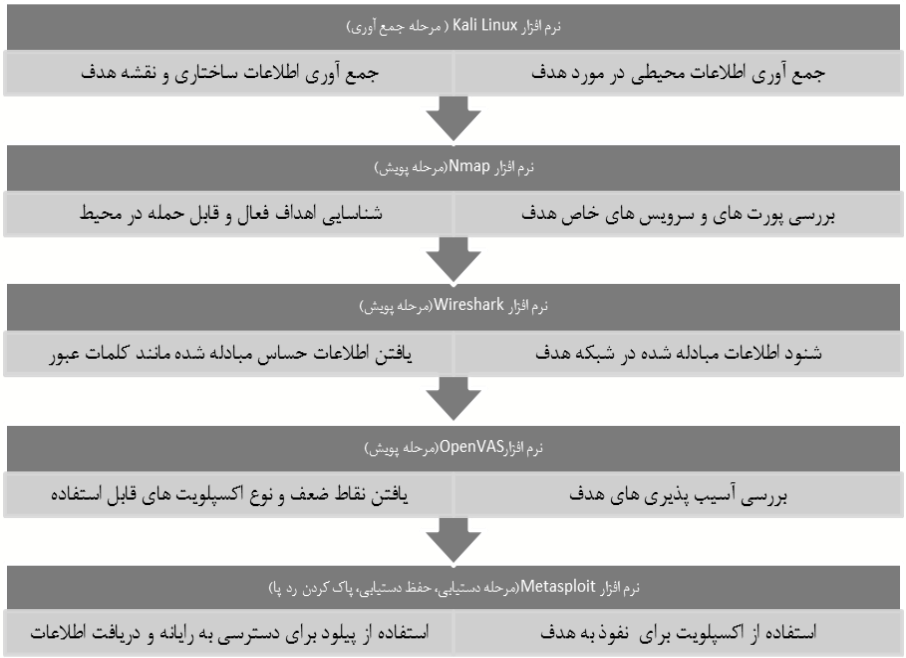
دقیق آنچه را که از طریق کابل می‌گذرد شنود کرده و موردبررسی قرار می‌دهد و در مرحله پویش، شناسایی و نفوذ شبکه بسیار کاربرد دارد. Wireshark نام جدید برنامه معروف Ethereal است که هم کنون در برخی از دانشگاه‌ها تدریس می‌شود. این برنامه بسیار قوی می‌تواند پروتکل‌های مختلف را شناسایی و حتی بسته‌های مختلف را که بر اساس مدل‌های شبکه از هم دورافتاده‌اند تشخیص داده در کنار یکدیگر قرار دهد و در حقیقت بسته را بازسازی نماید.

برای هک کردن سایت باید نقاط آسیب‌پذیری یا نقاط ضعف سیستم را تعیین کرد که برای این موضوع ابزارهای پویش و پویش نقاط آسیب‌پذیری بسیار زیادی وجود دارد اما از بین تمام این ابزارها OpenVAS که مبتنی بر Nessus است، ویژگی‌های بسیار بهتری دارد (طاهریان ریزی & اصغرزاده امین, ۱۳۸۹). ویژگی‌های این نرم‌افزار شامل موارد زیر است:

- کد برنامه‌نویسی آن open source و در اختیار عموم است.
- می‌توان کدهای لازم برای یک نقطه‌ضعف جدید را تعریف کنیم.
- تمام قابلیت‌های nmap در OpenVAS وجود دارد.
- OpenVASدر linux و انواع ویندوز قابل‌نصب است.
- OpenVAS دارای هزاران pluginاست که برای سنجش آسیب‌پذیری‌ها باید plugin مربوط به آن آسیب‌پذیری روی نرم‌افزار وجود داشته (به‌روزرسانی شده) و فعال باشد.

نرم‌افزار Metasploit یک نرم‌افزار قوی برای نفوذ به سیستم‌های دیگر است. این نرم‌افزار امکان دسترسی به شل قربانی را به راحتی حتی بر روی ویندوز ۷ فراهم می‌کند (Wilhelm & Neely, 2013) و در مرحله نفوذ و گرفتن دسترسی بسیار کاربردی است. این نرم‌افزار، پیوندی بین IP موردنظر با فایل نفوذ داده شده ایجاد می‌کند. کسی که روی این پیوند کلیک کند، این فایل را وارد رایانه خود کرده و پس از وارد شدن این فایل به رایانه فرد، نفوذ گر می‌تواند به راحتی دستورهای گوناگون را بر روی رایانه قربانی اجرا کند. در حقیقت Metasploit یک ابزار قدرتمند برای اکسپلویت کردن و بهره‌برداری از آسیب‌پذیری‌ها و باگ های نرم‌افزاری سامانه‌ها است.

در شکل ۵ شمای به‌کارگیری ابزارهای سنجش نفوذ متن باز بر اساس روش بومی در مراحل پنج‌گانه اصلی ارائه می‌گردد:



شکل ۵: مراحل استفاده از ابزارهای سنجش نفوذپذیری

شکل فوق نشان می‌دهد که ابزارهای پویش در مرحله ۵ روش پیشنهادی از اهمیت بالاتری برخوردار است.

ارزیابی روش پیشنهادی مبتنی بر ابزار متن باز روی مراحل پنج‌گانه اصلی

به منظور ارزیابی روش پیشنهادی مبتنی بر ابزار متن باز روی مراحل پنج‌گانه (از مرحله ۴ تا ۸) ۲۰ شبکه که دارای ۵۰ تا ۸۰۰ رایانه بودند، انتخاب گردیدند. بر اساس این روش و با ابزارهای متن باز معرفی‌شده، شبکه‌ها موردسنجش نفوذپذیری قرار گرفتند. شبکه‌های انتخابی دارای وضعیت‌های مختلف امنیتی با برنامه‌ها، سرورها و تجهیزات مختلف شبکه و تنظیمات امنیتی متفاوت بودند و از الگوهای مختلف برای امنیت خود استفاده می‌کردند.

برای ارزیابی این روش از مقیاس لیکرت در امتیازدهی به عملکرد قابل‌قبول هر ابزار استفاده شد. در این روش امتیازدهی به صورت کم، نسبتاً کم، متوسط، زیاد و خیلی زیاد انجام گرفت و میزان موفقیت هر یک از ابزارها مبتنی بر نتایج ابزارهای مرحله قبل مورد ارزیابی قرار گرفت. برای ارزیابی نرم‌افزارهای متن

باز این ابزارها روی هر یک از شبکه‌ها به صورت شکل ۵ (نحوه به‌کارگیری ابزارها) اجرا گردید. به دلیل نوع تست و خروجی متفاوت هر یک از ابزارها حتی تست متفاوت آن‌ها، در پرسشنامه به جزئیات خروجی نرم‌افزارها نپرداخته‌ایم و فقط به میزان قابل‌قبول بودن خروجی و درصد موفقیت آن‌ها اشاره‌شده است. قابل‌قبول بودن خروجی هر یک از نرم‌افزارها بر اساس سابقه و تجربه محققان در فعالیت سنجش نفوذپذیری و قابل‌استفاده بودن هر یک از خروجی‌ها برای ابزار بعدی است. سؤالات پرسشنامه مبتنی بر نوع نرم‌افزار و وظیفه هر نرم‌افزار در مراحل سنجش نفوذ تعریف‌شده است. هم‌چنین لازم به ذکر است ازآنجایی‌که هر یک از این ابزارها باید وظایف مطرح‌شده در هر پرسش را به صورت یک‌پارچه انجام دهد تا خروجی قابل‌اندازه‌گیری به صورت پارامتری واحد از آن به دست آید، لذا نیاز است در پرسش‌های مطرح‌شده حتماً چند وظیفه مرتبط با آن ابزار در کنار یکدیگر قرار گیرد تا خروجی موردنظر به عنوان یک پارامتر استخراج شود.

۱- آیا خروجی نرم‌افزار kali linux در جمع‌آوری اطلاعات محیطی و ساختاری و نقشه شبکه هدف قابل‌استفاده بوده و از کیفیت لازم برای ورودی مرحله پویش برخوردار است؟

۲- تا چه میزان خروجی نرم‌افزار Nmap شامل اهداف فعال، قابل حمله و سرویس‌های فعال هدف را نشان می‌دهد؟

۳- خروجی نرم‌افزار Wireshark تا چه حدی حاوی اطلاعات حساس و مبادله شده در شبکه هدف است؟

۴- آیا خروجی نرم‌افزار Openvas حاوی آسیب‌پذیری‌های شبکه هدف بوده و این آسیب‌پذیری‌ها قابلیت استفاده به عنوان ورودی مرحله دست‌یابی را دارد؟

۵- آیا نرم‌افزار Metasploit قابلیت نفوذ به هدف، حفظ دسترسی و پاک کردن رد پا را در هر حمله به هدف دارا است. به‌عنوان‌مثال در صورتی که نرم‌افزار OpenVAS نتایج متوسطی از تحلیل آسیب‌پذیری‌ها ارائه می‌کرد، چون نرم‌افزار Metasploit بر اساس نتایج OpenVAS از مرحله قبل، عمل می‌کند لذا خروجی آن وابسته به مراحل قبلی بوده و باید میزان موفقیت این نرم‌افزار مبتنی بر نتایج مرحله قبل ارزیابی گردد. نام‌گذاری شبکه‌ها به دلیل حفظ محرمانگی به صورت حروف الفبا انجام‌شده است.

جدول ۳ نتایج ارزیابی را بر اساس مقیاس لیکرت و میزان موفقیت هر ابزار در مراحل پنج‌گانه (۴ تا ۸) روش پیشنهادی نشان می‌دهد.

جدول ۳- ارزیابی موفقیت ابزارهای متن باز سنجش نفوذ در مراحل پنج‌گانه (٤ تا ٨) از روش پیشنهادی

ابزارمتن / شبکه‌ها	Kali	Nmap	Wireshark	OpenVAS	Metasploit
شبکه ۱	زیاد	متوسط	زیاد	خیلی زیاد	زیاد
شبکه ۲	زیاد	زیاد	زیاد	زیاد	زیاد
شبکه ۳	متوسط	زیاد	متوسط	متوسط	متوسط
شبکه ۴	خیلی زیاد	خیلی زیاد	زیاد	خیلی زیاد	زیاد
شبکه ۵	زیاد	زیاد	زیاد	متوسط	متوسط
شبکه ۶	متوسط	متوسط	متوسط	متوسط	متوسط
شبکه ۷	زیاد	زیاد	متوسط	متوسط	متوسط
شبکه ۸	متوسط	متوسط	متوسط	کم	خیلی کم
شبکه ۹	خیلی زیاد	خیلی زیاد	خیلی زیاد	خیلی زیاد	خیلی زیاد
شبکه ۱۰	کم	کم	متوسط	خیلی کم	کم
شبکه ۱۱	متوسط	کم	متوسط	کم	کم
شبکه ۱۲	زیاد	زیاد	زیاد	متوسط	متوسط
شبکه ۱۳	زیاد	خیلی زیاد	خیلی زیاد	زیاد	زیاد
شبکه ۱۴	زیاد	متوسط	کم	متوسط	کم
شبکه ۱۵	خیلی زیاد	متوسط	زیاد	زیاد	زیاد
شبکه ۱۶	خیلی کم	کم	خیلی کم	کم	کم
شبکه ۱۷	زیاد	خیلی زیاد	خیلی زیاد	خیلی زیاد	خیلی زیاد
شبکه ۱۸	کم	خیلی کم	متوسط	کم	خیلی کم
شبکه ۱۹	متوسط	متوسط	کم	متوسط	متوسط
شبکه ۲۰	خیلی زیاد	زیاد	زیاد	زیاد	متوسط

جدول ۴ بیانگر نگاشت یک معیار عددی به معیار کیفی در طیف لیکرت است.

جدول ٤- طیف لیکرت

معیار	وزن
خیلی کم	۱
کم	۲
متوسط	۳
زیاد	۴
خیلی زیاد	۵

سعی شده است با استفاده از این طیف، مقادیر کیفی به‌دست‌آمده در جدول ۳ را بـه یـک مقـدار کمـی نگاشت کرد و نتیجه آن به صورت میانگین برای هر ابزار و میانگین کلی موفقیت ابزارها در ایـن روش کـه مبتنی بر نتایج مرحله قبل است، ارائه شود.

جدول ۵ نتایج حاصل از ارزیابی نهایی مبتنی بر میـانگین و انحـراف معیـار از موفقیـت ابزارهـا و روش پیشنهادی ارائه‌شده است.

جدول ۵- نتایج میانگین و انحراف معیار ارزیابی روش پیشنهادی

ابزار / شاخص	Kali	Nmap	Wireshark	OpenVAS	Metasploit
میانگین	۳,۶	۳,۴۵	۳,۴۵	۳,۳	۳,۰۵
انحراف معیار	۱,۰۶۷۷۰۸	۱,۱۱۶۹۱۵	۱,۰۲۳۴۷۴	۱,۱۴۴۵۵۲	۱,۱۱۶۹۱۵

میانگین نهایی حاصل از روش پیشنهادی ۳,۳۷ و انحراف معیار نهایی داده‌ها ۱,۱۱ ارزیابی‌شده است که نشان‌دهنده بالاتر بودن موفقیت ابزارها از حد متوسط و به سمت زیاد است که قابل‌قبـول بـودن ایـن روش مبتنی بر ابزارهای اشاره‌شده را تأیید می‌کند.

میزان موفقیت هر یک از ابزارها به مفهوم میزان کارایی و اثربخشی هر یک از ابزارها است. کارایی هر ابزار به میزان درست انجام دادن وظایف تعیین‌شـده بـرای هـر یـک از گـام‌هـای فرآینـد سـنجش نفـوذ و اثربخشی هر ابزار به خروجی مناسب و قابل بهره‌برداری برای مرحله بعدی که درنهایت منجر بـه در اختیـار گرفتن سیستم هدف شود، بستگی دارد.

با توجـه بـه نتـایج حاصـل از جـدول ۵ ابزارهـایی کـه در مراحـل جمع‌آوری و پـویش مورداسـتفاده قرارگرفته‌اند میزان موفقیت بالاتری نسبت به مراحل بعدی دارند. هم‌چنین ابزارهـای kali و wireshark از موفقیت بالاتری نسبت به سایر ابزارها برخوردار می‌باشد.

ضریب همبستگی روشی برای اندازه‌گیری میزان شدت وابستگی دو متغیر به یکـدیگر اسـت کـه تـأثیر افزایش یک متغیر برافزایش یا کاهش متغیر دیگر را نشان می‌دهد. با محاسبه این ضریب می‌توان وابستگی دو ابزار را به یکدیگر در مراحل مختلف سنجش نفوذ روش پیشنهادی نشان داد.

جدول ۶ شدت وابستگی و میزان همبستگی ابزارهای سنجش نفوذ برای مراحل مختلف را نشان می‌دهد.

جدول ٦- ضریب همبستگی بین ابزارهای سنجش نفوذ

همبستگی بین ابزارها	Kali & Nmap	Nmap & Wireshark	Wireshark & OpenVAS	OpenVAS & Metasploit	Kali & Metasploit	Nmap & Metasploit	Wireshark & Metasploit
ضریب همبستگی	۰,۷۳۷۹۲۱	۰,۶۹۷۶۴۳	۰,۶۹۵۷۳۷	۰,۸۸۷۸۵۱	۰,۶۸۷۶۰۸	۰,۷۸۳۵۶۷	۰,۷۲۳۸۸۷

با توجه به جدول ۶، وابستگی دو ابزار پویش آسیب‌پذیری (OpenVAS) و بهره‌برداری از آسیب‌پذیری برای نفوذ (Metasploit) از سایر ابزارهای دیگر در مراحل مختلف سنجش نفوذ بالاتر است و می‌توان نتیجه گرفت که با افزایش کارایی و اثربخشی ابزار OpenVAS و خروجی جامع و مناسب از تحلیل آسیب‌پذیری‌ها، می‌توان عملیات نفوذ و دسترسی به هدف توسط Metasploit را با موفقیت بیشتری انجام داد. هم‌چنین ابزار پویش پورت و شناسایی هدف (Nmap) از تأثیرگذاری بالایی برای موفقیت ابزار Metasploit برخوردار است.

درواقع اگر ابزارهای مراحل اولیه دارای خروجی قابل‌قبول با اثربخشی بالایی باشند سبب افزایش موفقیت ابزارهای مراحل نهایی می‌گردد.

نتایج

در ابتدا روش‌های مختلف سنجش نفوذپذیری، استانداردها و تاکتیک‌های مختلف بررسی شدند. سپس با توجه به تجربیات محققان و بررسی عمیق روش‌های سنجش نفوذ، یک فرآیند سنجش نفوذپذیری بومی برای محیط‌هایی که دارای شرایط خاص حاکمیتی و سیاست‌های ویژه و سخت‌گیرانه‌ای هستند، ارائه شد که این متدولوژی برای محیط‌های غیر سازمانی یا محیط‌های بااهمیت کم‌تر نیز کاربردی است. فرآیند ارائه‌شده دارای پنج مرحله اصلی شامل جمع‌آوری، پویش، دست‌یابی، نگه‌داری دست‌یابی و پاک کردن رد پا است که برای این مراحل، ابزار حرفه‌ای متن باز Kali، Nmap، Wireshark، OpenVAS و Metasploit انتخاب و مورداستفاده قرار گرفت.

بر اساس روش پیشنهادی از این ابزارها در ۲۰ شبکه استفاده گردید که نتایج موفقیت هر یک از ابزارها بر اساس طیف لیکرت نشان داد که میانگین ۳,۳۷ با انحراف معیار ۱,۱۱ بوده و بالاتر از حد متوسط است و می‌تواند به عنوان یک روش قابل‌اطمینان استفاده گردد. هم‌چنین بر اساس مقایسه میزان ضریب همبستگی بین ابزارهای سنجش نفوذ، ابزار نفوذ و حفظ دسترسی با ضریب همبستگی ۰,۸۸۷۸۵۱ بیش‌ترین وابستگی را به ابزار پویش آسیب‌پذیری دارد. فرآیند سنجش نفوذ پیشنهادی به همراه ابزارهای معرفی‌شده می‌تواند به منظور سنجش و ارزیابی میزان نفوذپذیری شبکه‌های داخلی مورداستفاده قرار گیرد. با استفاده از ایـن روش می‌توان، نقاط ضعف شبکه و سامانه‌ها را شناسایی و تا قبل از سو استفاده توسط افراد ناراضی و نفوذ گر هـا نسبت به ایمن‌سازی و رفع آن‌ها اقدام کرد.

کتابنامه

اصغرزاده امین، (۱۳۸۹). ***آموزش گام به گام هک و ضد هک کامپیوتر***، تهران: انتشارات طاهریان.

نوری، رضا و دیگران، (۱۳۸۹). ***راهنمای جامع آزمون نفوذ گر اخلاقی***، تهران: انتشارات انستیتو ایز ایران.

Faircloth, J. (2011). Penetration Tester's Open Source Toolkit. waltham: syngress.

Graves, K. (2010). CEH: Certified Ethical Hacker Study Guide. Indianapolis: Wiley.

Haubris, K. P., & Pauli, J. J. (2013). Improving the Efficiency and Effectiveness of Penetration Test Automation. 2013 10th International Conference on Information Technology: New Generations, 387-391.

herzog, p., & Barceló, M. (2010). OSSTMM 3– The Open Source Security Testing Methodology Manual. ISECOM.

McClure, S., Scambray, J., & Kurtz, G. (2009). HACKING EXPOSED 6:NETWORK SECURITY SECRETS & SOLUTIONS. New York: McGraw-Hill.

Muller, A., & Meucci, M. (2014). OWASP TESTING GUIDE v4.0.

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R. K.,... Chavan, U. (2006). Information Systems SecurityAssessment Framework(ISSAF)draft 0.2. Open Information Systems SecurityGroup.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. Gaithersburg: National Institute of Standards and Technology.

sectools. (2014). Top network security tools. Retrieved 2014, from WWW.SECTOOLS.ORG

T. Simpson, M., Backman, K., & E. Corley, J. (2011). Hands-On Ethical Hacking and Network Defense,Second Edition. Boston,: Course Technology, Cengage Learning.

Wilhelm, T., & Neely, M. (2013). Professional penetration testing– Second edition. Waltham: Elsevier, Inc.

Yeo, J. (2013). Using penetration testing to enhance your company's security. Computer Fraud & Security, 17-20.

Young, S. (2014). Using Open Source Reconnaissance Tools for Business Partner Vulnerability Assessment. SANS Institute.