اولین همایش ملی پیشرفت های تکنولوژی در مهندسی برق، الکترونیک و کامپیوتر

First National Conference of Technology Developments on Electronical, Electronics and Computer Engineering

. . . W W W . T D E C O N F . I R . . .

نفوذ در یک شبکه با استفاده ازآسیب پذیریهای پروتکل مدیریت آسان شبکه و ایجاد اختلال با استفاده از حملات انسداد سرویس

حامد حدادی[۱]، دکتر مینا زلفی لیقوان[۲]

[۱]دانشگاه آزاد اسلامی واحد اهر، haddadi_vcc@yahoo.com

[۲]دانشگاه تبریز،mzolfy@tabrizu.ac.ir

چکیده: پروتکل مدیریت آسان شبکه (SNMP) برای مدیریت و مانیتورینگ شبکه از راه دور بکار میرود و اغلب از ارتباطات UDP بر روی پورتهای ۱۶۱ و ۱۶۲ استفاده میکند.با استفاده از این پروتکل می توان کنترل و پیکربندی روترها را از راه دور بدست گرفت.در این پژوهش آسیب پذیریهای پروتکل مدیریت آسان شبکه بررسی شده و نتایج حاصل از نفوذ به یکی از روترها در یک شبکه از طریق این آسیب پذیریها نشان داده شده است.همچنین یک نمونه از حملات انسداد سرویس(DoS)که موجب اختلال در شبکه میشود انجام شده و در انتها راه حل هایی جهت جلوگیری از این نوع حملات ارائه داده شده است.هدف از این کار تحقیقاتی یافتن برخی ضعفها و آسیب پذیریهای موجود و ارائه راهکار برای جلوگیری از خطرات احتمالی میباشد.

واژگان کلیدی: UDP ، SNMP ، DoS

مقدمه

اهمیت شبکه های رایانه ای بر کسی پوشیده نیست. در جهان امروز، رایانه به عنوان یک وسیلهٔ مجرد، به تنهایی نمی تواند به طور کامل مفید واقع شود و بازدهی کامل داشته باشد. آنچه به رایانه اهمیتی فراتر از سابق می بخشد نقش آن در ارتباطات و انتقال دریای عظیمی از اطلاعات گوناگون است. هرچه زمان می‌گذرد حجم اطلاعاتی که انسان با آن سر و کار دارد بیشتر و بیشتر می شود. با توجه به مزیت های مختلف شبکه (کاهش هزینه، صرفه جویی در وقت، حذف محدودیت های جغرافیایی و ...)، شاهد پیشرفت روزافزون این شاخه علمی می شویم. شبکه های رایانه‌ای امروزی، فصل نوینی در انفورماتیک گشوده‌اند و نزدیک است مفهوم دهکدهٔ جهانی را تحقق بخشند. مدیریت شبکه مفهومی است که از ابزارها و تکنیک های مختلف به منظور مدیریت شبکه ها و سیستم ها استفاده می کند. مدیریت شبکه شامل پنج عملکرد اصلی است که عبارتند از: مدیریت خطا، مدیریت تنظیمات، مدیریت حسابداری، مدیریت اجرا و مدیریت امنیت[۱].

در شبکه های کامپیوتری که ترکیبی از روترها، سوییچ ها و سرورها هستند، به منظور مدیریت همه ابزارها در شبکه باید کاری انجام شود تا بتوان از کارکرد بهینه آنها آگاه شد .اینجاست کهSNMP ، پروتکل مدیریت آسان شبکه، می تواند کمک کند. این پروتکل در سال ۱۹۸۸ معرفی شد تا احتیاجات رشد یافته‌ای را در پروتکلی به منظور مدیریت ابزارهایی که بر پایه پروتکل IP کار می کنند، اعمال کند. هسته اصلی SNMP مجموعه ساده‌ای از عملیات است که به مدیران سیستم توانایی تغییر در محدوده ابزارهایی که بر پایه این پروتکل کار می کنند را، فراهم می کند. همچنین امکان اداره کردن، بازبینی و پشتیبانی از شبکه های کامپیوتری دور یا محلی که بر اساس TCP/IP کار می کنند، میسر می شود و در واقع راهی استاندارد به منظور یافتن اطلاعات شبکه ای است. در مقایسه با SGMP که تنها برای مدیریت روترهای اینترنت ایجاد شد، SNMPبرای مدیریت Unix، Windows، پرینتر ها، Modem Rackها و غیره به کار می رود. مانیتور کردن شبکه به منظور درک بهتر چگونگی کارکرد شبکه، از دیگر عملکردهای مدیریت شبکه است که نه تنها برای ترافیک های محلی به کار نمی رود، بلکه برای interface های شهری نیز استفاده می شود[۱].

۱- پروتکل

یک پروتکل شبکه، زبانی است که سیستم ها از آن استفاده می کنند تا با یکدیگر ارتباط برقرار کنند. وقتی که دو سیستم بخواهند با یکدیگر ارتباط برقرار کنند، برای این منظور زبان مشابهی (یا پروتکل) لازم است. شبکه های کامپیوتری به پروتکل‌های مختلفی نیاز دارند. این پروتکل‌ها صریح و دارای چارچوب مشخص میباشند. پروتکل‌ها در انواع مختلفی وجود دارند. در پایین‌ترین سطح، پروتکل‌ها دقیقاً تعریف میکنند که چه نوع سیگنال های الکتریکی مولد ۱ و چه نوع آنها مولد ۰ میباشند. در بالاترین سطح، پروتکل این امکان را به کاربر کامپیوتر میدهد تا پیغامی را از طریق پست الکترونیکی به دوست خود در آن سوی دنیا ارسال کند[۲].برخی از پروتکلهای پرکاربرد در شبکه عبارتند از :

۱-۱- TCP/IP

پروتکلی جهت ارتباط بین کامپیوترها در یک شبکه برای انتقال داده بر اساس استاندارد پروتکلهای اینترنت می‌باشد و اینترنت نیز ارتباطی از سیستمهای تحت شبکه که جهت ارتباط در سطح جهان از پروتکلTCP/IP استفاده میکنند[۲].

DHCP -۲-۱

DHCP پروتکلی جهت تخصیص آدرسهای IP به صورت اتوماتیک به تجهیزات موجود در شبکه می‌باشد. با استفاده از این پروتکل کامپیوتر در لحظه اتصال به شبکه می تواند یک آدرس از همان شبکه را به خود اختصاص دهد[۲].

DNS -۳-۱

DNS یک سرویس اینترنتی است که نامهای دامنه را به آدرسهای IP ترجمه می کند. چرا که اسم دامنه بر اساس حروف الفباء بوده و امکان یادگیری آن آسان می باشد. در حالیکه اینترنت برپایه آدرس IP کار می‌کند[۲].

VLAN -۴-۱

VLAN پروتکلی است که امکان دسته بندی چندین LAN را در اختیار می‌گذارد.بدین معنا که ماشینهای هر VLAN بر روی یک شبکه LAN بدون دسترسی به ماشینهای دیگر در شبکه کارکنند که مزایای آن قابلیت مدیریت و امنیت است[۲] .

TFTP -۵-۱

TFTP یک فرم ساده FTP است که از پروتکل UDP برای انتقال استفاده می کند که هیچ امنیتی روی انتقال داده ندارد و فقط امکان به اشتراک گذاشتن فایل را فراهم می سازد[۲].

FTP -۶-۱

FTP پروتکلی روی اینترنت برای تبادل فایل است که از پروتکل TCP/IP برای انتقال استفاده می کند و بنابراین علاوه بر برقراری امنیت امکان به اشتراک گذاری دایرکتوری را فراهم می کند[۲] .

UDP -۷-۱

UDP پروتکلی از مجموعه پروتکل TCP/IP است که عموما" برای انتقال بسته های Video وreal-time Voice استفاده میشود و بازیابی خطا در آن انجام نمی‌گیرد[۲].

SNMP -۸-۱

SNMP ازمجموعه پروتکلهای مدیریتی برای مدیریت شبکه‌های پیچیده است. اولین ورژن آن در اوائل سال ۸۰ ارائه شد و به طور کلی یک پروتکل مانیتورینگ روی تجهیزات شبکه و عملکرد آنها است. SNMP محدود به شبکه های TCP/IP نمی باشد[۲].

۲- پروتکل مدیریت آسان شبکه (SNMP)

پروتکلSNMP برای سیستم های مدیریت در شبکه به منظور مانیتورینگ تجهیزات نصب شده در شبکه کاربرد دارد و شامل یک لایه کاربردی، یک پایگاه داده و بخش داده میباشد. داده مدیریتی، پیکربندی سیستم را توصیف می نماید. داده ها توسط کاربردهای مدیریتی تنظیم و مقداردهی می شوند. معماری و ساختار SNMP متشکل از مجموعه ای از ایستگاه‌های مدیریت شبکه و المان‌های شبکه است. المان‌های مدیریتی کاربردهای مربوط به مدیریت را اجرا می کنند . این المان ها وظیفه کنترل و مانیتورینگ تجهیزات شبکه را بر عهده دارند. SNMP ارتباط بین المانهای مدیریتی و المان‌های شبکه را در لایه کاربرد OSI برقرار می نماید. هر سیستم مدیریتی با استفاده از یک بخش نرم‌افزاری (agent) اطلاعات لازم را از طریق SNMP به سیستم مدیریتی منتقل می نماید. مدیریت می‌تواند درخواستها را از طریق هر پورت مبدا به پورت ۱۶۱ یک agent بفرستد و هر agent پاسخ درخواست مدیریت را به پورتهای مبدا میفرستد. مدیریت، پیامهای هشدار و اطلاع رسانی را از طریق پورت ۱۶۲ دریافت می‌نماید، اما یک agent اجازه دارد پیام‌های هشدار و اطلاع رسانی را از طریق هر پورت در دسترس خود ارسال نماید.تاکنون سه نسخه از این پروتکل ارائه گردیده است[۳].

تجهیزات شبکه که از پروتکل SNMP استفاده می نمایند، یک گره مدیریتی در شبکه تشکیل میدهند. این گره‌ها و تجهیزات مدیریتی، وظیفه جمع آوری و ذخیره اطلاعات مدیریتی و تبدیل آ نها به داده هایی قابل استفاده برای SNMP را بر عهده دارند[۳].

یک agent درواقع یک ماژول نرم افزاری مدیریت شبکه است و در مورد داده های محلی گره شبکه، اطلاعات مدیریتی دارد وآنها را به فرمت قابل تفسیر SNMP ، ترجمه مینماید[۳].

ساختار مدیریتی توسط زیربخشی از SNMP با نام MIB تعریف می شود.MIB ساختار مدیریتی یک سیستم را توصیف می کند. هر واحد MIB با نام OID یا (Object Identifier) نام دارد و متغیری را در بر میگیرد که توسط SNMP قابل خواندن و تفسیر میباشد. هر OID می تواند به لایه ای از OSI مربوط باشد[۳].

پروتکل SNMP ، دارای یک متعادل کننده بار نیز می باشد. این بخش (dispatcher) وظیفه مدیریت ترافیک بار را در SNMP برعهده دارد. برای بسته های داده ای که خارج میشوند، یک dispatcher نوع پیام و نوع پردازشی که باید روی آن انجام پذیرد، را مشخص مینماید. سپس پیام را به ماژول مورد نظر راهنمایی مینماید. Dispatcher پیام مربوطه را برای ارسال به لایه انتقال می سپارد .برای پیام های ورودی ، dispatcher پیام ها را از لایه انتقال دریافت مینماید و هر پیام را به ماژول متناظر برای پردازش می دهد و پیام را به کاربرد موردنظر راهنمایی مینماید[۳].

بخش های امنیتی همانند احراز هویت، محرمانگی و یکپارچگی در نسخه سوم SNMP مورد توجه قرار گرفته است. در بخش احراز هویت از الگوریتمهای رمزنگاری MD5 و SHA1 استفاده می شود و DES ، 3DES و AES در رمزگذاری بسته ها در پروتکل SNMP v3 کاربرد دارد. به منظور حفظ محرمانگی، احراز هویت پیام بایستی الزامی باشد[۴].

۳- آسیب پذیریهای پروتکل مدیریت آسان شبکه

با اینکه SNMP به عنوان یک ابزار مانیتورینگ و لاگ گیری برای مدیران شبکه کاربرد فراوانی دارد اما دارای ضعف های امنیتی متعددی است. اغلب مدیران شبکه از نسخه پیش فرض این پروتکل جهت کنترل و نظارت بر شبکه بهره میگیرند که با توجه به اینکه در نگارش ۱ و ۲ از این پروتکل، اطلاعات بصورتی ارسال می شود که قابل خواندن توسط انسان می باشد. در نتیجه اطلاعات ارسالی، قابل شنود و دستکاری است. به عبارت دیگر نسخه های ۱ و ۲ این پروتکل بدلیل عدم استفاده از رمزنگاری در برابر حملات packet sniffing آسیب پذیر هستند. همچنین به دلیل اینکه منشا و فرستنده درخواست های SNMP قابل تائید و شناسایی نیست، امکان ارسال درخواست‌هایی با نشانی های IP جعلی وجوددارد. همه نگارش‌های پروتکل SNMP نیز در مقابل حملات از نوع Brute Force آسیب‌پذیر هستند. همچنین این پروتکل در مقابل حملات لغت‌نامه‌ای ناامن است. همچنین در برخی پیاده‌سازی‌های نسخه سوم این پروتکل آسیب‌پذیری Authentication ByPass گزارش شده که براساس آن امکان کاهش طول کد HMAC بسته ها، تا یک بایت و امکان حمله جستجوی کامل وجود دارد. HMAC(Hash-based message authentication code) یک الگوریتم احراز هویت پیام است و اساسا روشی برای ترکیب کردن کلید مخفی با الگوریتمهای درهم ساز فعلی میباشد.نفوذگر با استفاده از این آسیب پذیری می‌تواند اشیا تحت مدیریت را پیکربندی کند. موقعی که پروتکل snmp فعال است، مهاجمان می توانند با ارسال ناهنجار پیامهای snmp به تجهیزات آسیب پذیر آنها را از کار بیاندازند و با استفاده از DoS آن تجهیزات را از راه دور کنترل کنند[۴].

۴- حملات انسداد سرویس یا DoS

حملات اینترنتی و سایبری فقط شامل بدست آورن پسورد و تخریب سیستم ها نمی باشند، در برخی از حملات ایجاد اختلال در سیستم ها و عدم دسترسی کاربران به سیستم های حمله شده هدف مهاجمان و هکرها می باشد. این نوع حملات به حملات اختلال سیستم، عدم دسترسی، انسداد سرویس یا Dos(Denial of Service) معروف می‌باشند که از خطرناک‌ترین حملات سایبری هستند و موجب قطع سرویس‌دهی و به بار آمدن زیان‌های مالی هنگفتی می‌شوند که میزان آن به مدت‌زمان حمله بستگی دارد. هدف اکثر مهاجمان در این نوع حملات وب سرورهای بانکها، درگاههای پرداخت الکترونیکی و Name server ها می‌باشد. حملات DoS فقط مختص شبکه های کامپیوتری نمی‌باشد. برای مثال در برنامه های مدیریت منابع CPU نیز از این حملات استفاده می‌شود. در DoS مهاجم به واسطه یک برنامه درخواست‌های متعدد به سرور هدف ارسال می‌کند تا بدین وسیله دسترسی به شبکه را از سرور وب سلب کند. به این سبب دیگر کاربران معتبر قادر به دسترسی به وبسایت نیستند. در این هنگام اگر شما سعی در بارگزاری وبسایت داشته باشید با پیغام خطای Network Timeout مواجه خواهید شد[۵].

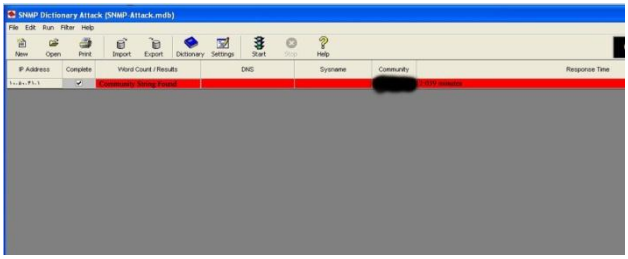
۵- آزمایشات انجام یافته

۵-۱- نفوذ به یک شبکه با استفاده از SNMP

با توجه بر اینکه تمامی بانکها و موسسات مالی از خط دیتا جهت ارتباطات خود استفاده میکنند نفوذ و حمله به آنها خارج از شبکه تقریبا غیرممکن است ولی کاربران داخلی بدلیل اینکه به شبکه دسترسی دارند می توانند از طریق پورتهای باز، شبکه را تحت تاثیر نفوذ و حمله خود قرار دهند. به عنوان مثال در راستای انجام آزمایشات این پژوهش شبکه یکی از موسسات مالی که از نسخه دوم پروتکل SNMP استفاده میکنند انتخاب شده است. پس از دسترسی به این شبکه پیکربندی روتر آن بدست آمد.برای این منظور ابتدا برنامه SolarWinds Engineer نصب شد. شکل ۱ نوار ابزار برنامه solarwinds را نشان میدهد.

شکل ۱ نوار ابزار برنامه solarwinds

سپس با استفاده از ابزار SNMP Dictionary Attack، snmp در روتر هدف پیدا شد(شکل ۲).

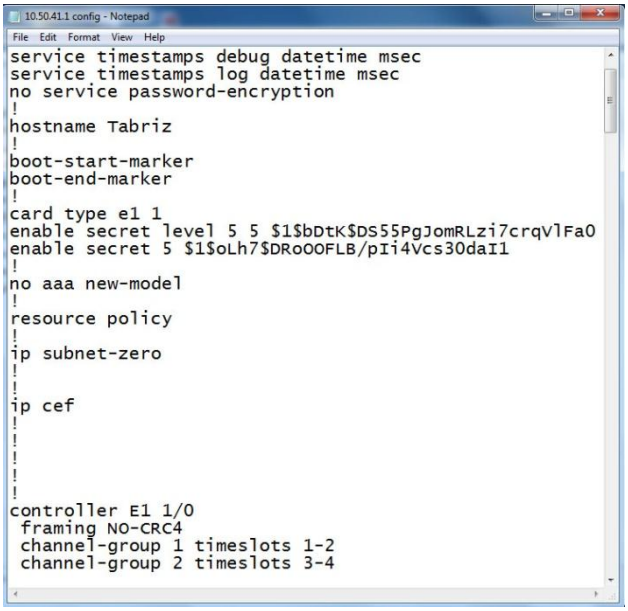


شکل ۲ بدست آوردن snmp روتر هدف

پس از آن snmp و IP روتر مورد نظر در برنامه cisco config download قرار داده شد و براحتی پیکربندی روتر هدف مورد دسترسی قرار گرفت(شکل ۳).

شکل ۳ بدست آوردن پیکربندی روتر هدف

البته این عملیات بسته به نوع و Range روترهایی که اسکن میشود دارد دربسیاری موارد میتوان از طریق snmp dictionary attack به جواب رسید و در صورت عدم موفقیت آمیز بودن این روش، می توان از snmp brute force attack به جواب رسید. شکل ۴ پیکربندی بدست آمده از روتر در مورد آزمایش را نشان میدهد.



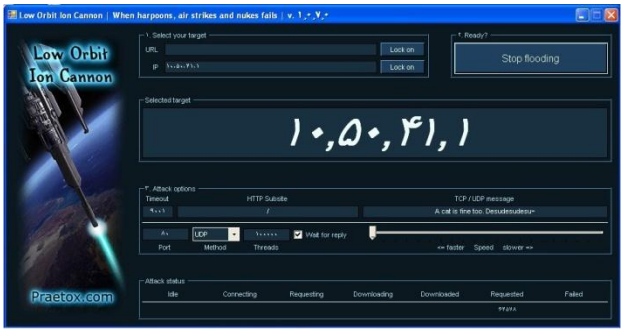
شکل ۴ پیکربندی روتر

پس از بدست آوردن پیکربندی روتر می توان username و password روتر را که در config بدست آمده وجود دارد کشف و با یک telnet ساده وارد روتر شد ولی چون همانطور که در شکل۴ مشاهده میشود پسورد رمز شده است ما با استفاده از برنامه cisco router password decryption رمز را هم بدست آوردیم (شکل ۵)

شکل ۵ کدگشایی رمز روتر

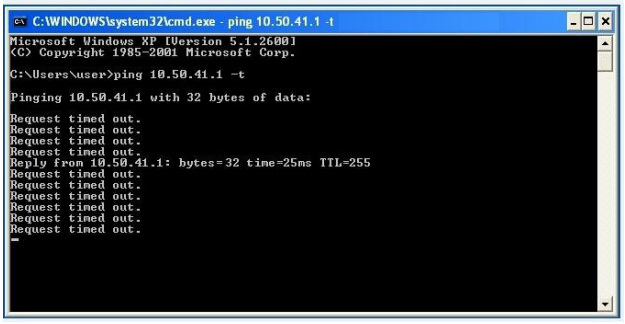
۵-۲- ایجاد اختلال در شبکه با استفاده از حملات DoS

برنامه Low Orbit Ion Cannon نرم افزاری جهت ارسال درخواستهای مکرر به یک وبسایت ، یک روتر و یا یک سوئیچ از طریق پورتهای باز آنها میباشد به عبارت دیگر یک نرم افزار جهت ایجاد ping مرگبار(حملات DoS) است. شکل ۶ نحوه ارسال ۱۰۰۰۰۰ درخواست مکرر از طریق پروتکل UDP به پورت ۸۰ روتر شبکه مورد آزمایش را نشان میدهد.



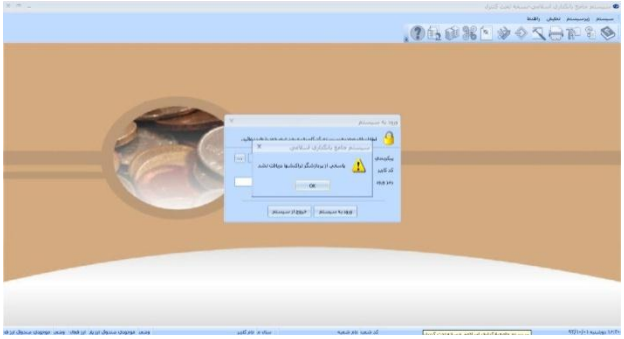
شکل ۶ نرم افزار Low Orbit Ion Cannon

تنها پس از گذشت چند ثانیه شبکه داخلی این موسسه دچار اختلال میشود. شکل ۷ عدم امکان پاسخ روتر مرکزی را نشان میدهد.



شکل ۷ عدم پاسخ روتر به درخواستهای کاربران

به این ترتیب روتر مرکزی پس از مواجهه با درخواستهای مکرر down شده و هیچدام از کاربران قادر به اتصال به آن نیستند و هنگام تلاش جهت برقراری ارتباط با پیغام "پاسخی از پردازشگر تراکنشها دریافت نشد" روبرو میشوند. شکل ۸ عدم برقراری ارتباط با سرور شعبه را نشان میدهد.



شکل ۸ عدم امکان برقرای ارتباط برای کاربران معتبر

۶- نتیجه گیری

در صورتی که یک متجاوز اطلاعاتی، قادر به جمع‌آوری ترافیک SNMP دریک شبکه گردد، از اطلاعات مربوط به ساختار شبکه موجود به همراه سیستم‌ها و دستگاه‌های متصل شده به آن، نیز آگاهی خواهد یافت. اگر ضرورتی به استفاده از پروتکل SNMP نیست مدیران سیستم باید آنرا غیرفعال نمایند. در صورتیکه استفاده از آن به هر دلیلی ضروری باشد می‌بایست امکان دستیابی به صورت فقط خواندنی در نظر گرفته شود و با بکارگیری روش هایی نظیر Access Control List دسترسی به آن را محدود سازند. همچنین برای اطمینان بیشتر، قابلیت Read/Write پروتکل SNMP را غیرفعال سازند ، مگر آنکه واقعا ضروری باشد. دسترسی به دستگاههای تحت SNMP را نیز باید با روش های احراز هویت قوی، مدیریت نمود. به منظور جلوگیری از امکان جعل هویت و دسترسی به بسته‌های ارسالی در شبکه، از نسخه ۳ این پروتکل استفاده نمایند و در این نسخه از الگوریتمهای احراز هویت (SHA1 و MD5) جهت احراز هویت و از الگوریتم AES128 (بدلیل عدم امکان رمزگشایی بسته ها و پایین آوردن CPU Lpoad روتر) برای رمزنگاری بسته های ارسالی در شبکه استفاده نمایند. در صورت امکان، صرفا به تعداد اندکی از رایانه‌ها امتیاز استفاده از سرویس دهنده SNMPاعطاء گردد[۶].

مدیران شبکه می‌بایست به صورت ادواری، اقدام به تست امنیتی تمام رایانه‌های موجود در شبکه (سرویس گیرندگان، سرویس دهندگان، سوئیچ‌ها، مسیریاب‌ها، دیوار آتش‌ها و سیستم‌های تشخیص مزاحمین) نمایند. تست امنیت شبکه پس از اعمال هر گونه تغییر اساسی در پیکربندی شبکه نیز می‌بایست انجام شود[۷] .

طراحی شبکه بگونه ای که بتواند در مقابل حملات DoS مقاومت کند کار بسیار دشواری است و اگر کسی ادعا کند که می تواند بطور کامل این حملات را متوقف کند، ادعای درستی ندارد. اما یکی از ساده ترین راه ها برای متوقف کردن این حمله علیه یک IP خاص، ردگیری درخواستهایی که به قصد حمله ارسال میشوند و مسدود کردن تمام ترافیکی است که از حمله کننده به مقصد ارسال میشود. این کار با استفاده از نوشتن Access Control List توسط مدیر شبکه صورت می‌گیرد[۸]. البته این راه حل یکی از چند راه حل ممکن می‌باشد.

مراجع

[۱] سهراب نیازی. امنیت شبکه.قابل دسترس در :www.niazisoft.blogfa.com

[۲] فرامرز گیوه کی, اصول مهندسی شبکه‌های کامپیوتری: دانشگاه تربیت دبیر شهید رجایی, ۱۳۸۹.

[3] J. Case, M. Fedor, M. Schoffstall, and C. Davin, "A simple network management protocol (SNMP)," ed: Network Information Center, SRI International, 1989.

[4] D. Aspinall, "Internet attacks and defences," 2013.

[5] S. Yu, "An Overview of DDoS Attacks," in *Distributed Denial of Service Attack and Defense*, ed: Springer, 2014, pp. 1-14.

[6] D. Donohue, *CCNP Routing and Switching SWITCH 300-115 Quick Reference*: Cisco Press, 2014.

[7] J. M. Kizza, *Guide to Computer Network Security*: Springer, 2013.

[8] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," *Wireless personal communications*, vol ,۷۳ .pp. 95-126, 2013.