انواع حملات در شبکه های کامپیوتری (بخش اول)

امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری از جمله موضوعاتی است که این روزها در کانون توجه تمامی سازمان ها و موسسات قرار گرفته شده است . در یک شبکه کامپیوتری به منظور ارائه خدمات به کاربران ، سرویس ها و پروتکل های متعددی نصب و پیکربندی می گردد. برخی از سرویس ها دارای استعداد لازم برای انواع حملات بوده و لازم است در مرحله اول و در زمان نصب و پیکربندی آنان ، دقت لازم در خصوص رعایت مسائل ایمنی انجام و در مرحله دوم سعی گردد که از نصب سرویس ها و پروتکل های غیرضروری ، اجتناب گردد . در این مقاله قصد داریم از این زاویه به مقوله امنیت اطلاعات و ایمن سازی شبکه های کامپیوتری پرداخته و در ادامه با انواع حملاتی که امروزه متوجه شبکه های کامپیوتری است ، بیشتر آشنا شویم . قطعا" شناسائی سرویس های غیرضروری و انواع حملاتی که مهاجمان با استفاده از آنان شبکه های کامپیوتری را هدف قرار می دهند ، زمینه برپاسازی و نگهداری شبکه های کامپیوتری ایمن و مطمئن را بهتر فراهم می نماید .

مقدمه

حملات در یک شبکه کامپیوتری حاصل پیوند سه عنصر مهم سرویس ها ی فعال ، پروتکل های استفاده شده و پورت های باز می باشد . یکی از مهمترین وظایف کارشناسان فن آوری اطلاعات ، اطیمنان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیارخطیر و سنگین) . در زمان ارائه سرویس دهندگان ، مجموعه ای از سرویس ها و پروتکل ها به صورت پیش فرض فعال و تعدادی دیگر نیز غیر فعال شده اند.این موضوع ارتباط مستقیمی با سیاست های یک سیستم عامل و نوع نگرش آنان به مقوله امنیت دارد. در زمان نقد امنیتی سیستم های عامل ، پرداختن به موضوع فوق یکی از محورهائی است که کارشناسان امنیت اطلاعات با حساسیتی بالا آنان را دنبال می نمایند.

اولین مرحله در خصوص ایمن سازی یک محیط شبکه ، تدوین ، پیاده سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه ریزی در خصوص ایمن سازی شبکه را شامل می شود . هر نوع برنامه ریزی در این رابطه مستلزم توجه به موارد زیر است :

- بررسی نقش هر سرویس دهنده به همراه پیکربندی انجام شده در جهت انجام وظایف مربوطه در شبکه
- انطباق سرویس ها ، پروتکل ها و برنامه های نصب شده با خواسته ها ی یک سازمان
- بررسی تغییرات لازم در خصوص هر یک از سرویس دهندگان فعلی (افزودن و یا حذف سرویس ها و پروتکل های غیرضروری ، تنظیم دقیق امنیتی سرویس ها و پروتکل های فعال)

تعلل و یا نادیده گرفتن فاز برنامه ریزی می تواند زمینه بروز یک فاجعه عظیم اطلاعاتی را در یک سازمان به دنبال داشته باشد . متاسفانه در اکثر موارد توجه جدی به مقوله برنامه ریزی و تدوین یک سیاست امنیتی نمی گردد . فراموش نکنیم که فن آوری ها به سرعت و به صورت مستمر در حال تغییر بوده و می بایست متناسب با فن آوری های جدید ، تغییرات لازم با هدف افزایش ضریب مقاومت سرویس دهندگان و کاهش نقاط آسیب

پذیر آنان با جدیت دنبال شود . نشستن پشت یک سرویس دهنده و پیکربندی آن بدون وجود یک برنامه مدون و مشخص ، امری بسیار خطرناک بوده که بستر لازم برای بسیاری از حملاتی که در آینده اتفاق خواهند افتاد را فراهم می نماید . هر سیستم عامل دارای مجموعه ای از سرویس ها ، پروتکل ها و ابزارهای خاص خود بوده و نمی توان بدون وجود یک برنامه مشخص و پویا به تمامی ابعاد آنان توجه و از پتانسیل های آنان در جهت افزایش کارائی و ایمن سازی شبکه استفاده نمود. پس از تدوین یک برنامه مشخص در ارتباط با سرویس دهندگان ، می بایست در فواصل زمانی خاصی ، برنامه های تدوین یافته مورد بازنگری قرار گرفته و تغییرات لازم در آنان با توجه به شرایط موجود و فن آوری های جدید ارائه شده ، اعمال گردد . فراموش نکنیم که حتی راه حل های انتخاب شده فعلی که دارای عملکردی موفقیت آمیز می باشند ، ممکن است در آینده و با توجه به شرایط پیش آمده قادر به ارائه عملکردی صحیح ، نباشند .

وظیفه یک سرویس دهنده

پس از شناسائی جایگاه و نقش هر سرویس دهنده در شبکه می توان در ارتباط با سرویس ها و پروتکل های مورد نیاز آن به منظور انجام وظایف مربوطه ، تصمیم گیری نمود . برخی از سرویس دهندگان به همراه وظیفه آنان در یک شبکه کامپیوتری به شرح زیر می باشد :

- Server Logon : این نوع سرویس دهندگان مسئولیت شناسائی و تائید کاربران در زمان ورود به شبکه را برعهده دارند . سرویس دهندگان فوق می توانند عملیات خود را به عنوان بخشی در کنار سایر سرویس دهندگان نیز انجام دهند .
- Server Services Network : این نوع از سرویس دهندگان مسئولیت میزبان نمودن سرویس های مورد نیاز شبکه را برعهده دارند. این سرویس ها عبارتند از :

- DHCP – (Dynamic Host Configuration Protocol)
- DNS – (Domain Name System)
- WINS – (Windows Internet Name Service)
- SNMP – (Simple Network Management Protocol)

- Server Application : این نوع از سرویس دهندگان مسئولیت میزبان نمودن برنامه ها ی کاربردی نظیر بسته نرم افزاری Accounting و سایر نرم افزارهای مورد نیاز در سازمان را برعهده دارند .
- Server File : از این نوع سرویس دهندگان به منظور دستیابی به فایل ها و دایرکتوری های کاربران ، استفاده می گردد .
- Server Print : از این نوع سرویس دهندگان به منظور دستیابی به چاپگرهای اشتراک گذاشته شده در شبکه ، استفاده می شود .
- Server Web : این نوع سرویس دهندگان مسئولیت میزبان نمودن برنامه های وب و وب سایت های داخلی و یا خارجی را برعهده دارند .
- Server FTP : این نوع سرویس دهندگان مسئولیت ذخیره سازی فایل ها برای انجام عملیات Downloading و Uploading را برعهده دارند. سرویس دهندگان فوق می توانند به صورت داخلی و یا خارجی استفاده گردند .
- Server Email : این نوع سرویس دهندگان مسئولیت ارائه سرویس پست الکترونیکی را برعهده داشته و می توان از آنان به منظور میزبان نمودن فولدرهای عمومی و برنامه های Gropuware ، نیز استفاده نمود.

- Server (News/Usenet (NNTP : این نوع سرویس دهندگان به عنوان یک سرویس دهنده newsgroup بوده و کاربران می توانند اقدام به ارسال و دریافت پیام هائی بر روی آنان نمایند .

به منظور شناسائی سرویس ها و پروتکل های مورد نیاز بر روی هر یک از سرویس دهندگان ، می بایست در ابتدا به این سوال پاسخ داده شود که نحوه دستیابی به هر یک از آنان به چه صورت است ؟ : شبکه داخلی ، شبکه جهانی و یا هر دو مورد . پاسخ به سوال فوق زمینه نصب و پیکربندی سرویس ها و پروتکل های ضروری و حذف و غیر فعال نمودن سرویس ها و پروتکل های غیرضروری در ارتباط با هر یک از سرویس دهندگان موجود در یک شبکه کامپیوتری را فراهم می نماید .

سرویس های حیاتی و موردنیاز

هر سیستم عامل به منظور ارائه خدمات و انجام عملیات مربوطه ، نیازمند استفاده از سرویس های متفاوتی است . در حالت ایده آل ، عملیات نصب و پیکربندی یک سرویس دهنده می بایست صرفا" شامل سرویس ها و پروتکل های ضروری و مورد نیاز به منظور انجام وظایف هر سرویس دهنده باشد. معمولا" تولید کنندگان سیستم های عامل در مستندات مربوطه به این سرویس ها اشاره می نمایند. استفاده از مستندات و پیروی از

روش های استاندارد ارائه شده برای پیکربندی و آماده سازی سرویس دهندگان ،زمینه نصب و پیکربندی مطمئن با رعایت مسائل ایمنی را بهتر فراهم می نماید . زمانی که کامپیوتری در اختیار شما گذاشته می شود ، معمولا" بر روی آن نرم افزارهای متعددی نصب و پیکربندی های خاصی نیز در ارتباط با آن اعمال شده است . یکی از مطمئن ترین روش ها به منظور آگاهی از این موضوع که سیستم فوق انتظارات شما را متناسب با برنامه تدوین شده ، تامین می نماید ، انجام یک نصب Clean با استفاده از سیاست ها و لیست ها ی از قبل مشخص شده است . بدین ترتیب در صورت بروز اشکال می توان به سرعت از این امر آگاهی و هر مشکل را در محدوده خاص خود بررسی و برای آن راه حلی انتخاب نمود. (شعاع عملیات نصب و پیکربندی را به تدریج افزایش دهیم) .

مشخص نمودن پروتکل های مورد نیاز

برخی از مدیران شبکه عادت دارند که پروتکل های غیرضروری را نیز بر روی سیستم نصب نمایند ، یکی از علل این موضوع ، عدم آشنائی دقیق آنان با نقش و عملکرد هریک از پروتکل ها در شبکه بوده و در برخی موارد نیز بر این اعتقاد هستند که شاید این پروتکل ها در آینده مورد نیاز خواهد بود. پروتکل ها همانند سرویس ها ، تا زمانی که به

وجود آنان نیاز نمی باشد ، نمی بایست نصب گردند . با بررسی یک محیط شبکه با سوالات متعددی در خصوص پروتکل های مورد نیاز برخورد نموده که پاسخ به آنان امکان شناسائی و نصب پروتکل های مورد نیاز را فراهم نماید .

- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) با سرویس دهندگان ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس دهنده با سرویس دهنده ، نیاز می باشد ؟
- به چه نوع پروتکل و یا پروتکل هائی برای ارتباط سرویس گیرندگان (Desktop) از راه دور با سرویس دهندگان ، نیاز می باشد ؟
- آیا پروتکل و یا پروتکل های انتخاب شده ما را ملزم به نصب سرویس های اضافه ای می نمایند ؟
- آیا پروتکل های انتخاب شده دارای مسائل امنیتی خاصی بوده که می بایست مورد توجه و بررسی قرار گیرد ؟

در تعداد زیادی از شبکه های کامپیوتری ،از چندین سیستم عامل نظیر ویندوز ، یونیکس و یا لینوکس ، استفاده می گردد . در چنین مواردی می توان از پروتکل TCP/IP به

عنوان فصل مشترک بین آنان استفاده نمود. در ادامه می بایست در خصوص فرآیند اختصاص آدرس های IP تصیم گیری نمود (به صورت ایستا و یا پویا و به کمک DHCP) . در صورتی که تصمیم گرفته شود که فرآیند اختصاص آدرس های IP به صورت پویا و به کمک DHCP ، انجام شود، به یک سرویس اضافه و با نام DHCP نیاز خواهیم داشت . با این که استفاده از DHCP مدیریت شبکه را آسانتر می نماید ولی از لحاظ امنیتی دارای درجه پائین تری نسبت به اختصاص ایستای آدرس های IP ، می باشد چراکه کاربران ناشناس و گمنام می توانند پس از اتصال به شبکه ، بلافاصله از منبع صادرکننده آدرس های IP ، یک آدرس IP را دریافت و به عنوان یک سرویس گیرنده در شبکه ایفای وظیفه نمایند. این وضعیت در ارتباط با شبکه های بدون کابل غیرایمن نیز صدق می نماید. مثلا" یک فرد می تواند با استقرار در پارکینگ یک ساختمان و به کمک یک Laptop به شبکه شما با استفاده از یک اتصال بدون کابل ، متصل گردد. پروتکل TCP/IP ، برای "معادل سازی نام به آدرس " از یک سرویس دهنده DNS نیز استفاده می نماید . در شبکه های ترکیبی شامل چندین سیستم عامل نظیر ویندوز و یونیکس و با توجه به این که ویندوز NT 4.0 و یا ۲۰۰۰ شده است ، علاوه بر DNS به سرویس WINS نیز نیاز می باشد . همزمان با انتخاب پروتکل ها و سرویس های مورد نیاز آنان ، می بایست بررسی لازم در خصوص چالش های امنیتی هر یک از آنان نیز

بررسی و اطلاعات مربوطه مستند گردند(مستندسازی ، ارج نهادن به زمان خود و دیگران است) . راه حل انتخابی ، می بایست کاهش تهدیدات مرتبط با هر یک از سرویس ها و پروتکل ها را در یک شبکه به دنبال داشته باشد .

مزایای غیرفعال نمودن پروتکل ها و سرویس های غیرضروری

استفاده عملیاتی از یک سرویس دهنده بدون بررسی دقیق سرویس ها ، پروتکل ها و پیکربندی متناظر با هر یک از آنان زمینه بروز تهدیدات و حملات را در یک شبکه به دنبال خواهد داشت . فراموش نکنیم که مهاجمان همواره قربانیان خود را از بین سرویس دهندگانی که به درستی پیکربندی نشده اند ، انتخاب می نمایند. بنابراین می بایست به سرعت در خصوص سرویس هائی که قصد غیرفعال نمودن آنان را داریم ، تصمیم گیری شود . قطعا" نصب سرویس ها و یا پروتکل هائی که قصد استفاده از آنان وجود ندارد ، امری منطقی و قابل قبول نخواهد بود. در صورتی که این نوع از سرویس ها نصب و به درستی پیکربندی نگردند ، مهاجمان می توانند با استفاده از آنان ، آسیب های جدی را متوجه شبکه نمایند . تهدید فوق می تواند از درون شبکه و یا خارج از شبکه متوجه یک شبکه کامپیوتری گردد . بر اساس برخی آمارهای منتشر شده ، اغلب آسیب ها و

تهدیدات در شبکه یک سازمان توسط کارکنان کنجکا و و یا ناراضی صورت می پذیرد تا از طریق مهاجمان خارج از شبکه .

بخاطر داشته باشید که ایمن سازی شبکه های کامپیوتری مستلزم اختصاص زمان لازم و کافی برای برنامه ریزی است . سازمان ها و موسسات علاقه مندند به موازات عرضه فن آوری های جدید ، به سرعت از آنان استفاده نموده تا بتوانند از مزایای آنان در جهت اهداف سازمانی خود استفاده نمایند. تعداد و تنوع گزینه های انتخابی در خصوص پیکربندی هر سیستم عامل ، به سرعت رشد می نماید . امروزه وجود توانائی لازم در جهت شناسائی و پیاده سازی سرویس ها و پروتکل های مورد نیاز در یک شبکه خود به یک مهارت ارزشمند تبدیل شده است. بنابراین لازم است کارشناسان فن آوری اطلاعات که مسئولیت شغلی آنان در ارتباط با شبکه و ایمن سازی اطلاعات است ، به صورت مستمر و با اعتقاد به اصل بسیار مهم " اشتراک دانش و تجارب " ، خود را بهنگام نمایند. اعتقاد عملی به اصل فوق ، زمینه کاهش حملات و تهدیدات را در هر شبکه کامپیوتری به دنبال خواهد داشت .

حملات (Attacks)

با توجه به ماهیت ناشناس بودن کاربران شبکه های کامپیوتری ، خصوصا" اینترنت ،امروزه شاهد افزایش حملات بر روی تمامی انواع سرویس دهندگان می باشیم . علت بروز چنین حملاتی می تواند از یک کنجکاوی ساده شروع و تا اهداف مخرب و ویرانگر ادامه یابد.

برای پیشگیری ، شناسائی ، برخورد سریع و توقف حملات ، می بایست در مرحله اول قادر به تشخیص و شناسائی زمان و موقعیت بروز یک تهاجم باشیم . به عبارت دیگر چگونه از بروز یک حمله و یا تهاجم در شبکه خود آگاه می شویم ؟ چگونه با آن برخورد نموده و در سریعترین زمان ممکن آن را متوقف نموده تا میزان صدمات و آسیب به منابع اطلاعاتی سازمان به حداقل مقدار خود برسد ؟ شناسائی نوع حملات و نحوه پیاده سازی یک سیستم حفاظتی مطمئن در مقابل آنان یکی از وظایف مهم کارشناسان امنیت اطلاعات و شبکه های کامپیوتری است .شناخت دشمن و آگاهی از روش های تهاجم وی ، احتمال موفقیت ما را در رویاروئی با آنان افزایش خواهد داد. بنابراین لازم است با انواع حملات و تهاجماتی که تاکنون متوجه شبکه های کامپیوتری شده است ، بیشتر آشنا شده و از این رهگذر تجاربی ارزشمند را کسب تا در آینده بتوانیم به نحو مطلوب از آنان استفاده نمائیم . جدول زیر برخی از حملات متداول را نشان می دهد :

انواع حملات

Denial of Service (DoS) & Distributed Denial of Service (DDoS)

Spoofing	Back Door
Replay	Man in the Middle
Weak Keys	TCP/IP Hijacking
Password Guessing	Mathematical
Dictionary	Brute Force
Software Exploitation	Birthday
Viruses	Malicious Code
Trojan Horses	Virus Hoaxes
Worms	Logic Bombs
Auditing	Social Engineering
	System Scanning

در بخش دوم این مقاله به بررسی هر یک از حملات فوق ، خواهیم پرداخت .

انواع حملات در شبکه های کامپیوتری (بخش دوم) مدیریت شبکه 3834 7 4

انواع حملات در شبکه های کامپیوتری (بخش دوم)

در بخش اول این مقاله به ضرورت شناسائی سرویس ها و پروتکل ها ی غیرضروری ، نصب و پیکربندی سرویس ها و پروتکل های مورد نیاز با لحاظ نمودن مسائل امنیتی در یک شبکه ، اشاره گردید . همانگونه که در بخش اول این مقاله اشاره شد ، حملات در یک شبکه کامپیوتری ، حاصل پیوند سه عنصر مهم سرویس ها ی فعال ، پروتکل های استفاده شده و پورت های باز می باشد. کارشناسان امنیت اطلاعات می بایست با تمرکز بر سه محور فوق ، شبکه ای ایمن و مقاوم در مقابل انواع حملات را ایجاد و نگهداری نمایند.

انواع حملات

Denial of Service (DoS) & Distributed Denial of Service (DDoS)

Spoofing	Back Door
Replay	Man in the Middle
Weak Keys	TCP/IP Hijacking
Password Guessing	Mathematical
Dictionary	Brute Force
Software Exploitation	Birthday
Viruses	Malicious Code
Trojan Horses	Virus Hoaxes
Worms	Logic Bombs
Auditing	Social Engineering
	System Scanning

حملات از نوع DoS

هدف از حملات DoS ، ایجاد اختلال در منابع و یا سرویس هائی است که کاربران قصد دستیابی و استفاده از آنان را دارند (از کار انداختن سرویس ها) . مهمترین هدف این نوع از حملات ، سلب دستیابی کاربران به یک منبع خاص است . در این نوع حملات، مهاجمان با بکارگیری روش های متعددی تلاش می نمایند که کاربران مجاز را به منظور دستیابی و استفاده از یک سرویس خاص ، دچار مشکل نموده و بنوعی در مجموعه

سرویس هائی که یک شبکه ارائه می نماید ، اختلال ایجاد نمایند . تلاش در جهت ایجاد ترافیک کاذب در شبکه ، اختلال در ارتباط بین دو ماشین ، ممانعت کاربران مجاز به منظور دستیابی به یک سرویس ، ایجاد اختلال در سرویس ها ، نمونه هائی از سایر اهدافی است که مهاجمان دنبال می نمایند . در برخی موارد و به منظور انجام حملات گسترده از حملات DoS به عنوان نقطه شروع و یک عنصر جانبی استفاده شده تا بستر لازم برای تهاجم اصلی ، فراهم گردد . استفاده صحیح و قانونی از برخی منابع نیز ممکن است ، تهاجمی از نوع DoS را به دنبال داشته باشد . مثلا" یک مهاجم می تواند از یک سایت FTP که مجوز دستیابی به آن به صورت anonymous می باشد ، به منظور ذخیره نسخه هائی از نرم افزارهای غیرقانونی ، استفاده از فضای ذخیره سازی دیسک و یا ایجاد ترافیک کاذب در شبکه استفاده نماید . این نوع از حملات می تواند غیرفعال شدن کامپیوتر و یا شبکه مورد نظر را به دنبال داشته باشد . حملات فوق با محوریت و تاکید بر نقش و عملیات مربوط به هر یک از پروتکل های شبکه و بدون نیاز به اخذ تائیدیه و یا مجوزهای لازم ، صورت می پذیرد . برای انجام این نوع حملات از ابزارهای متعددی استفاده می شود که با کمی حوصله و جستجو در اینترنت می توان به آنان دستیابی پیدا کرد . مدیران شبکه های کامپیوتری می توانند از این نوع ابزارها ، به منظور تست ارتباط

ایجاد شده و اشکال زدائی شبکه استفاده نمایند. حملات DoS تاکنون با اشکال متفاوتی ، محقق شده اند . در ادامه با برخی از آنان آشنا می شویم .

- Smurf/smurfing : این نوع حملات مبتنی بر تابع Reply پروتکل ICMP Internet (Control Message Protocol) ،بوده و بیشتر با نام ping شناخته شده می باشند .(Ping ، ابزاری است که پس از فعال شدن از طریق خط دستور ، تابع Reply پروتکل ICMP را فرامی خواند) . در این نوع حملات ، مهاجم اقدام به ارسال بسته های اطلاعاتی Ping به آدرس های Broadcast شبکه نموده که در آنان آدرس مبداء هر یک از بسته های اطلاعاتی Ping شده با آدرس کامپیوتر قربانی ، جایگزین می گردد .بدین ترتیب یک ترافیک کاذب در شبکه ایجاد و امکان استفاده از منابع شبکه با اختلال مواجه می گردد.
- Fraggle : این نوع از حملات شباهت زیادی با حملات از نوع Smurf داشته و تنها تفاوت موجود به استفاده از UDP (User Datagram Protocol) در مقابل ICMP ، برمی گردد . در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی UDP به آدرس های Broadcast (مشابه تهاجم Smurf)

می نمایند . این نوع از بسته های اطلاعاتی UDP به مقصد پورت ۷ (echo) و یا پورت ۱۹ (Chargen) ، هدایت می گردند.

- Ping flood : در این نوع تهاجم ، با ارسال مستقیم درخواست های Ping به کامپیوتر قربانی ، سعی می گردد که سرویس ها بلاک و یا فعالیت آنان کاهش یابد. در یک نوع خاص از تهاجم فوق که به ping of death ، معروف است ، اندازه بسته های اطلاعاتی به حدی زیاد می شود که سیستم (کامپیوتر قربانی) ، قادر به برخورد مناسب با اینچنین بسته های اطلاعاتی نخواهد بود .
- SYN flood : در این نوع تهاجم از مزایای three-way handshake مربوط به TCP استفاده می گردد . سیستم مبداء اقدام به ارسال مجموعه ای گسترده از درخواست های SYN (synchronization) نموده بدون این که ACK (acknowledgment) نهائی آنان را ارسال نماید. بدین ترتیب half-open TCP sessions (ارتباطات نیمه فعال) ، ایجاد می گردد . با توجه به این که پشته TCP ، قبل از reset نمودن پورت ، در انتظار باقی خواهد ماند ، تهاجم فوق ، سرریز بافر اتصال کامپیوتر مقصد را به دنبال داشته و عملا" امکان ایجاد ارتباط وی با سرویس گیرندگان معتبر ، غیر ممکن می گردد .

- Land : تهاجم فوق، تاکنون در نسخه های متفاوتی از سیستم های عامل ویندوز ، یونیکس ، مکینتاش و IOS سیسکو،مشاهده شده است . در این نوع حملات ، مهاجمان اقدام به ارسال یک بسته اطلاعاتی (TCP/IP synchronization SYN) که دارای آدرس های مبداء و مقصد یکسان به همراه پورت های مبداء و مقصد مشابه می باشد ، برای سیستم های هدف می نمایند . بدین ترتیب سیستم قربانی، قادر به پاسخگوئی مناسب بسته اطلاعاتی نخواهد بود.
- Teardrop : در این نوع حملات از یکی از خصلت های UDP در پشته TCP/IP برخی سیستم های عامل (TCPپیاده سازی شده در یک سیستم عامل) ، استفاده می گردد. در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی fragmented برای سیستم هدف با مقادیر افست فرد در دنباله ای از بسته های اطلاعاتی می نمایند . زمانی که سیستم عامل سعی در بازسازی بسته های اطلاعاتی اولیه fragmented می نماید، قطعات ارسال شده بر روی یکدیگر بازنویسی شده و اختلال سیستم را به دنبال خواهد داشت . با توجه به عدم برخورد مناسب با مشکل فوق در برخی از سیستم های عامل ، سیستم هدف Crash ، و یا راه اندازی مجدد می گردد .

- Bonk : این نوع از حملات بیشتر متوجه ماشین هائی است که از سیستم عامل ویندوز استفاده می نمایند . در حملات فوق ، مهاجمان اقدام به ارسال بسته های اطلاعاتی UDP مخدوش به مقصد پورت ۵۳ DNS ، می نمایند بدین ترتیب در عملکرد سیستم اختلال ایجاد شده و سیستم Crash می نماید .
- Boink : این نوع از حملات مشابه تهاجمات Bonk می باشند. با این تفاوت که در مقابل استفاده از پورت ۵۳ ، چندین پورت ، هدف قرارمی گیرد .

Service	Port
Echo	7
Systat	11
Netstat	15
Chargen	19
FTP-Data	20
FTP	21
SSH	22
Telnet	23
SMTP	25
TACACS	49
DNS	53

HTTP	80
POP3	110
Portmap	111
SNMP	161/162
HTTPS	443
RADIUS	1812

متداولترین پورت های استفاده شده در حملات DoS

یکی دیگر از حملات DoS ، نوع خاص و در عین حال ساده ای از یک حمله DoS می باشد که با نام DDoS (Distributed DoS) ، شناخته می شود .در این رابطه می توان از نرم افزارهای متعددی به منظور انجام این نوع حملات و از درون یک شبکه ، استفاده بعمل آورد. کاربران ناراضی و یا افرادی که دارای سوء نیت می باشند، می توانند بدون هیچگونه تاثیری از دنیای خارج از شبکه سازمان خود ، اقدام به ازکارانداختن سرویس ها در شبکه نمایند. در چنین حملاتی ، مهاجمان نرم افزاری خاص و موسوم به Zombie را توزیع می نمایند . این نوع نرم افزارها به مهاجمان اجازه خواهد داد که تمام و یا بخشی از سیستم کامپیوتری آلوده را تحت کنترل خود درآورند. مهاجمان پس از آسیب اولیه به سیستم هدف با استفاده از نرم افزار نصب شده Zombie ، تهاجم نهائی خود را با بکارگیری مجموعه ای وسیع از میزبانان انجام خواهند داد. ماهیت و نحوه

انجام این نوع از حملات ، مشابه یک تهاجم استاندارد DoS بوده ولی قدرت تخریب و آسیبی که مهاجمان متوجه سیستم های آلوده می نمایند ، متاثر از مجموع ماشین هائی (Zombie) است که تحت کنترل مهاجمان قرار گرفته شده است .

به منظور حفاظت شبکه ، می توان فیلترهائی را بر روی روترهای خارجی شبکه به منظور دورانداختن بسته های اطلاعاتی مشمول حملات DoS ، پیکربندی نمود .در چنین مواردی می بایست از فیلتری دیگر که امکان مشاهده ترافیک (مبداء از طریق اینترنت) و یک آدرس داخلی شبکه را فراهم می نماید ، نیز استفاده گردد .

حملات از نوع Back door

Back door ، برنامه ای است که امکان دستیابی به یک سیستم را بدون بررسی و کنترل امنیتی ، فراهم می نماید . برنامه نویسان معمولا" چنین پتانسیل هائی را در برنامه ها پیش بینی تا امکان اشکال زدائی و ویرایش کدهای نوشته شده در زمان تست بکارگیری نرم افزار ، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق ، مستند نمی گردند ، پس از اتمام مرحله تست به همان وضعیت باقی مانده و تهدیدات امنیتی متعددی را به دنبال خواهند داشت .

برخی از متداولترین نرم افزارها ئی که از آنان به عنوان back door استفاده می گردد ، عبارتند از :

- Back Orifice : برنامه فوق یک ابزار مدیریت از راه دور می باشد که به مدیران سیستم امکان کنترل یک کامپیوتر را از راه دور (مثلا" از طریق اینترنت) ، خواهد داد. نرم افزار فوق ، ابزاری خطرناک است که توسط گروهی با نام Cult of the Dead Cow Communications ، ایجاد شده است . این نرم افزار دارای دو بخش مجزا می باشد : یک بخش سرویس گیرنده و یک بخش سرویس دهنده . بخش سرویس گیرنده بر روی یک ماشین اجراء و زمینه مانیتور نمودن و کنترل یک ماشین دیگر که بر روی آن بخش سرویس دهنده اجراء شده است را فراهم می نماید .
- NetBus : این برنامه نیز نظیر Back Orifice ، امکان دستیابی و کنترل از راه دور یک ماشین از طریق اینترنت را فراهم می نماید.. برنامه فوق تحت سیستم عامل ویندوز (نسخه های متفاوت از NT تا ۹۵ و ۹۸) ، اجراء و از دو بخش جداگانه تشکیل شده است : بخش سرویس دهنده (بخشی که بر روی کامپیوتر قربانی مستقر خواهد شد) و بخش سرویس گیرنده (برنامه ای که مسولیت یافتن و کنترل سرویس دهنده را برعهده دارد) . برنامه فوق ، به حریم خصوصی

کاربران در زمان اتصال به اینترنت ، تجاوز و تهدیدات امنیتی متعددی را بـه دنبـال خواهد داشت .

- SubSeven (Sub7) ، این برنامه برنامه نیز تحت ویندوز اجراء شـده و دارای عملکردی مشـابه Orifice Back و NetBus مـی باشـد . پـس از فعـال شـدن برنامه فوق بر روی سیستم هدف و اتصال به اینترنت ،هر شخصـی کـه دارای نـرم افزار سرویس گیرنده باشد ، قادر به دستیابی نامحدود به سیستم خواهد بود .

نرم افزارهای Back Orifice، Sub7 ،NetBus دارای دو بخـش ضـروری سـرویس دهنده و سرویس گیرنده، می باشند. سرویس دهنده بر روی ماشین آلوده مستقر شده و از بخش سرویس گیرنده به منظور کنترل از راه دور سرویس دهنده ، استفاده می گردد.به نرم افزارهای فوق ، " سرویس دهندگان غیرقانونی " گفته می شود .

برخی از نرم افزارها از اعتبار بالائی برخوردار بوده ولی ممکن است توسـط کـاربرانی کـه اهداف مخربی دارند ، مورد استفاده قرار گیرند :

- VNC Virtual Network (Computing) : نرم افزار فوق توسـط آزمایشـگاه T&AT و با هدف کنترل از راه دور یک سیستم ، ارائه شده است . بـا اسـتفاده از برنامه فوق ، امکان مشاهده محیط Desktop از هر مکانی نظیر اینترنـت ، فـراهم

می گردد . یکی از ویژگی های جالب این نرم افزار ، حمایت گسترده از معماری های متفاوت است .

- PCAnywhere : نرم افزار فوق توسط شرکت Symantec ، با هدف کنترل از راه دور یک سیستم با لحاظ نمودن فن آوری رمزنگاری و تائید اعتبار ، ارائه شده است . با توجه به سهولت استفاده از نرم افزار فوق ، شرکت ها و موسسات فراوانی در حال حاضر از آن و به منظور دستیابی به یک سیستم از راه دور استفاده می نمایند .
- Services Terminal : نرم افزار فوق توسط شرکت مایکروسافت و به همراه سیستم عامل ویندوز و به منظور کنترل از راه دور یک سیستم ، ارائه شده است .

همانند سایر نرم افزارهای کاربردی ، نرم افزارهای فوق را می توان هم در جهت اهداف مثبت و هم در جهت اهداف مخرب بکارگرفت.

بهترین روش به منظور پیشگیری از حملات Back doors ، آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود می باشد. به کاربران می بایست آموزش داده شود که صرفا" از منابع و سایت های مطمئن اقدام به دریافت و نصب نرم افزار بر روی سیستم خود نمایند . نصب و استفاده از برنامه های آنتی ویروس می تواند

Backکمک قابل توجهی در بلاک نمودن عملکرد اینچنین نرم افزارهائی (نظیر : Orifice, NetBus, and Sub7) را به دنبال داشته باشد . برنامه های آنتی ویروس می بایست به صورت مستمر بهنگام شده تا امکان شناسائی نرم افزارهای جدید ، فراهم گردد .