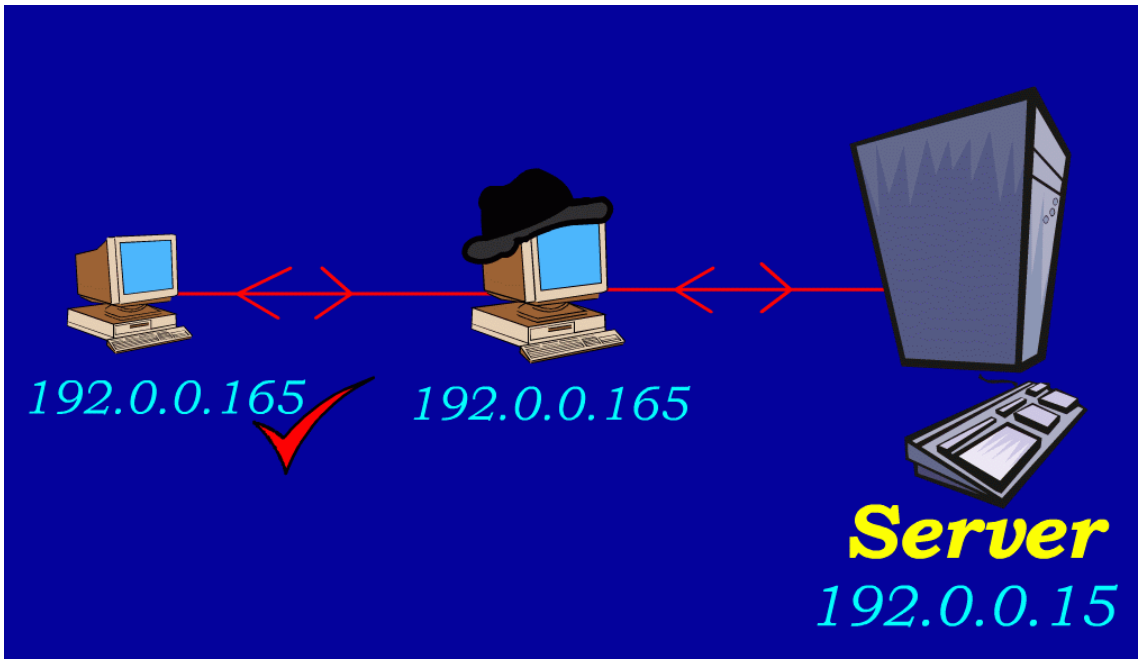
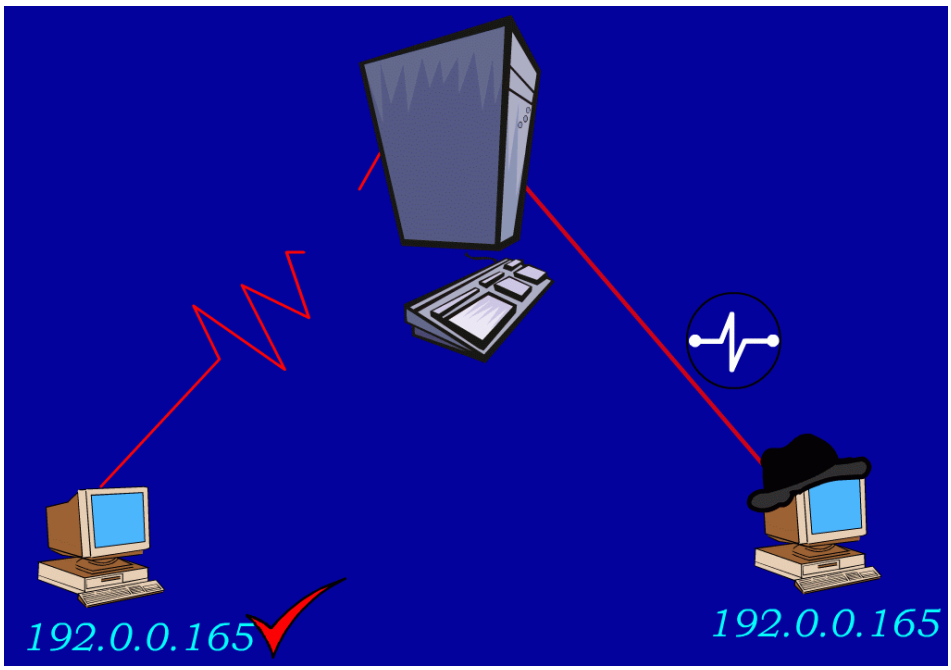
راه‌هاي نفوذ

- ***حمله از طريق IP***: در اين روش ابتدا هكر به روشهاي مختلف IP سرويس دهنده (ايگاه وب، ISP و ..) را بدست مي‌آورد. اين كار با پيدا كردن نقشه شبكه راحت‌تر است سپس هكر خود را در بين سرويس‌دهنده و كاربر قرار مي‌دهد و با ارسال بسته‌هاي تقلبي اطلاعات را به سرقت مي‌برد. در اين روش در واقع هكر خود را براي سرويس دهنده، گيرنده و براي كاربر سرويس دهنده معرفي مي‌كند و به عنوان واسط بين كاربر و Server قادر است بسته‌هاي خود را با شماره‌هاي صحيح انتقال دهد.



- ***حمله به TCP*:** اين حمله از متداولترين نوع حمله به سرويس دهنده‌ها در اينترنت مي‌باشد. هكر در اين روش ارتباط كاربر را از سرويس دهنده قطع مي‌كند و IP خود را به جاي كاربر به سرويس دهنده معرفي مي‌كند و از اين پس هر گونه تبادل اطلاعات بين سرويس دهنده و هكر صورت مي‌گيرد. مزيت اين روش به روش حمله به IP اين است كه در اين روش هكر تنها يك بار حمله مي‌كند و از مقابله با سيستمهاي امنيتي رمز عبور در مراحل بعد فرار مي‌كند. "برخلاف حمله به IP"



- ***حملات جاسوسي***: در نمونه‌اي از اين روش هكر در ارتباط TCP ناهماهنگي ايجاد مي‌كند. شماره سريال بسته‌هايي كه براي سرويس دهنده ارسال مي‌شوند. در بين راه توسط هكر با سريال بسته‌هاي بعدي تعويض مي‌شود و در اين حالت كه شماره سريال با سريال بسته كاربر متفاوت است، سرويس دهنده آن بسته را به كاربر مرجوع كرده و هكر كه منتظر چنين عملي است بسته را براي خود نسخه‌برداري مي‌كند.

پس از اين كار هكر براي بار ديگر بسته مورد نظر خود را مي‌فرستد. ولي اين بار با شماره سريال صحيح و چون شماره سريال تصحيح شده سرويس دهنده آنها را قبول مي‌كند و بدين صورت بدون اينكه كاربر و سرويس دهنده بفهمند اطلاعات توسط هكر كم و زياد مي‌گردد.

استفاده از برنامه Telnet ويندوز يكي از راه‌هاي حملات جاسوسي مي‌باشد. با اجراي اين برنامه از منوي Run ويندوز و پس از گفتن نام ميزبان راه دور يا IP آن و برقراري اتصال با ميزبان سيستم به عنوان بخشي از سرويس شروع به نمايش اطلاعات مي‌كند!

- **جعل اطلاعات :**

- جعل IP
- جعل Email
- جعل يك وب

جعل IP : در سرويسهاي UDP و TCP به آدرس ميزبان اطمينان داريد، هكر مي‌تواند با مسيريابي خود را به عنوان ميزبان و يا كاربر معتبر معرفي كند. هكر آدرس سرويس دهنده را مطابق با آدرس كاربر جعل و سپس براي كاربر يك آدرس جديد مي‌سازد و به اين صورت هكر ارتباط كاربر را با سرويس دهنده قطع و ارتباط خود را با همان آدرس جعل

شده کاربر با سرويس دهنده برقرار مي‌كند. در بسياري از موارد نيز ممكن است هكر منتظر بماند تا كاربر كامپيوتر خود را خاموش كند سپس يك ارتباط با ميزبان برقرار مي‌كند و خود را به عنوان كاربر معرفي مي‌كند.

جعل Email : جعل Email در اينترنت بسيار آسان مي‌باشد و غالباً نمي‌توان به Email هاي فاقد سيستمهاي امنيتي اطمينان 100 % پيدا كرد. با استفاده از TelNet مي‌توان به پورت SMTP متصل شد. همچنين فرستادن Email جعلي از طرف يك كاربر با IP مشخص توسط هكر به راحتي امكان پذير است. كافيست هكر اطلاعاتي در زمينه برنامه‌نويسي و فرستادن Email داشته باشد و با پروتكل‌هاي SMTP آشنايي داشته باشد.

جعل وب : يكي ديگر از شيوه‌هاي حمله هكرها جعل يك صفحه وب مي‌باشد. در اين روش يك نسخه از وب سايت نسخه‌برداري مي‌گردد و هكر نسخه ذخيره شده را تغيير مي‌دهد ولي تمامي ظواهر وب بدون تغيير باقي مي‌ماند. هكر صفحه جعل شده را Upload مي‌كند و به طريقي توجه كاربر را براي ورود به آن صفحه جلب مي‌كند. كاربر با كليك روي لينك فرستاده شده هكر به صفحه جعل شده هدايت مي‌شود و چون شكل ظاهري صفحه درست مي‌باشد احتمال استفاده كاربر از آن صفحه وجود دارد. كه در اين صورت هكر به هدف خود مي‌رسد. اين شيوه بيشتر در امور تجاري نقش دارد. مثلاً در بسياري از خريدهاي اينترنتي از خريدار خواسته مي‌شود تا كد كارت اعتباري خود را وارد كند. حال اگر اين سايت جعلي باشد كد كارت اعتباري شما به هكر فرستاده مي‌شود.

هك كردن از طريق جعل وب از روشهاي هك از طريق مهندسي اجتماعي محسوب مي‌شود.

- ***Appletها*** : علاوه بر خدماتي كه Applet هاي جاوا در طراحي صفحاتن وب انجام مي‌دهند. اين كدها مي‌توانند خطرناك باشند. زيرا Applet ها مستقيماً توسط مرورگر به حافظه بارگذاري مي‌گردند يعني با ورود به يك صفحه وب مرورگر به طور اتوماتيك كدهاي جاوا را اجرا مي‌كند. هكر مي‌تواند كدهاي مخربي بنويسد و برنامه جاسوس خود را بر روي كامپيوتر كاربر نصب كند و يا اطلاعات مورد نياز را بدست بياورد ... . اين نوع حمله از متداولترين و مخرب‌ترين نوع حملات هكرها محسوب مي‌شود.
- ***Cookieها*** : كوكي‌ها فايلهاي كوچكي هستند كه صفحات پوياي وب مي‌تواند روي كامپيوتر كاربر ايجاد كند. حداكثر طول اين فايلها 4 كيلوبايت مي‌باشد. بسياري از صفحات وب اطلاعات پر شده فرمهاي سايت توسط كاربر و يا اطلاعات مورد نياز خود را براي ورودهاي بعدي به صفحه توسط كاربر در فايلهايي به نام Cookie در كامپيوتر كاربر ذخيره مي‌كنند. اين كار با اجازه خود كاربر و يا در مواردي بدون نظرخواهي كاربر روي كامپيوتر او ذخيره مي‌گردد. هكر مي‌تواند از اطلاعات داخل اين كوكيها نهايت استفاده را ببرد و با دزديدن اين اطلاعات زمينه نفوذ را فراهم كند.
- ***حمله به كلمات عبور*** : در اين روش هكر با پيدا كردن كلمات عبور شامل رمز عبور اطلاعات محرمانه، تجاري، امنيتي و حتي كلمه عبور Email افراد كنترل تمامي قسمتهاي مورد نياز را به دست مي‌گيرد.

شكستن كلمات عبور به دو صورت انجام مي‌شود:

1- توليد كليه رمزهاي محتمل و امتحان كردن آنها در اين روش از نرمافزارهايي استفاده مي‌شود كه قادرند در هر ثانيه چندين كلمه عبور را جستجو كنند و با پيدا كردن تمامي تركيبات حروف و تست كردن اتوماتيك آنها رمز عبور شكسته مي‌شود.

بهترين حالت براي هكر اين است كه رمز عبور از كلمات با معني باشد كه در اين صورت نرمافزار هكر به جاي توليد تمامي تركيبات حروف از DataBase ديكشنري‌ها يا DB اسامي و ... براي پيدا كردن رمز عبور استفاده مي‌كند. اتفاقاً افراد در بسياري از موارد كلمات عبور خود را ساده و طوري انتخاب مي‌كنند تا فراموش نشود.

2- در روش ديگري از پيدا كردن رمز عبور هكر از ديكد كردن رمز كد شده استفاده مي‌كند. در هر سيستم معمولاً كلمات عبور به صورت رمز شده در فايلي روي كامپيوتر كاربر يا شبكه ذخيره مي‌شوند هكر با دزديدن اين فايل و يافتن الگوريتم رمز گشايي آن كلمه عبور را پيدا مي‌كند. در اين موارد اگر رمز گذاري فايل از روشهاي معمول و شناخته شده نباشد ديكد كردن رمز براي هكر بسيار مشكل است. مثلاً تمامي پسوردها و كليه Account number ها در ويندوز NT درون فايلي با نام SAM در ويندوز نگهداري مي‌شود كه علاوه بر اينكه از رمز گذاري قوي و پيچيده نظير (MD4) استفاده شده ولي باز هم شكست پذير است.

در روش Hash كه براي رمزهاي ويندوز NT صورت مي‌گيرد كلمه عبور به صورت 14 كاراكتر تنظيم مي‌شود و سپس روي آن روش MD4 سه بار اعمال مي‌شود تا كلمه عبور به رمز در آيد. اين روش با تمام قدرتي كه دارد باز هم با تركيبي از روش (1) و استفاده از MD4 قابل شكستن است.

در مورد فايل SAM ويندوز NT ... هكر نمي‌تواند به راحتي آن را در حال اجراي سيستم عامل بدست آورد زيرا اين فايل كاملاً توسط هسته ويندوز محافظت مي‌شود و حتي خود كاربر نمي‌تواند مستقيماً اين فايل را دستكاري كند و يا آن را پاك كند يا از آن نسخه‌برداي كند!

- ***حمله به برنامه‌هاي كاربردي***: در اين روش هكر مستقيماً به برنامه‌هاي كاربردي تحت وب حمله مي‌كند. هكر در اين روش معمولاً User ID و Password عبور را بدست مي‌آورد.

به اين ترتيب كه وقتي يك برنامه كاربردي مانند Internet explorer درخواست يك كلمه عبور مي‌شود. اگر كاربر نام عبور را اشتباه وارد كند. در خط آدرس دستور نوع نادرستي نام عبور گزارش داده مي‌شود و در واقع در اين روش يك بيت صحت و يا نادرستي كلمه عبور مشخص مي‌شود. هكر به اين وسيله مرحله به مرحله نام عبور را پيدا مي‌كند و سپس با يك جستجوگر رمز عبور آن نام را پيدا مي‌كند.

كلاً هكرها در بسياري از موارد از ضعف‌هاي برنامه‌هاي تحت وب آگاهي پيدا مي‌كنند و از اين ضعفها براي نفوذ استفاده مي‌كنند. اين ضعف‌ها گاهي در نسخه‌هاي بعدي اين نرمافزارهاي كاربردي رفع مي‌شوند و گاهي امكان رفع آن براي شركت سازنده نيست و اين موضوع به نفع هكر تمام مي‌شود.