بسم الله الرحمن الرحیم

موضوع: SSh

تهیه کننده : ابوالفضل صبری عارفی

درس : آزمایشگاه ریزپردازنده

زیرنظر استاد محترم جناب آقای یغمایی

نیمسال 4022

در گذشته ریموت کردن (اتصال کامپیوترها) با پروتکل‌های بسیار ساده‌ای به نام(telnet) انجام می‌شد.

تلنت اصلاً امن نیست و مناسب شبکه محلی به صورت موقت است.

تلنت در سال ۱۹۶۹ برای ارتباط و ریموت کردن یک کامپیوتر از راه دور به وسیله خط فرمان درون شبکه ابداع شد.

این پروتکل اطلاعات را بدون هیچ لایه امنیتی و خیلی واضح ارسال می‌کند و هکرها می‌توانند بین راه اتصال این پروتکل قرار گیرند.

و امروزه این پروتکل جای خودرا به پروتکل امن تر و جدیدتر مانند ssh داده است.

Ssh یا secure shell که پروتکل پوسته امن نامیده می شود که در سال 1995 توسط یک مهندس کامپیوتر به نام tatu ylonen در دانشگاه کشور فنلاند توسعه یافت.

Ssh تحت استاندارد IEFT (internet engineering task force) و روی پورت شماره 22 کار میکند. IEFT سازمانی است که از سال 1986 بر پروتکل های کامپیوتری نظارت دارد.

Ssh در سال 1995 طراحی شد پس از اینکه نقص هایی در نسخه اولیه پیدا شد در سال 2006 نسخه دوم یعنی ssh-2 توسعه پیدا کرد. این دو نسخه به دلیل تفاوت‌هایی که در نوع کدگذاری دارند با هم سازگار نیستند.

کلید ssh چیست ← کلید ssh همان کد امضای دیجیتال است که اتصالات و ارسال و دریافت داده ها بر اساس آن کدگذاری و به اصطلاح Hash می شود تا اطلاعات با امنیت منتقل شوند. در واقع امضای دیجیتال در ابتدای اتصال برای هردو کامپیوتر به صورت خودکار تنظیم می شود تا در حین ارسال اطلاعات رمزنگاری شوند و حین دریافت با همین امضای دیجیتال اطلاعات بازگشایی می شود.

در واقع امضای دیجیتال رشته کدی است که لا به لای اطلاعات پخش می شود و کل اطلاعات را ناخوانا می کند. هیمن امر باعث ایجاد یک لایه امنیتی می شود.

پروتکل ssh اطلاعات را با ترکیبی از الگوریتم های RSA PUBLIC KEY , SHA-512, SHA-256 رمزنگاری میکند. امضای دیجیتال ← RSA

کلید های ssh در پوشه ی ssh. در پوشه اصلی کاربر ذخیره می شود.

در V2RAY هم از ssh استفاده می شود. v2ray یک فناوری جدید که از ترکیب فناوری VPN و پروتکل هایی مانند shadow socks , MTproto , Vless , Vmess اطلاعات را با پروتکل ssh رمزنگاری میکند .

کاربرد پروتکل ssh چیست ← اساساً این پروتکل برای ارتباط امن و تأیید امنیت اتصالات کاربرد دارد. با توجه به امکاناتی که به این پورت اضافه شده است، می‌توان گفت که SSH مانند یک فایروال عمل می‌کند و می‌تواند جلوی رخنه‌های امنیتی را بگیرد. از امکانات و کاربردهای SSH می‌توان به موارد زیر اشاره کرد:

- **امکان تایید کاربران**
- **ایجاد تونل امن در بستر TCP/IP**
- **انتقال فایل امن و محافظت شده**
- **بالا بردن امنیت زیر ساخت‌های شبکه**
- **ایجاد شبکه‌های ارتباط امن با V2ray**

چرا ssh روی پورت 22 کار میکند ؟

در فضای اینترنت شماره پورت ها توسط (IANA (internet assigned numbers authority

اختصاص داده می شود. در اون دوران پروتکل telnet روی پورت 21 بود و FTP روی پورت 23 بود ، بنابراین اقای Ybnen تصمیم گرفت روی پورت 22 رزرو کند برای شناخته شدن بیشترssh

سرور ssh چیست ← سرور های میزبان مخصوصا سرور های لینوکسی برای دسترسی به اطلاعات و پیکر بندی از راه دور می بایست همزمان پکیج ssh را روی خود نصب و اجرا داشته باشند. در این حالت به این سرور ، سرور ssh گفته می شود.

وصل شدن به سرور با ssh ← در سیستم عامل های مکینتاش و لینوکس بدون هیچ نرم افزار جانبی می توان از طریق ترمینال به کامپیوتر مقصد متصل شد.

با کد ← ssh root@serverip –p port

در ویندوز هم در صورت نصب بودن پکیج ها (OpenSSH Client)می شود با windows power shell به سرور وصل شد.

با کد ← ssh username(root)@192.1.1.10

و همچنین در ویندوز می توانید از نرم افزار منبع باز و رایگان Putty استفاده کنید.(رایج ترین راه)

سوالات:

1 - امکانات و کاربرد های پروتکل sshچیست ؟

- **امکان تایید کاربران**
- **ایجاد تونل امن در بسترTCP/IP**
- **انتقال فایل امن و محافظت شده**
- **بالا بردن امنیت زیر ساخت‌های شبکه**
- **ایجاد شبکه‌های ارتباط امن با V2ray**

2 – چرا ssh روی پورت 22 کار می کند؟

چون پروتکل telnet روی پورت 21 بود و FTP روی پورت 23 بود ، برای شناخته تر شدن ssh آن را روی پورت 22 رزرو کردند.

3 – کلید ssh چیست ؟

کلید ssh همان کد امضای دیجیتال است که اتصالات و ارسال و دریافت داده ها بر اساس آن کدگذاری و به اصطلاح Hash می شود تا اطلاعات با امنیت منتقل شوند.

4 – پروتکل ssh اطلاعات را با چه الگوریتم هایی رمزنگاری می کند؟

با ترکیبی از الگوریتم های RSA PUBLIC KEY , SHA-512, SHA-256

5 – نرم افزار ویندوزی برای اتصال به سرور از طریق ssh چیست؟؟

نرم افزار منبع باز و رایگان Putty