

بسم الله الرحمن الرحيم

SSH

ابوالفضل صبرى عارفى



پروتکل Telnet



- 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 خود را به پروتکل امن تر و جدیدتر مانند **ssh** داده است.

ssh چیست



- Ssh یا secure shell که پروتکل پسته امن نامیده می شود که در سال ۱۹۹۵ توسط یک مهندس کامپیوتر به نام tatu ylonen در دانشگاه کشور فنلاند توسعه یافت.
- Ssh تحت استاندارد IETF (internet engineering task force) و روی پورت شماره ۲۲ کار میکند.
- IETF سازمانی است که از سال ۱۹۸۶ بر پروتکل های کامپیوتری نظارت دارد.



- Ssh در سال ۱۹۹۵ طراحی شد پس از اینکه نقص هایی در نسخه اولیه پیدا شد در سال ۲۰۰۶ نسخه دوم یعنی ssh-2 توسعه پیدا کرد. این دو نسخه به دلیل تفاوت هایی که در نوع کدگذاری دارند با هم سازگار نیستند.

کلید SSH



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. همین امر باعث ایجاد یک لایه امنیتی می شود.

الگوریتم های رمزنگاری SSH



پروتکل **ssh** اطلاعات را با ترکیبی از الگوریتم های زیر رمزنگاری میکند.

۰۳

SHA-256

۰۲

SHA-512

۰۱

RSA PUBLIC KEY

یک نمونه کلید SSH

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyBLAABArMFQyORQrnsqOPnP6v6/j6rIRl9ie8TrY3uWXq1MQ
Hk6DwdvUMZbvQo9NnpNMsxE9JTS+mNwjri7/Me9/Q5m6AeoC+me+FCG/vxLjWerF
fD2s8AVSRz/57A+2218URgqx8yfUJMNf1/1jcWg0IpUpylDhol3ELgON5PntVr7
ygME0ITgsuRN8o6r1Cj2E7SkBgsfbQfPwmmGAE0oyM7VM5EWMPE418iXoN8gnMYk
4towZR/92n3caDs7kY7dcjY0dLorOWYaJV9yVjyu4muhSGnmYwLX7tyGNyKsFERl
fG4U7kfS3Qze013eNJsVMqOmK2wNuHjjTM9YwIBIwKCAQEAwltbbcaQWtVyndkU
blvw1HCqCRFDzgWRfyo0AEfLXC99ZJnVJMFMyvLOIYtO0vGb29+MVi4A41B+oxit
oeSC4A05zKP2hYQ9aEeFcqRxIA04SLgtjqJQOZ7E9MHONcYfWMLDPLnusbGpgs4M
t58Ly4zIGwoJF231bh8jNNANz5VGmovGrZrK59W4Ger+3M1NokIQJpV8/In7w5Q7
IQZjQ8PNZvx1Dl0UWzVgTzECskxttWStZPlCf3u549TedJ0mUp1ed111gkpzPTva
nU15/QsJBkfoJdDkLigy0F4WxDnhW4qeCmBAUAmB1KQLLbu7LYgQjy9ce9JEUcPUt
a574mwKBgQDlflmCmLW1g5GdeUm/V//aeMML+gBprgqASE6LSvRBVPNIfi6xqSC/
hi2sm8pgkZ+y1b01BPuu5tlwZ4JvI5Gvauow7rXJc3yYmBbRlZU7H0MB7yR7Jo0t
zNgC3vlaVIqOuSsqkvUWDPBQ3tjOKPgyYkdazrMFoUPhCO7WcFEy2BQKBgQDfLoC1
JD0F90KNPQqIPsqIuCHoiJLQRPob+YKPIMGEIdQUYJxBoU/YTn9s22nhddKie5Mu
UEDToLCZYs15NgfGLWElnzrqgqWj7kwFopEMdkEjqQwvoJS+oUnVdaBuzVPfIoOH
eD31I5RH1LXpBEVD3cJ6bwaGahEGHXsvUGNaRwKBgQCWz19kcvsQ4W5RijfG4g6I
QLqWGVC6ea8hGZKzToNA4A2WCcbpxumibQykoOQTkuVJomZkq4DSBWPRLhPiolhr
9c0Y12GEYdWIlbKm++W5IywIldYlCrSLz8EmdUTGVNAUpZENK+vZ5abiyDB/apqQ
JVKTVESVAgI6JzzUR9qjfwKBgQDMDUJrGdFkiB+XEzzUVqqLoQkPHcg03/qd0+UV
JUM2+luAWFRZQwcsKoMhsqnytN3WY1quAEE2hEmwz1zG18yYTg+tXmHAd3LfBcHZ
RCzYMZqkQs1QHcnS3JtG0fHEY/TpRCB726ZceE0OPtIOISlint2xxJhAYPmfMOWn
mfRvywKBgQDS+c/92OQwJ4g7KHY9tdxoNKbfyUbw+KX+1FU61If2KmE5wg/Y9GzO
8lu7SOMb6wTSSdkV4a9K+z+zRqE78/zmYh3QcN97Zj5DLeUW8KrSrJHCI7yXImHP
8oq/wlCYVMcLn8Qpu9Sx3TKAZDOju0Jp66QrcI3/DZV1A/B2aMIAJw==
-----END RSA PRIVATE KEY-----
```



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

```
Command Prompt - ssh-keygen
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

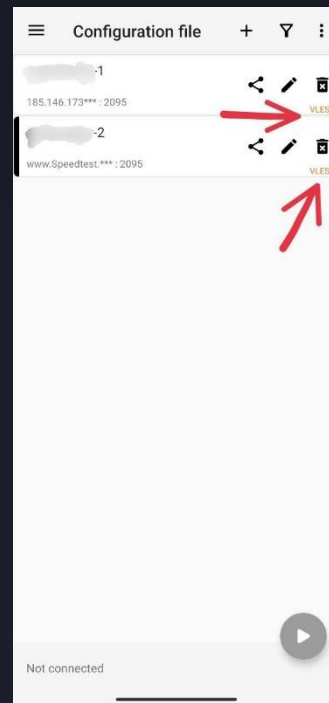
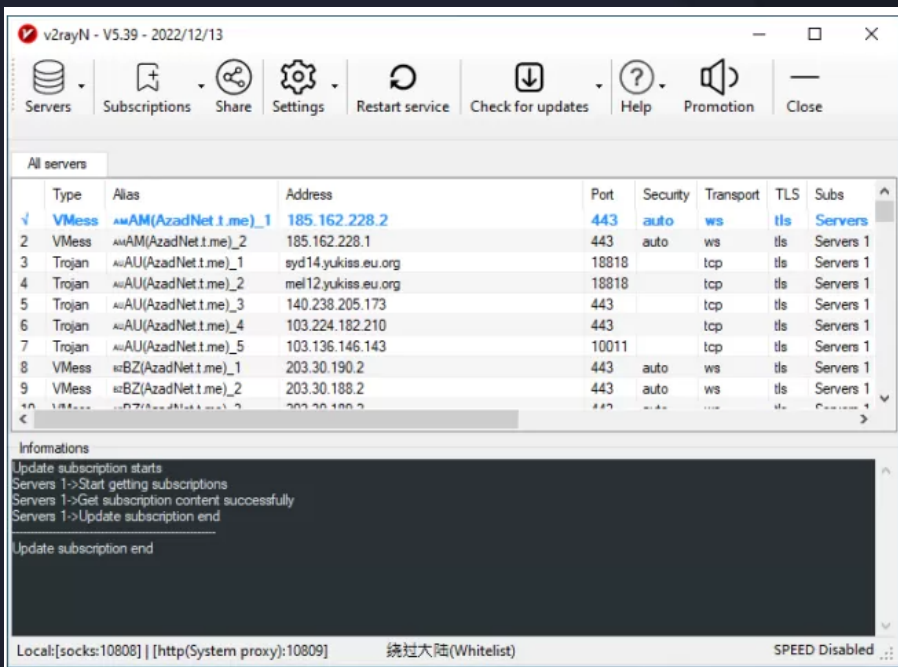
H:\>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\dlefevre\.ssh\id_rsa): _
```

This PC > Local Disk (C:) > Users > dlefevre > .ssh

Name	Date modified	Type	Size
id_rsa شناسه	7/15/2022 12:47 PM	File	3 KB
id_rsa.pub کلید عمومی	7/15/2022 12:47 PM	PUB File	1 KB



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



کاربرد پروتکل SSH



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.

امکانات و کاربردهای SSH

- امکان تأیید 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.

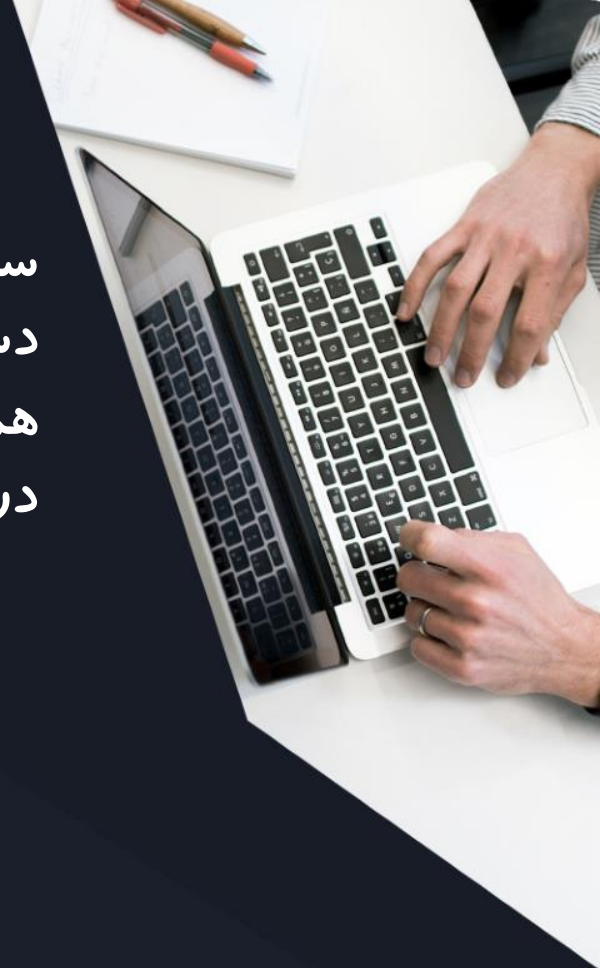
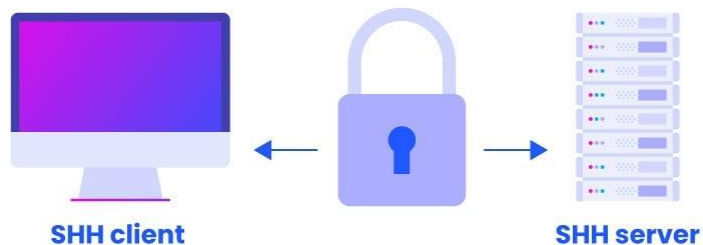


Internet Assigned Numbers Authority

در اون دوران پروتکل telnet روی پورت ۲۱ بود و FTP روی پورت ۲۳ بود ، بنابراین اقای Ybnen تصمیم گرفت روی پورت ۲۲ رزرو کند برای شناخته شدن بیشتر ssh

سرور SSH

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`

```
Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

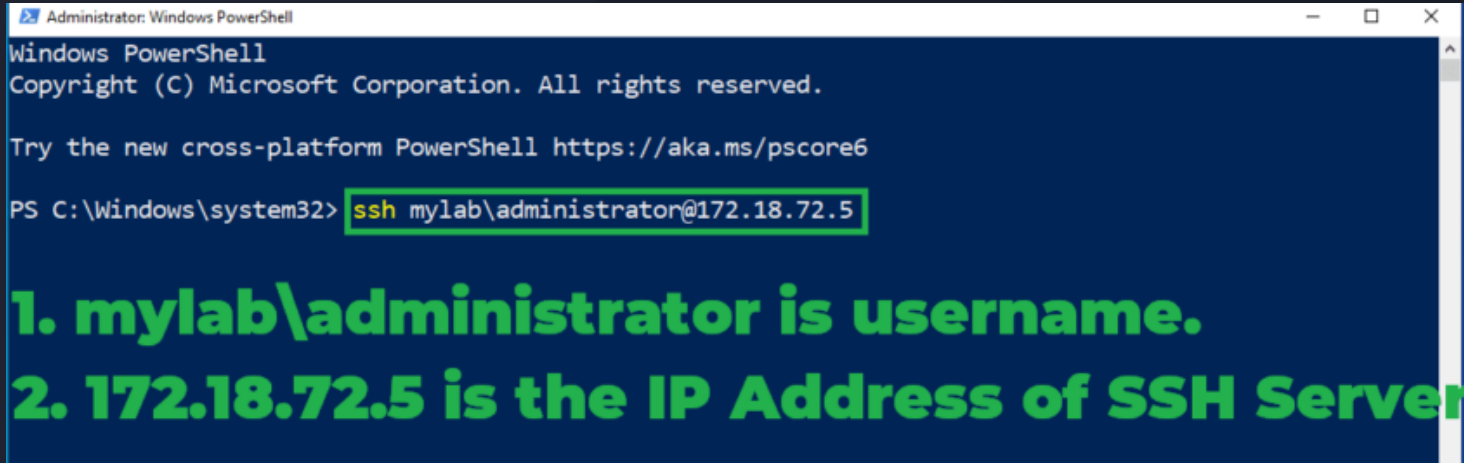
C:\Users\iran>ssh root@192.168.1.1 -p 22|
```



وصل شدن به سرور با SSH

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`

A screenshot of a Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The window has a dark blue background with white text. It displays the standard PowerShell startup text: "Windows PowerShell", "Copyright (C) Microsoft Corporation. All rights reserved.", and "Try the new cross-platform PowerShell https://aka.ms/pscore6". The prompt "PS C:\Windows\system32>" is followed by the command "ssh mylab\administrator@172.18.72.5", which is highlighted with a green rectangular box.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> ssh mylab\administrator@172.18.72.5
```

1. mylab\administrator is username.

2. 172.18.72.5 is the IP Address of SSH Server



نرم افزار Putty



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

PuTTY یک نرم افزار رایگان ارتباط از راه دور است که از پروتکل های مختلفی چون SSH، Telnet، SCP و rLogin پشتیبانی می کند.

این نرم افزار بصورت رسمی برای سیستم عامل ویندوز ارائه شده است، اما در پلت فرم های مختلف **UNIX** نیز، در دسترس است.

از جمله کاربرد **Putty** را می توان به این صورت تعریف کرد که با بعنوان یک ابزاری است که امکان اتصال به سرور مجازی یا سرور ابری از طریق **SSH** می دهد.

چگونه با Putty به سرور متصل شویم



۰۱

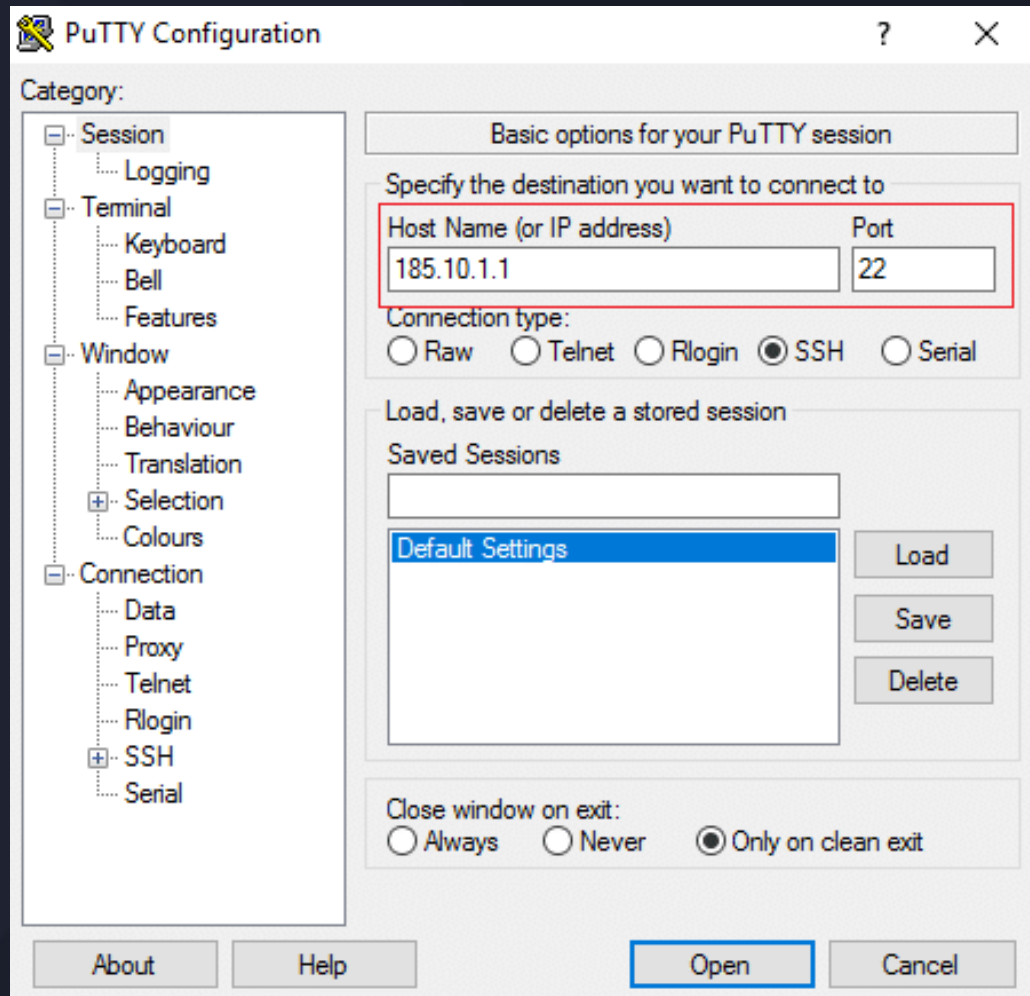
در بخش Host آدرس IP
سرور مقصد را وارد می‌کنیم.

۰۲

در بخش PORT شماره
پورت را وارد می‌کنیم.
پیش فرض ۲۲.

۰۳

نوع ارتباط را در بخش
Connection type
بر روی SSH قرار می‌دهیم.



با تشکر از توجه شما

