امنیت فیزیکی، Hashing، SHA، خط‌مشی‌های امنیتی مدیریت

آموزش رایگان دوره نتورک‌پلاس (Network+) (بخش 53)

در شماره گذشته آموزش نتورک‌پلاس با ریسک‌های بدافزاری، ارزیابی امنیتی و ابزارهای پویش آسیب‌پذیری‌ها آشنا شدیم. در این شماره مبحث فوق را ادامه خواهیم داد.

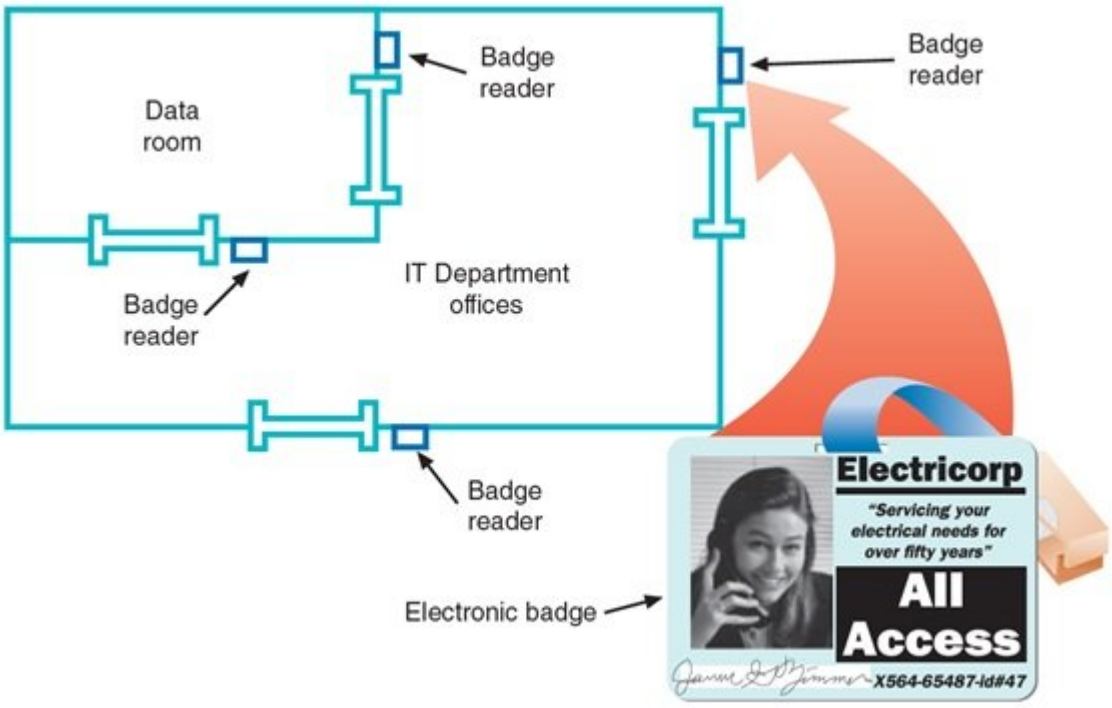
برای مطالعه بخش پنجاه و دوم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

امنیت فیزیکی

در بحث امنیت فیزیکی لازم است دسترسی فیزیکی به تمام مولفه‌های حیاتی شبکه محدود و کنترل شود. در بحث تهدیدات فیزیکی به مواردی همچون آسیب‌رساندن به تجهیزات گران‌قیمت یا سرقت دستگاه‌ها، اتصال تجهیزات غیرمجاز به پورت‌های کنسول محافظت نشده و.... می‌توان اشاره کرد. در بحث امنیت فیزیکی تنها کارمندان قابل اعتماد باید به اتاق‌های سرور، مراکز داده، اتاق‌های ذخیره‌ساز و سایر مکان‌هایی که تجهیزات حساس درون آن‌ها قرار دارد دسترسی داشته باشند. از جمله مکانیزم‌ها و ابزارهایی که به لحاظ فیزیکی مانع دسترسی افراد به مکان‌های حساس می‌شوند به مواردی همچون **keypad** یا **cipher lock** (قفل‌های فیزیکی هستند که برای باز کردن یک درب به کد نیاز دارند و ریسک گم شدن کلیدها را کاهش می‌دهند)، **key fob** (یک مکانیزم کنترل از راه دور را همراه با سامانه‌های امنیتی به قفل‌ها اضافه می‌کند و اجازه می‌دهد از راه دور قفل درب‌ها را باز یا بسته کنید)

access badge (بیشتر سازمان‌ها به کارمندانی نیاز دارند که نوع خاصی از شناسه دسترسی هویتی موسوم به badge را دارند، شناسه‌ای که شامل تصویر، عنوان و سایر اطلاعاتی هویتی است. البته برخی از سازمان‌ها نیز از کارت‌های هوشمندی استفاده می‌کنند که افراد برای باز کردن درب‌ها با کشیدن آن‌ها روی محفظه خاصی درب را باز

می‌کنند)، **proximity card** (مکانیسم برخی از کارت‌های هوشمند که به نام کارت‌های مجاورتی نیز شناخته می‌شوند به گونه‌ای است که افراد نیازی ندارند تا کارت را به شکل مستقیم روی محفظه کارت‌خوان بکشند، زیرا کارت‌خوان درون یک دیوار یا محفظه مربوطه جاسازی می‌شود. به‌طور معمول این کارت‌ها در بازه 10 تا 5 سانتی‌متری توسط تراشه مربوطه شناسایی می‌شوند.)



biometrics(یک راهکار امنیتی گران‌قیمت است که از ویژگی‌های منحصر به فراد زیستی افراد به منظور دسترسی به دستگاه‌ها یا مکان‌های مختلف استفاده می‌کند. به‌طور مثال، شما با هندسه کف دست یا الگو عنبیه یا اثرانگشت خود قادر هستید درب‌هایی را باز کرده یا به دستگاه‌هایی دسترسی داشته باشید.) اشاره کرد.

راهکاهایی که برای دسترسی فیزیکی ایمن به آن‌ها اشاره کردیم، هر یک معایب خاص خود را دارند و ممکن است رخنه‌ای در آن‌ها مستتر باشد. کلید محافظت از داده‌های حساس و ایمن تشخیص نفوذ در کوتاه‌ترین زمان و پاسخ‌گویی مناسب به آن است. علاوه بر تشخیص وجود یک رخنه، سازمان‌های بزرگ از فناوری‌های پیشرفته تشخیصی همچون حس‌گرهای تشخیص دما (**Tamper detector**) به منظور بررسی دمای محیط، سامانه‌ها و حس‌گرهای تشخیص حرکت، دوربین‌های نظارت تصویری **CCTV** سرنام **closed-circuit TV**، برچسب‌های پیگیری دارایی‌ها (**Asset tracking tags**) که برای بررسی وضعیت یک محصول استفاده می‌شوند همچون برچسب‌های **آراف‌ای‌دی** استفاده می‌کنند.

نکته: آزمون نتورک‌پلاس از شما انتظار دارد در بحث امنیت فیزیکی بتوانید خلاصه‌ای از اقدامات و راهکارهایی که امنیت فیزیکی را برای زیرساخت‌ها به ارمغان می‌آورند را تشریح کنید. پیشنهاد می‌کنم برای هر یک از کلیدواژه‌هایی که در بالا به آن‌ها اشاره شد، جست‌وجویی در اینترنت انجام دهید.

Device Hardening

در کنار ایمن‌سازی دستگاه‌های شبکه در برابر تهدیدات خارجی، شما باید در راستای بهبود ایمنی دستگاه‌های شبکه چه در بعد نرم‌افزار و چه در بعد سخت‌افزاری گام‌های بیشتری بردارید. این راهکارها به نام Device hardening شناخته می‌شود. از جمله این راهکارها می‌توان به موارد زیر اشاره کرد.

به‌روزرسانی‌ها و وصله‌های امنیتی: به‌روزرسانی سیستم‌عامل، نرم‌افزارها و میان‌افزار دستگاه‌ها با هدف برطرف کردن باگ‌ها، اضافه کردن قابلیت‌های جدید و بستن شکاف‌های امنیتی انجام می‌شود. نصب وصله‌های امنیتی قواعد خاص خود را دارد و بهتر است به شکل گام به گام انجام شود. به عبارت دیگر، مرحله اول شناسایی-discovery (در این مرحله کشف می‌کنید چه موجودیت‌هایی در شبکه شما قرار دارند که باید از آن‌ها محافظت شود) است، مرحله دوم استانداردسازی-standardization (به‌روزرسانی مداوم سیستم‌عامل و نرم‌افزارهایی است که روی شبکه اجرا می‌شوند)، مرحله سوم، امنیت لایه‌بندی شده-layered security (امنیت لایه‌بندی شده اشاره به دفاع‌های متعددی دارد که از یک شبکه واحد محافظت می‌کنند)، مرحله چهارم، گزارش‌گیری آسیب‌پذیری‌ها-vulnerability reporting (شناسایی و اولویت‌بندی مسائل مربوط به امنیت و انتشار وصله‌های ضروری است.)، مرحله پنجم، پیاده‌سازی-implementation (پیاده‌سازی وصله‌ها که شامل اعتبارسنجی، اولویت‌بندی، آزمایش و استفاده از آن‌ها است.)، مرحله ششم، ارزیابی-assessment (شما موفقیت پیاده‌سازی وصله‌ها و تاثیر کلی وصله‌ها را ارزیابی می‌کنید.) و در نهایت مرحله هفتم، کم کردن ریسک-risk mitigation (در بعضی موارد ممکن است امکان نصب وصله‌ها وجود نداشته باشد. به‌طور مثال، یک وصله جدید ممکن است با نرم‌افزار قدیمی روی سرور سازگاری نداشته باشد.)

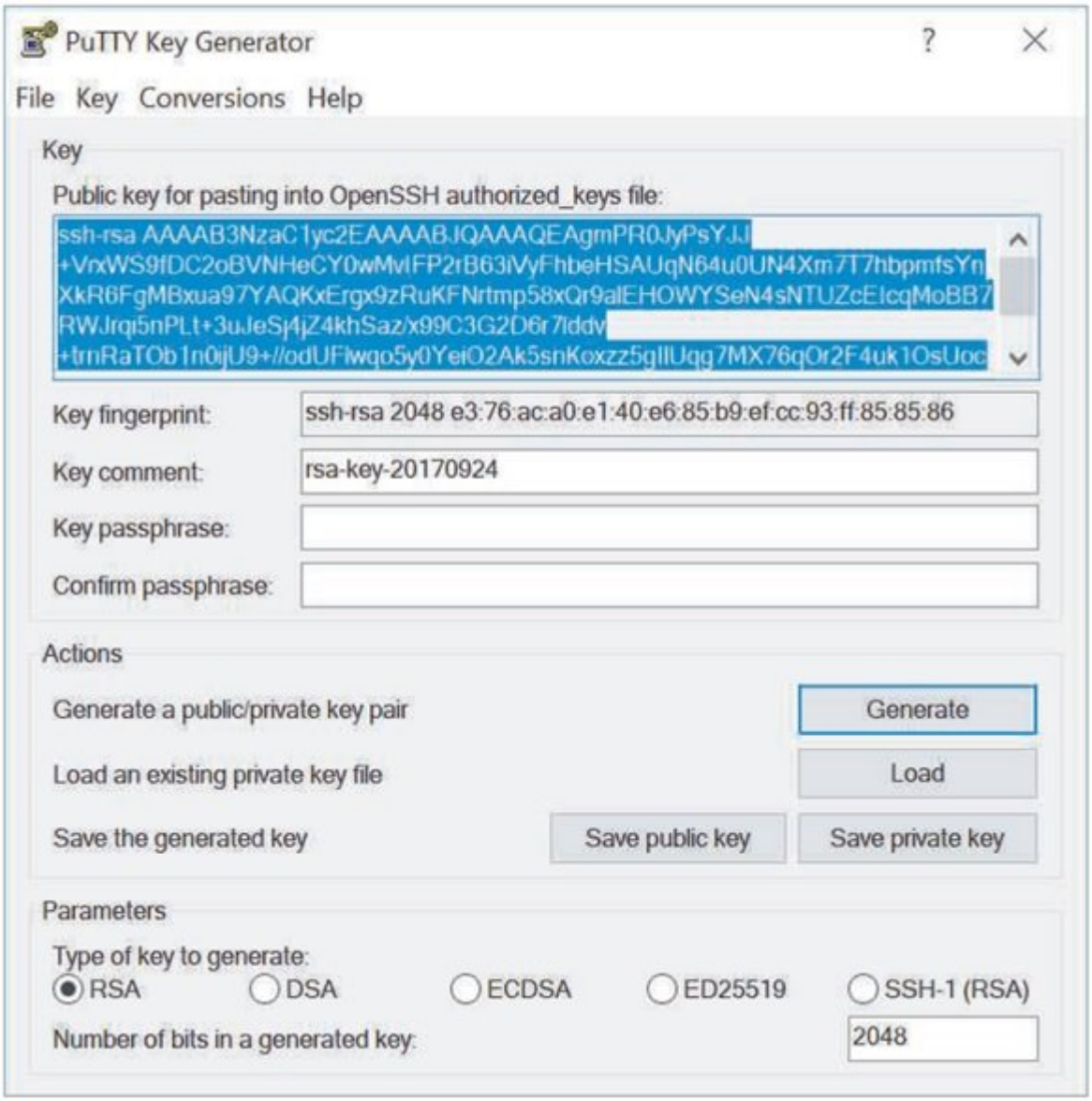
نکته: آزمون **نتورک‌پلاس** از شما انتظار دارد برای محافظت از تجهیزات تحت شبکه یک سناریو مناسب را ارائه کرده، فناوری‌ها و راهکارهای رایج در این زمینه را توصیف کنید.

گواهی‌نامه‌های مدیریتی

بیشتر دستگاه‌ها از طریق یک رابط مدیریتی مرکزی که نام کاربری و گذرواژه پیش‌فرضی که معمولا admin یا 12345 روی آن‌ها قرار گرفته است مدیریت می‌شوند. با توجه به این‌که ترکیب فوق بیش از اندازه رایج است، در نتیجه غیر ایمن است و متاسفانه مدیران شبکه‌ها حتا در سازمان‌های بزرگ نیز سعی نمی‌کنند پارامترهای پیش‌فرض را تغییر دهند. (برای اطلاع بیشتر در ارتباط با مباحث مرتبط با رمزهای عبور به بخش **گذرواژه‌ها** در سایت مجله شبکه رجوع کنید.)

اگر به خاطر داشته باشید به شما گفتیم که ویژگی دسترسی و مدیریت از راه دور روی بسیاری از دستگاه‌ها تعبیه شده است. پروتکل SSH یکی از پر استفاده‌ترین‌های این حوزه است که از کلید این پروتکل می‌توان برای تأیید اعتبار دستگاه‌هایی که قصد برقراری ارتباط از راه دور را دارند استفاده کرد. این رویکرد به ویژه برای مدیران سیستمی، کاربران خاص یا زمانی که استفاده از اتصالات SSH برای فرآیندهای خودکار مانند انتقال فایل، معاملات مالی یا به‌روزرسانی تنظیمات نیاز است، راهگشا است. در زمان برقراری ارتباطات از راه دور کلیدهای SSH ایمن‌تر از گذرواژه‌ها هستند، زیرا فرآیند شکستن یک کلید رمزنگاری شده ایمن به مراتب سخت‌تر از یک گذرواژه عادی است. با این وجود همانند گذرواژه‌ها و نام‌های کاربری تنظیمات این کلیدها نیز باید از حالت پیش‌فرض خارج شود.

شکل زیر یک PuTTY Ky Generator را نشان می‌دهد که برای ساخت جفت کلیدهای SSH از آن استفاده می‌شود.



Security Policies for Users

یکی دیگر از موضوعات مرتبط با شبکه‌ها و به ویژه مدیریت شبکه‌ها در ارتباط با مجوزها و سطح دسترسی کاربران است. یک مدیر شبکه باید به کارمندان یک سازمان بر اساس جایگاه شغلی که در اختیار دارند مجوزهای مربوطه را تخصیص دهد. برای اطلاع بیشتر در خصوص انواع مختلف مجوزها پیشنهاد می‌کنم به مطلب **Types of 7 Privileged Accounts You Should Know** مراجعه کنید.

Hashing

هش کردن به معنای تبدیل داده‌ها از طریق به‌کارگیری الگوریتمی است که عموما فضای مورد نیاز برای داده‌ها را کاهش می‌دهد. هش کردن متفاوت از رمزگذاری است، هرچند در اغلب موارد به عنوان یک نوع رمزگذاری به آن اشاره می‌شود که به شیوه مشابهی، داده‌ها را از یک فرمت به فرمت دیگری تبدیل می‌کند. داده‌های رمزگذاری شده را می‌توان رمزگشایی کرد، اما این امکان برای داده‌های هش شده میسر نیست. هش کردن عمدتا براي اطمینان از صحت داده‌ها و این‌که تغییری در داده‌ها به وجود نیامده باشد استفاده می‌شوند. با این حال، هش‌ها می‌توانند نقش مهمی در یک پروتکل رمزنگاری بازی کنند. اگر از یک الگوریتم امن استفاده شود، بازگرداندن هش‌ها تقریبا ناممکن است. متداول‌ترین الگوریتم هش‌سازی که امروزه از آن استفاده می‌شود الگوریتم SHA سرنام Secure Hash Algorithm است. مزیت اصلی SHA در مقایسه با الگوریتم‌های قدیمی‌تر به پایداری آن در برابر تصادم باز می‌گردد.

یک تصادم زمانی اتفاق می‌افتد که دو منبع داده متفاوت هش یکسانی را تولید می‌کنند. با این حال، مکانیزم‌های امنیتی بیشتری برای جلوگیری از به وجود آمدن تصادم ابداع شده است تا هش‌های طولانی‌تر و ایمن‌تری ایجاد شوند. چندین نسخه مختلف از SHA به شرح زیر طراحی شده است:

• SHA-0- نسخه اصلی SHA توسط سازمان NSA توسعه داده و بعدها SHA-0 نامیده شد. این نسخه از یک تابع هش 160 بیتی استفاده می‌کند.

• SHA-1 - نسخه اصلی به واسطه نقص‌های امنیتی به سرعت و یکسری تغییرات با نسخه SHA-1 جایگزین شد. SHA-1 نیز پس از مدتی جای خود را به نسخه بعدی داد، هرچند هنوز هم برخی از سیستم‌ها از نسخه SHA-1 آسیب‌پذیر استفاده می‌کنند.

• SHA-2-نیز توسط NSA طراحی شده است. SHA-2 از انواع مختلف هش پشتیبانی می‌کند که محبوب‌ترین آن‌ها SHA-256 (با هش 256 بیتی) و SHA-512 (با هش 512 بیتی) است. توجه داشته باشید که 2 در SHA-2 به شماره نسخه اشاره دارد، در حالی که مقادیر همراه با واژه SHA همچون SHA-256 و SHA-512 به طول توابع هش اشاره دارند.

SHA-3 - جدیدترین نسخه SHA، نگارش سوم (SHA-3) است که توسط طراحان خصوصی در سال 2012 طراحی شده است. SHA-3 در عمل متفاوت از SHA-2 است، هرچند که این نسخه نیز از توابع هش با طول 256 و 512 بیت استفاده می‌کند.

در بیشتر موارد SHA-2 و SHA-3 برای افزایش امنیت زیرساخت‌ها با یکدیگر استفاده می‌شوند.

نرم‌افزار ضدبدافزار

برخی تصور می‌کنند نصب یک برنامه ضدویروس روی یک شبکه همه مشکلات را برطرف می‌کند. در حالی که محافظت از زیرساخت‌ها در برابر کدهای مخرب به نرم‌افزارهایی به مراتب بیشتر از ضدویروس‌ها نیاز دارد. نرم‌افزارهایی موسوم به ضدبدافزار (**anti-malware**) برای پاسخ‌گویی به چنین نیازی طراحی شده‌اند. یک کاربر ممکن است بلافاصله متوجه وجود نرم‌افزارهای مخرب روی سیستم خود نشود، زیرا نرم‌افزارهای مخرب می‌توانند نشانه‌های وجود خود را به سرعت از یک سیستم پاک کنند. برای اطلاع بیشتر در خصوص ضدبدافزارها و نحوه انتخاب آن‌ها به مقاله **ضدویروس یا ضدبدافزار ،کدام‌یک را باید انتخاب کنیم؟** مراجعه کنید.

زمانی که صحبت از پیاده‌سازی نرم‌افزار ضدبدافزار روی شبکه به میان می‌آید، شما باید یک تصمیم مهم اتخاذ کنید. این نرم‌افزار قرار است در کجا نصب شود. در این زمینه چند سناریو به شرح زیر وجود دارد:

host-based: اگر نرم‌افزار ضد تروجان را روی هر دسکتاپی نصب کنید، ممکن است یکسری مشکلات رایج را برطرف کنید، اما یک اصل مهم که فایل‌های آلوده روی سرور است را نادیده گرفته‌اید. ضد تروجان مبتنی بر میزبان ممکن است بخشی قابل توجهی از یک شبکه مجازی شده را پوشش ندهد.

• server-based: اگر نرم افزار ضد تروجان روی سرور قرار گیرد و هر فایل و تراکنشی را چک کند، از فایل‌های مهم محافظت می‌کند، اما عملکرد شبکه را به میزان قابل توجهی کاهش می‌دهد.

• network-based: ایمن‌سازی گیت‌وی‌های شبکه به معنای آن است که شما مکانی که اینترنت با شبکه داخلی ارتباط برقرار می‌کند را با اضافه کردن یک لایه دفاعی قدرتمند ایمن می‌کنید. با این حال، این مکانیزم از شبکه در برابر خطر فایل‌های آلوده‌ای که روی درایوهای فلش، لپ‌تاپ‌ها یا گوشی‌های هوشمند قرار دارند و ممکن است شبکه را آلوده کنند محافظت نمی‌کند.

• cloud-based: بیشتر راه‌حل‌های ضدبدافزاری از مدت‌ها قبل روی ابر میزبانی شده‌اند. مزیت اصلی ضدبدافزارهای ابرمحور در گسترش‌پذیری، افزایش بهره‌وری، کاهش هزینه‌ها و منابع مشترک استوار است. البته این مدل با یکسری چالش‌ها روبرو است که ممکن است همه شبکه را به درستی تحت پوشش قرار ندهد. دقت کنید راه‌حل های ابرمحور به میزان قابل توجهی ترافیک اینترنت را برای انجام وظایف خود مصرف می‌کنند.

خط‌مشی‌های امنیتی مدیریت کاربران

منشا بروز بیشتر نقض‌های امنیتی شبکه خطای انسانی است. اما راهکارهایی برای به حداقل رساندن این مدل خرابی‌ها وجود دارد که خط‌مشی‌های امنیتی که به خوبی برنامه‌ریزی شده و قادر هستند به شکل درستی کاربران را مدیریت کنند از جمله این موارد هستند. یک خط‌مشی امنیتی وضعیت کاربران شبکه، اهداف امنیتی، ریسک‌ها، سطح اختیارات، مسئولیت‌ها و نحوه هماهنگ کردن کارمندان با یکدیگر و دپارتمان امنیت اطلاعات را مشخص می‌کند. علاوه بر این، مشخص کننده این مسئله است که چگونه به نقض‌های امنیتی باید رسیدگی شود، اما در عین حال قرار نیست به شکل دقیق مشخص کند چه سخت‌افزاری، نرم‌افزار، معماری یا پروتکل‌هایی برای اطمینان‌بخشی باید استفاده شوند و همچنین قرار نیست مشخص کند چگونه سخت‌افزارها یا نرم‌افزارها نصب و پیکربندی شوند، زیرا این جزییات دائما در حال تغییر هستند و فقط مدیران شبکه یا مدیران ارشد باید از آن اطلاع داشته باشند. بر همین اساس باید اهدافی که قرار است در خط‌مشی امنیتی لحاظ شوند در قالب یک سند سازمانی تدوین شوند. برای اطلاع بیشتر در این خصوص به مطلب **Information Security Principles of Success** مراجعه کنید.

در شماره آینده آموزش **نتورک‌پلاس** مبحث مدیریت ریسک‌ها در شبکه را خاتمه داده و به سراغ امنیت در طراحی شبکه خواهیم رفت.

تاریخ انتشار:
01 خرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/network-tricks/15374/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3-network-%D8%A8%D8%AE%D8%B4-53