

برقراری ارتباط ایمن در شبکه‌های ناامن

(با آموزش دستورات متنی و پیکره‌بندی نرم افزار PuTTY
جهت استفاده در محیط سر، مبتنی بر ویندوز، لینوکس و یونیکس)

نویسندگان:

مصطفی اخوان صفار

(عضو هیات علمی دانشگاه پیام نور)

مصطفی مختاری اردکان

(عضو هیات علمی دانشگاه پیام نور)

سرشناسه	اخوان صفار، مصطفی، ۱۳۶۱-
عنوان و نام پدیدآور	برقراری ارتباط ایمن در شبکه‌های ناامن (با آموزش دستورات متنی و پیکره‌بندی نرم افزار PuTTY جهت استفاده در محیط‌های مبتنی بر ویندوز، لینوکس و یونیکس) / نویسندگان مصطفی اخوان صفار، مصطفی مختاری اردکان.
مشخصات نشر	مشهد: انتشارات خط اول، ۱۳۹۴
مشخصات ظاهری	۱۱۲ ص: مصور، جدول، نمودار
شابک	978-600-95208-8-6
وضعیت فهرست‌نویسی	فیا
موضوع	سامانه‌های امنیتی - نرم افزار
موضوع	پروتکل‌های شبکه کامپیوتری
موضوع	کامپیوترها - ایمنی اطلاعات
شناسه زوده	مختاری اردکان، مصطفی، ۱۳۶۳
رده‌بندی کنگه	۱۳۹۴ الف ۳۷/ب ۳۷۳۷/۳
ردیف ملی	۶۲۱/۳۸۹۲
شماره ثبت‌شناسی ملی	۴۱۳۴۴۲۹



تلفن: ۰۵۱۳۷۵۲۹۹۹۳

www.khate-aval.com

info@khate-aval.com

نام ناشر: انتشارات خط اول

نام کتاب: برقراری ارتباط ایمن در شبکه‌های ناامن

نویسندگان: مصطفی اخوان صفار، مصطفی مختاری اردکان

صفحه‌آرا: نفیسه اسماعیلی

شمارگان: ۱۰۰۰ جلد

نوبت چاپ: اول / زمستان ۱۳۹۴

چاپخانه: معین

قیمت: ۶۵۰۰ تومان

شابک: ۹۷۸-۶۰۰-۹۵۲۰۸-۸-۶

نماینده‌ی فروشی: مشهد- خیابان سعدی- بازارچه کتاب- شماره ۲۵- کتابفروشی درخشش

تلفن: ۰۵۱۳۲۲۵۱۹۲۳

این اثر مشمول قانون حمایت مولفان و مصنفان و هنرمندان است و هرگونه کپی برداری و نشر از تمام یا قسمتی از این اثر بدون اجازه مولف (ناشر) منع شرعی و قانونی داشته و مورد پیگرد قانونی قرار خواهد گرفت.

چکیده

با توجه به استفاده روزافزون از شبکه‌های کامپیوتری در کاربردهای تجارت الکترونیک و بانکداری الکترونیک نیاز به برقراری ارتباط ایمن در بین کاربران بیشتر احساس می‌شود. ایمنی را در لایه‌های مختلف شبکه می‌توان به وجود آورد. در لایه‌های بالایی شبکه به علت ایمن کردن بخشی از ترافیک، باعث کاهش سرشار به شبکه می‌شود به همین دلیل تلاشهای فراوانی برای ایجاد کانال‌های ایمن در این لایه صورت گرفته است. ایجاد ایمنی در لایه‌های بالای شبکه نیاز به اعمال تغییراتی در برنامه‌های کاربردی می‌باشد و برخلاف پروتکل‌های IP-sec، SSL و TLS طرفین ارتباط باید کاملاً از وجود کانال ایمن مطلع باشند.

در دهه گذشته برنامه‌های فراوانی برای کمک به ادگی استفاده از ایمنی در لایه کاربرد ارائه شده است که یکی از محبوب‌ترین و پرکاربردترین آنها نام PuTTY بوده است. در این کتاب به نحوه استفاده از این نرم افزار برای ایجاد یک کانال ایمن خواهیم پرداخت. این نرم افزار علاوه بر نشست SSH قابلیت ایجاد نشست‌های Telnet، Rlogin، Serial و Raw را نیز دارد که سعی شده بیشتر به پروتکل SSH بپردازیم.

در فصل اول مقدمه‌ای در مورد لزوم برقراری امنیت در لایه کاربرد و پروتکل‌های امنیتی موجود در آن بیان شده و تفاوت‌های نشست‌های ایجاد شده به کمک پروتکل‌های مختلف بیان گردیده است. در فصل دوم راهنمای سریع برای شروع به کار با این نرم افزار آورده شده. فصل سوم شامل مقدمه‌ای عمومی از برخی خصوصیات مهم PuTTY است. در این فصل پیکربندی‌های مهم نرم افزار PuTTY را توضیح می‌دهیم و وارد جزئیات هر یک از گزینه‌ها و منوهای نرم افزار می‌شویم. در فصل آخر هم چگونگی گرفتن این نرم افزار متن باز از اینترنت و طریقه نصب آن بر روی سیستم توضیح داده شده است.

فهرست مطالب

۳	چکیده
۱۳	فصل اول: مقدمه‌ای بر پروتکل‌های انتقال امن
۱۴	۱-۱ امنیت در لایه انتقال پروتکل‌های کاربردی
۱۵	۱-۲ پروتکل SSH و TS
۲۰	۱-۳ پروتکل SSH
۲۲	۱-۴ پروتکل IPsec
۲۳	۱-۵ پروتکل AH
۲۴	۱-۶ پروتکل (ESP)
۲۷	فصل دوم: شروع کار با نرم افزار PuTTY
۲۸	مقدمه
۳۰	۲-۱ شروع یک نشست
۳۱	۲-۲ واریسی کلید میزبان (برای پروتکل SSH)
۳۲	۲-۳ ورود به سیستم
۳۳	۲-۴ بعد از ورود به سرور
۳۳	۲-۵ خروج
۳۴	نتیجه
۳۵	فصل سوم: آموزش استفاده از PuTTY
۳۶	مقدمه
۳۶	۳-۱ در هنگام نشست
۳۶	۳-۱-۱ کپی کردن و الصاق کردن متن
۳۷	۳-۱-۲ بازگرداندن صفحه به عقب

- ۳۷..... ۳-۱-۳ منوی سیستم
- ۳۷..... ۳-۱-۳-۱ event log
- ۳۷..... ۳-۱-۳-۲ دستورات مخصوص
- ۳۹..... ۳-۱-۳-۳ شروع نشست جدید
- ۳۹..... ۳-۱-۳-۴ تغییر تنظیمات نشست
- ۴۰..... ۳-۱-۳-۵ کپی کردن همه فضای ذخیره سازی موقت داده (Clipboard)
- ۴۰..... ۳-۱-۳-۶ پاک کردن و بازنشانی (resetting) ترمینال
- ۴۰..... ۳-۱-۳-۷ حالت تمام صفحه (Full screen)
- ۴۰..... ۳-۲ جدول ثبت وقایع (log file) برای نشست
- ۴۱..... ۳-۳ تغییر تنظیمات مشخصات
- ۴۱..... ۳-۴ استفاده از روش انتقال X11 در SSH
- ۴۲..... ۳-۵ استفاده از port forwarding در SSH
- ۴۵..... ۳-۶ ایجاد اتصال raw TCP
- ۴۶..... ۳-۷ اتصال به یک خط سرور
- ۴۶..... ۳-۸ خطوط دستور نرم افزار P TTY
- ۴۶..... ۳-۸-۱ شروع یک نشست به کمک خط دستور
- ۴۷..... ۳-۸-۲ '-cleanup'
- ۴۷..... ۳-۸-۳ گزینه‌های خط دستور استاندارد
- ۴۷..... ۳-۸-۳-۱ '-load': بار کردن یک نشست ذخیره شده
- ۴۸..... ۳-۸-۳-۲ انتخاب یکی از پروتکل‌های '-ssh', '-rlogin', '-raw'
- ۴۸..... ۳-۸-۳-۳ توضیحات اضافه
- ۴۸..... ۳-۸-۳-۴ مشخص کردن نام ورودی
- ۴۸..... ۳-۸-۳-۵ '-L', '-R' and '-D': برای برقراری انتقال پورت (port forwarding)
- ۴۹..... ۳-۸-۳-۶ '-m': خواندن یک دستور از راه دور یا اسکریپت از یک فایل
- ۴۹..... ۳-۸-۳-۷ '-P': تعیین شماره پورت
- ۴۹..... ۳-۸-۳-۸ '-pw': مشخص کردن یک پسورد
- ۴۹..... ۳-۸-۳-۹ '-agent' و '-noagent': استفاده از روش Pageant برای اعتبار سنجی
- ۴۹..... ۳-۸-۳-۱۰ '-A' و '-a': کنترل انتقال agent

۵۰	 ۱۱-۳-۸-۳-۳: کنترل انتقال <i>VTI</i>
۵۰	 ۱۲-۳-۸-۳-۳: کنترل تخصیص ترینال کاذب <i>T</i> و <i>T</i>
۵۰	 ۱۳-۳-۸-۳-۳: توقف شروع یک <i>shell</i> یا دستور
۵۰	 ۱۴-۳-۸-۳-۳: یک اتصال شبکه از راه دور را به جای <i>shell</i> یا دستور از راه دور می‌سازد
۵۱	 ۱۵-۳-۸-۳-۳: فعال کردن فشرده سازی <i>C</i>
۵۱	 ۱۶-۳-۸-۳-۳: تعیین نسخه پروتکل <i>SSH</i> و <i>2</i>
۵۱	 ۱۷-۳-۸-۳-۳: تعیین نسخه <i>4</i> و <i>6</i> <i>IP</i>
۵۲	 ۱۸-۳-۳-۳: تعیین کلید خصوصی <i>SSH</i>
۵۲	 ۱۹-۳-۳-۳: نمایش اثر انگشت کلید <i>PGP</i>
۵۲	 نتیجه

فصل چهارم: آموزش پیکره‌بندی *PrFTT*..... ۵۳

۵۴	 مقدمه
۵۴	 ۱-۴ صفحه نشست
۵۴	 ۱-۱-۴ بخش نام‌هاست
۵۴	 ۲-۱-۴ بار کردن و ذخیره سازی یک نشست
۵۵	 ۳-۱-۴ بستن پنجره در هنگام خروج
۵۵	 ۲-۲ صفحه ثبت وقایع (<i>Logging</i>)
۵۵	 ۱-۲-۴ نام فایل ذخیره سازی
۵۵	 ۲-۲-۴ کنترل 'What to do if the log file already exists'
۵۶	 ۳-۲-۴ گزینه 'Flush log file frequently'
۵۶	 ۴-۲-۴ گزینه‌های موجود برای فایل ثبت وقایع در حالت استفاده از <i>SSH</i>
۵۶	 ۱-۲-۴-۲ 'Omit known password fields'
۵۶	 ۲-۲-۴-۲ 'Omit session data'
۵۶	 ۳-۲-۴ متنی <i>Translation</i>
۵۷	 ۱-۳-۴ قسمت <i>character set translation</i>
۵۸	 ۲-۳-۴ گزینه <i>Treat CJK ambiguous characters as wide</i>
۵۸	 ۳-۳-۴ <i>Caps Lock acts as Cyrillic switch</i>

- ۵۹..... ۴-۳-۴ کنترل و نمایش کاراکترهای رسم خط (line-drawing)
- ۵۹..... ۴-۳-۵ copy and paste of line drawing characters
- ۶۰..... ۴-۳-۶ copy and paste of line drawing characters
- ۶۰..... ۴-۴ منوی Selection
- ۶۱..... ۴-۴-۱ فرمت کاراکترهای paste شده
- ۶۱..... ۴-۴-۲ تغییر و کنترل با استفاده از mouse
- ۶۲..... ۴-۴-۳ Shift overrides application's use of mouse
- ۶۲..... ۴-۴-۴ Default selection mode
- ۶۲..... ۴-۴-۵ One-word-at-a-time کنترل و انتخاب مد
- ۶۳..... ۴-۵ منس Colours
- ۶۴..... ۴-۵-۱ Allow terminal to specify 4-bit colours
- ۶۴..... ۴-۵-۲ Allow terminal to use xterm 256-colour mode
- ۶۵..... ۴-۵-۴ Bolded text is a different colour
- ۶۵..... ۴-۵-۵ Attempt to use logical palettes
- ۶۶..... ۴-۵-۶ Use system colours
- ۶۶..... ۴-۵-۷ تنظیم رنگها در پنجره ترمینال
- ۶۶..... ۴-۶ منوی Connection
- ۶۷..... ۴-۶-۱ استفاده از keepalives برای جلوگیری از قطع شدن
- ۶۸..... ۴-۶-۲ Disable Nagle's algorithm
- ۶۹..... ۴-۶-۳ Enable TCP keepalives
- ۶۹..... ۴-۶-۴ Internet protocol
- ۶۹..... ۴-۷ منوی data
- ۷۰..... ۴-۷-۱ Auto-login username
- ۷۰..... ۴-۷-۲ Terminal-type string
- ۷۱..... ۴-۷-۳ Terminal speeds
- ۷۱..... ۴-۷-۴ environment variables
- ۷۲..... ۴-۸ منوی Proxy
- ۷۳..... ۴-۸-۱ proxy type

۷۳.....	۴-۸-۲ جلوه‌گیری از پروکسی شدن قسمتهایی از شبکه
۷۴.....	۴-۸-۳ تحلیل نام هنگام استفاده از پروکسی
۷۵.....	۴-۸-۴ Username and password
۷۶.....	۴-۸-۵ Telnet command or Local proxy command فیلد
۷۷.....	۴-۹ منوی Telnet
۷۷.....	۴-۹-۱ Handling of OLD ENVIRON ambiguity
۷۸.....	۴-۹-۲ Telnet negotiation modes
۷۸.....	۴-۹-۳ Keyboard sends Telnet special commands
۷۹.....	۴-۹-۴ Return key sends Telnet New Line instead of CR
۷۹.....	۴-۱۰ منوی login
۸۰.....	۴-۱۰-۱ Username
۸۰.....	۴-۱۱ منوی SSH
۸۱.....	۴-۱۱-۱ اجرای یک فرمان خاص
۸۱.....	۴-۱۱-۲ تنظیمات مربوط به پروتکل
۸۱.....	۴-۱۱-۳ Enable compression فیلد
۸۱.....	۴-۱۱-۴ Preferred SSH protocol version
۸۲.....	۴-۱۱-۵ Encryption algorithm selection
۸۳.....	۴-۱۲ منوی Kex
۸۴.....	۴-۱۲-۱ انتخاب الگوریتم تبادل کلید (Diffie-Hellman exchange algorithm selection)
۸۴.....	۴-۱۲-۲ تکرار تبادل کلید (Repeat key exchange)
۸۵.....	۴-۱۳ منوی Auth
۸۶.....	۴-۱۳-۱ Bypass authentication entirely فیلد
۸۷.....	۴-۱۳-۲ Attempt authentication using Pageant فیلد
۸۷.....	۴-۱۳-۳ Attempt TIS or CryptoCard authentication فیلد
۸۷.....	۴-۱۳-۴ Attempt keyboard-interactive authentication فیلد
۸۷.....	۴-۱۳-۵ Allow agent forwarding فیلد
۸۸.....	۴-۱۳-۶ Allow attempted changes of username in SSH-2
۸۸.....	۴-۱۳-۷ Private Key files for authentication

فهرست اشکال

۱۶	شکل ۱: لایه بندی در پروتکل SSL
۲۲	شکل ۲: موقعیت یک شبکه VPN در اینترنت
۴۳	شکل ۳: استفاده از port forwarding در SSH
۵۷	شکل ۴: منوی <i>Traslation</i> در بخش پیکربندی
۶۱	شکل ۵: منوی <i>Selection</i> در بخش پیکربندی نرم افزار
۶۴	شکل ۶: منوی <i>Colors</i> در بخش پیکربندی نرم افزار PuTTY
۶۷	شکل ۷: منوی <i>connection</i> در بخش پیکربندی نرم افزار PuTTY
۷۰	شکل ۸: پانل <i>data</i> در بخش <i>connection</i> پیکربندی نرم افزار PuTTY
۷۲	شکل ۹: منوی پروکسی واقع در قسمت <i>connection</i> در پیکربندی نرم افزار
۷۷	شکل ۱۰: منوی <i>Telnet</i> واقع در بخش <i>connection</i>
۷۹	شکل ۱۱: منوی <i>Rlogin</i> واقع در بخش <i>connection</i> نرم افزار
۸۰	شکل ۱۲: منوی پروتکل <i>SSH</i> واقع در بخش <i>connection</i> نرم افزار PuTTY
۸۳	شکل ۱۳: زیر منوی <i>Key</i> واقع در منوی <i>SSH</i>
۸۶	شکل ۱۴: زیر منوی <i>Auth</i> واقع در منوی <i>SSH</i>
۸۹	شکل ۱۵: زیر منوی <i>TTY</i> واقع در منوی <i>SSH</i>
۹۱	شکل ۱۶: زیر منوی <i>X11</i> واقع در منوی <i>SSH</i>
۹۳	شکل ۱۷: زیر منوی <i>Tunnels</i> واقع در منوی <i>SSH</i>
۹۹	شکل ۱۸: منوی <i>Serial</i> برای ایجاد یک ارتباط سریال به کمک PuTTY
۱۰۴	شکل ۱۹: نصب نرم افزار - مرحله ۱
۱۰۴	شکل ۲۰: نصب نرم افزار - مرحله ۲
۱۰۵	شکل ۲۱: نصب نرم افزار - مرحله ۳
۱۰۵	شکل ۲۲: نصب نرم افزار - مرحله ۴
۱۰۶	شکل ۲۳: نصب نرم افزار - مرحله ۵
۱۰۷	شکل ۲۴: نصب نرم افزار - مرحله ۵
۱۰۷	شکل ۲۵: نصب نرم افزار - مرحله ۶

- شکل ۲۶: نصب نرم افزار - مرحله ۷ ۱۰۸
- شکل ۲۷: نصب نرم افزار - مرحله ۸ ۱۰۸
- شکل ۲۸: نصب نرم افزار - مرحله ۸ ۱۰۹

www.ketab.ir