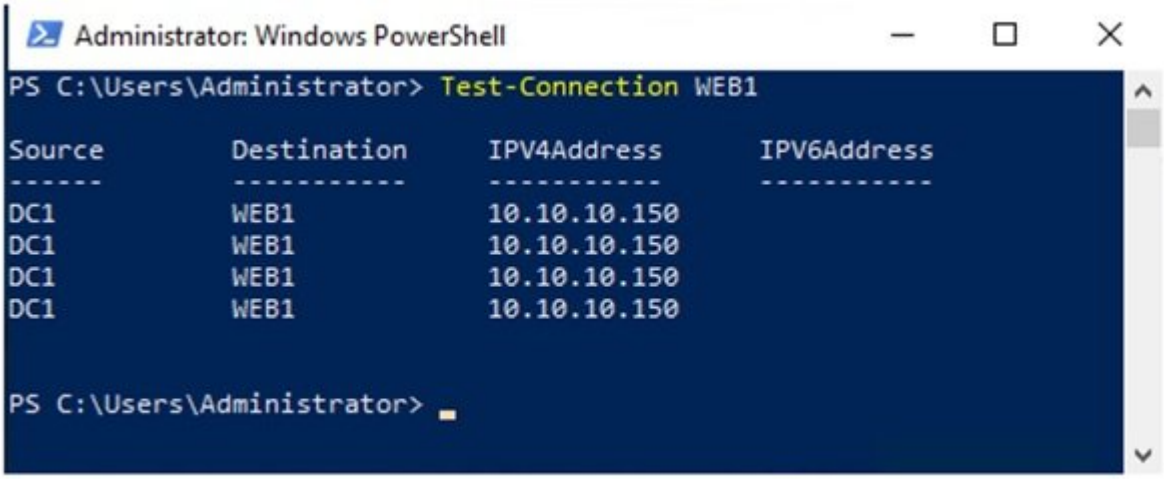
ابزارهایی که برای شناسایی مشکلات در شبکه‌های مبتنی بر ویندوز سرور 2019 در اختیار ما قرار دارند

ابزارهای نظارت بر شبکه‌های کامپیوترهای مبتنی بر ویندوز سرور 2019 به ما اجازه می‌دهند، قطعی یا اتصال در شبکه را بررسی کنیم و جزییات کاملی درباره علل بروز مشکلات پیدا کنیم.

برای مطالعه قسمت قبل آموزش رایگان ویندوز **سرور 2019** اینجا کلیک کنید.

Test-Connection

دستوراتی که تا این لحظه درباره آن‌ها صحبت کردیم را می‌توان از طریق خط فرمان یا پاورشل اجرا کرد، اکنون زمان آن رسیده که یک قدم روبه‌جلو برداریم و به سراغ دستوراتی برویم که تنها از طریق پاور شل اجرا می‌شوند. اولین ابزار Test-Connection نام دارد که نوعی پینگ است. اگر یک اعلان پاورشل را باز کنیم و فرمان Test-Connection WEB1 را اجرا کنیم خروجی شبیه به آن‌چه که با یک پینگ معمولی دریافت می‌کنیم را مشاهده می‌کنیم، اما اطلاعات به روشی ارائه می شود که چشم‌نوازتر هستند. همچنین یک ستون جدیدی از داده‌ها به‌نام Source وجود دارد.

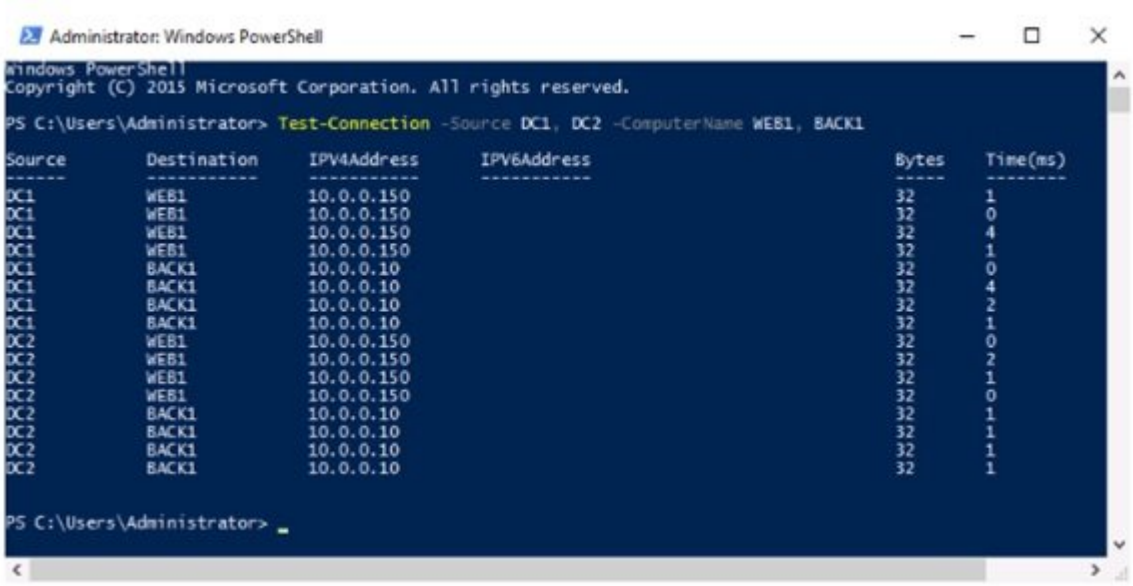


جالب است وقتی این دستور را روی کامپیوتر مبا اجرا کردیم به سرور DC1 وارد شدیم. این حرف بدان معنا است که من توانایی دستکاری کامپیوتر منبع با استفاده Test-Connection را دارم؟ پاسخ مثبت است. شبیه به سایر ابزارهای مدیریتی در ویندوز سرور 2019 ابزار فوق باید به سرور محلی وارد شود. فرمان Test-Connection اجازه می‌دهد در هر نقطه‌ای از شبکه پاورشل را باز کنید و اتصال بین دو نقطه پایانی مختلف را آزمایش کنید، حتی اگر به هیچ یک از آن‌ها وارد نشده باشید. بیایید این موضوع را آزمایش کنیم.

من هنوز در سرور DC1 قرار دارم، اما برای آزمایش اتصالات بین تعدادی از سرورهای شبکه در نظر دارم از فرمان Test-Connection استفاده کنم. مشاهده می‌کنید که نه تنها می‌توانید یک منبع متفاوتی را نسبت به کامپیوتری که در حال حاضر در آن قرار دارید، مشخص کنید، بلکه می‌توانید یک قدم روبه جلو بردارید و چند منبع و مقصد را با این ابزار قدرتمند مشخص کنید. بنابراین اگر در نظر داشته باشیم تا اتصال میان ماشین‌های مبدا مختلفی را با مقاصد مختلفی بررسی کنیم این‌کار به راحتی از طریق فرمان زیر اجرا می‌شود:

```
Test-Connection -Source DC1, DC2 -ComputerName WEB1, BACK1
```

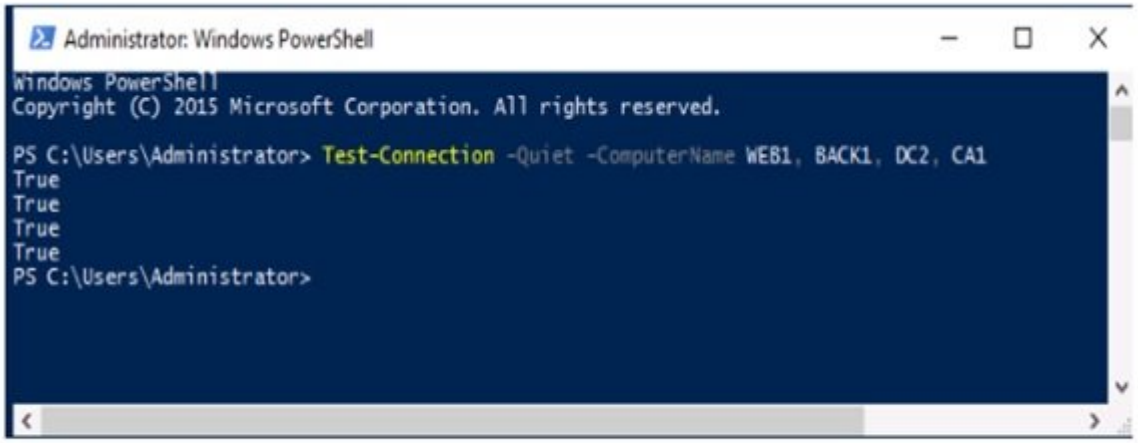
در تصویر زیر مشاهده می‌کنید که پینگی به DC1 و DC2 و به هر یک از سرورهای WEB1 و BACK1 در شبکه انجام دادیم. Test-Connection یکی از قدرتمندترین ابزارهای نظارت بر شبکه است.



زمانی که از سوئیچ -Quiet همراه با این فرمان استفاده کنید، انی توانایی را دارید تا خروجی شفافی را مشاهده کنید. با اضافه کردن سوییچ Quiet به دستور Test-Connection دو واژه True یا False که بیان‌گر یک ارتباط موفق یا ناموفق هستند را مشاهده می‌کنید و به جای آن‌که هر بسته جداگانه ICMP که ارسال شده است را نشان دهد تنها به شکل مختصر قطعی یا وصل بودن یک ارتباط را نشان می‌دهد. متأسفانه، شما نمی‌توانید دو سوییچ Source و Quiet را با یکدیگر ترکیب کنید، اما اگر روی کامپیوتر مبدا که به آن وارد شده‌اید از Test-Connection استفاده کنید شبیه به کاری که ما انجام دادیم، سوییچ Quiet عملکرد خیلی خوبی دارد. بیشتر اوقات، تمام آن‌چه ما واقعا به آن اهمیت می دهیم این است که بدانیم یک اتصال به درستی کار می‌کند یا خیر و ضرورتی ندارد تا چهار کوشش پشت سرهم را برای بررسی این موضوع انجام دهیم. از سوییچ Quiet شکل زیر استفاده می‌کنیم.

```
Test-Connection -Quiet -ComputerName WEB1, BACK1, DC2, CA1
```

اگر بخواهم از طریق Test-Connection به روش استاندارد استفاده کنیم و سعی کنمی با همه سرورهای موجود در شبکه ارتباط برقرار کنیم، خروجی‌های مختلفی خواهیم داشت. اما با استفاده از سوئیچ Quiet، تنها دو واژه True یا False برای نشان دادن وضعیت هر سرور استفاده می‌شود.



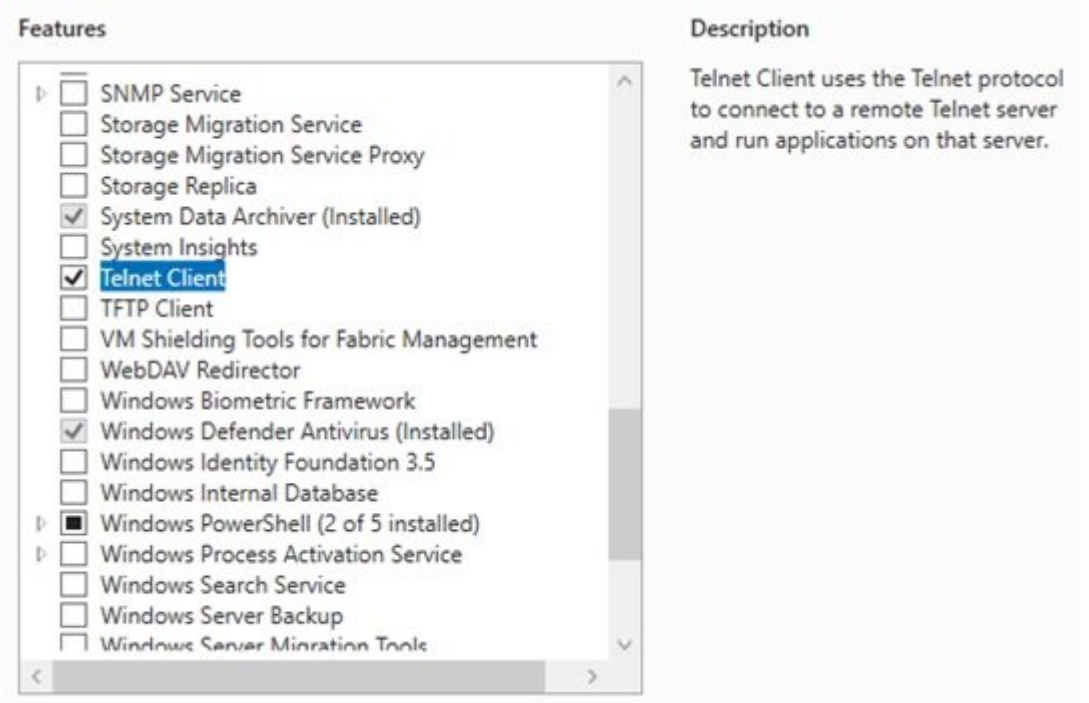
telnet

با استفاده از دستور telnet امکان برقراری ارتباط میان پورت‌ها دو سرور بررسی می‌شود. تل‌نت اجازه ایجاد ارتباط بین دو کامپیوتر به منظور دستکاری دستگاه‌ها از راه دور و از طریق یک اتصال ترمینال مجازی فراهم می‌کند. در اینجا ما در مورد عملکردهای واقعی که telnet فراهم می‌کند صحبت نمی‌کنیم، زیرا با توجه به رویکرد ما در شبکه‌سازی از تل‌نت به عنوان یک ابزار تست اتصال ساده مفید استفاده می‌کنیم.

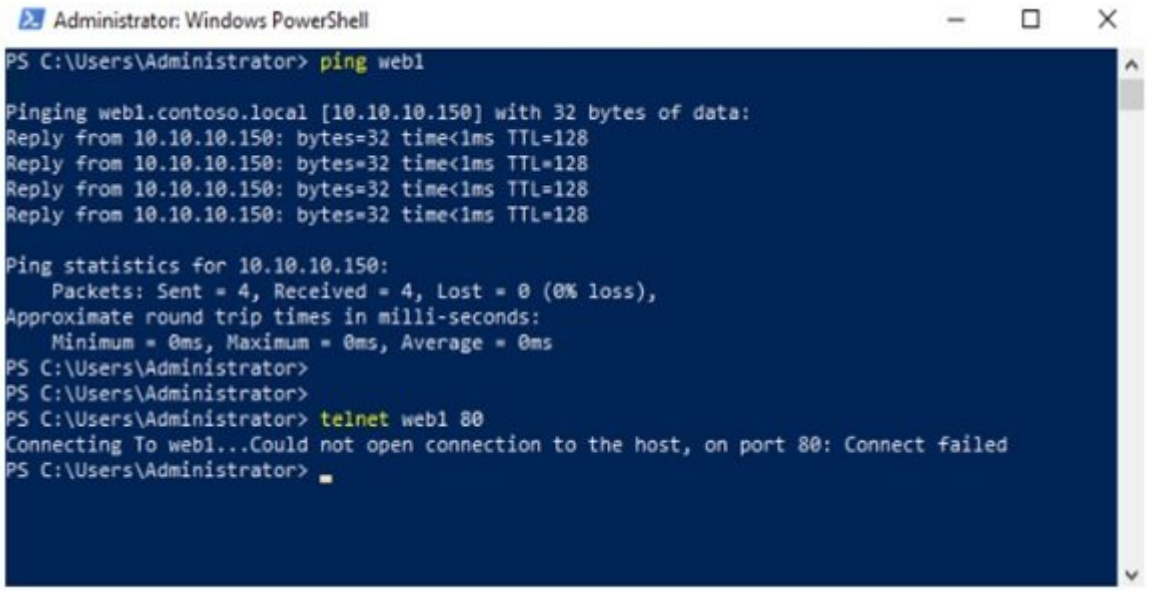
وقتی در مورد پینگ بحث می‌کنیم درباره یک روند متزلزل ICMP صحبت می‌کنیم: زیرا به راحتی مسدود می‌شود و در شبکه‌های امروزی ترجیح می‌دهند به اجازه ندهند خروجی فرمان پینگ موفقیت‌آمیز باشد. البته این موضوع خوشایند نیست، زیرا پینگ همیشه رایج‌ترین شکل آزمایش تست اتصال به شبکه شناخته می‌شود، اما واقعیت این است که اگر پینگ زندگی ما را آسان‌تر کند، زندگی هکرها را نیز آسان می‌کند. اگر نمی‌توانید به پینگ تکیه کنیم تا با اطمینان به ما بگوید که آیا می‌توانیم با یک سیستم از راه دور ارتباط برقرار کنیم، در عوض از چه فرمانی می‌توانیم استفاده کنیم؟ مورد دیگری که من اغلب مشاهده می‌کنم این است که ممکن است خود سرور به درستی پاسخ دهد، اما یک سرویس خاص که در آن سرور اجرا می‌شود ایراد داشته باشد و مانع پاسخ‌گویی درست شود. یک پینگ ساده ممکن است سرور را به صورت آنلاین نشان دهد، اما نمی‌تواند اطلاعاتی در مورد یک سرویس خاص ارائه دهد. با استفاده از دستورات Telnet Client، به راحتی می‌توانیم از راه دور پرس‌جویی روی سرور اجرا کنیم. مهم‌تر از همه، می‌توانیم درباره یک سرویس جداگانه محاوره‌ای روی سرور اجرا کنیم تا مطمئن شویم که سرویس به درستی در حال انجام کار است. اجازه دهید، با ذکر مثالی این موضوع را روشن کنیم:

بعد از نصب یک وب‌سرور جدید، این حس را پیدا می‌کنیم که می‌خواهیم از طریق اینترنت دسترسی به آن‌را آزمایش کنیم تا مطمئن شویم که سرور به درستی پاسخ می‌دهد. این یک روند معمول است، اما شاید خود وب‌سایت هنوز آنلاین و قابل استفاده نباشد، بنابراین نمی‌توانیم با اینترنت اکسپلورر آن‌را آزمایش کنیم. کاملا محتمل است که پینگ را در این سرور یا در سطح دیوارآتش غیرفعال کنیم، زیرا مسدود کردن ICMP خطر آسیب‌پذیری‌های امنیتی وب را کاهش می‌دهد. بنابراین سرور جدید من در حال اجرا است و فکر می‌کنیم که شبکه دقیق و جامعی در اختیار داریم، اما نمی‌توانم آزمایش پینگ روی سرور جدید را انجام دهم، زیرا با این مکانیزم طراحی جواب نمی‌دهد. از چه ابزاری برای آزمایش این موضوع استفاده کنیم؟ پاسخ telnet است. با ارسال یک دستور ساده telnet، می‌توانیم به کامپیوتر خود بگوییم که یک پورت خاص را در وب‌سرور وب جدید جست‌وجو کند تا بفهیم که آیا امکان اتصال هب آن درگاه وجود دارد یا خیر. با این‌کار یک اتصال سوکتی به پورت در آن سرور برقرار می‌شود که خیلی واقعی‌تر از یک فرمان پینگ عمل می‌کند، زیرا شبیه به ترافیک یک کاربر واقعی است. اگر یک فرمان telnet با موفقیت به منبع متصل شود، می‌دانید که ترافیک به سمت سرور می‌رود و به نظر می‌رسد سرویس سرور که روی آن پورت در حال اجرا است به درستی پاسخ می‌دهد.

امکان استفاده از Telnet به‌صورت پیش‌فرض در **ویندوز سرور 2019** یا هر سیستم‌عامل ویندوزی وجود ندارد و باید آن‌را نصب کنید، بنابراین برای نصب ویژگی Telnet Client ابتدا باید به Server Manager بروید و نقش‌ها و ویژگی‌ها زیر را اضافه کنید:



اکنون که ویژگی Telnet Client نصب شده، می‌توانیم از طریق خط فرمان یا پاورشل برای ایجاد اتصالات سوکتی از کامپیوتر به یک سرویس از راه دور استفاده کنیم. تنها کاری که باید انجام دهیم این است که سرور و پورتی که قرار است محاوره روی آن اجرا شود را مشخص کنیم. در ادامه telnet به‌سادگی متصل می‌شود یا خطای time out را نشان می‌دهد و بر اساس نتیجه‌ای که دریافت می‌کنیم، متوجه خواهیم شد که آن سرویس خاص روی سرور پاسخ می‌دهد یا خیر. اجازه دهید این موضوع را با سرور وب خودمان امتحان کنیم. به‌طور مثال، من وب‌سایت داخل IIS را خاموش کرده‌ام، بنابراین در موقعیتی هستیم که سرور آنلاین است اما وب‌سایت آفلاین شده است. اگر به WEB1 پینگ کنم، هنوز هم می‌توانم با خوشحالی پاسخی که ارائه می‌کند را دریافت کنم. شما می‌توانید مشاهده کنید که ابزارهای مانیتورینگ سرور که به ICMP متکی هستند دارای هشدارهای مثبت کاذب زیادی هستند که نشان می‌دهد که سرور به‌صورت آنلاین و در حال اجرا است، حتی اگر وب‌سایت ما غیرقابل دسترس باشد. درست در زیر پینگ موفق که در تصویر زیر مشاهده می‌کنید، محاوره‌ای به پورت 80 در سرور WEB1 انجام داده‌ام. دستوری که من برای آن استفاده کردم telnet web1 80 است. اما خروجی timed out است. این دستور به ما نشان می‌دهد وب‌سایتی که درگاه 80 روی آن در حال اجرا است، پاسخ نمی‌دهد:



اگر وب‌سایت را دوباره فعال کنیم و دومرتبه فرمان telnet web1 80 را آزمایش کنیم، این مرتبه پیغام خطای timeout را مشاهده نمی‌کنیم. این بار، پاورشل کرسر را در وضعیت آماده به دریافت قرار می‌دهد که نشان می‌دهد یک اتصال سوکتی موفق به پورت 80 روی وب‌سرور ایجاد شده و این نشان می‌دهد که وب‌سایت آنلاین است و پاسخ می دهد.

Test-NetConnection

اگر پینگ یک معادل قدرتمند و بهبود یافته به‌نام Test-Connection در پاورشل دارد، آیا پاورشل یک ابزار پیشرفته که عملکردش شبیه به تل‌نت باشد و برای آزمایش اتصالات سوکتی به منابع کار کند در اختیار ندارد؟ بدون تردید پاورشل چنین فرمانی را دارد. Test-NetConnection روش دیگری برای پیاده‌سازی محاوره‌ها روی درگاه‌ها یا سرویس‌های خاص در یک سیستم از راه دور است و خروجی نمایش داده شده نسبت به Telnet کاربرپسندتر است.

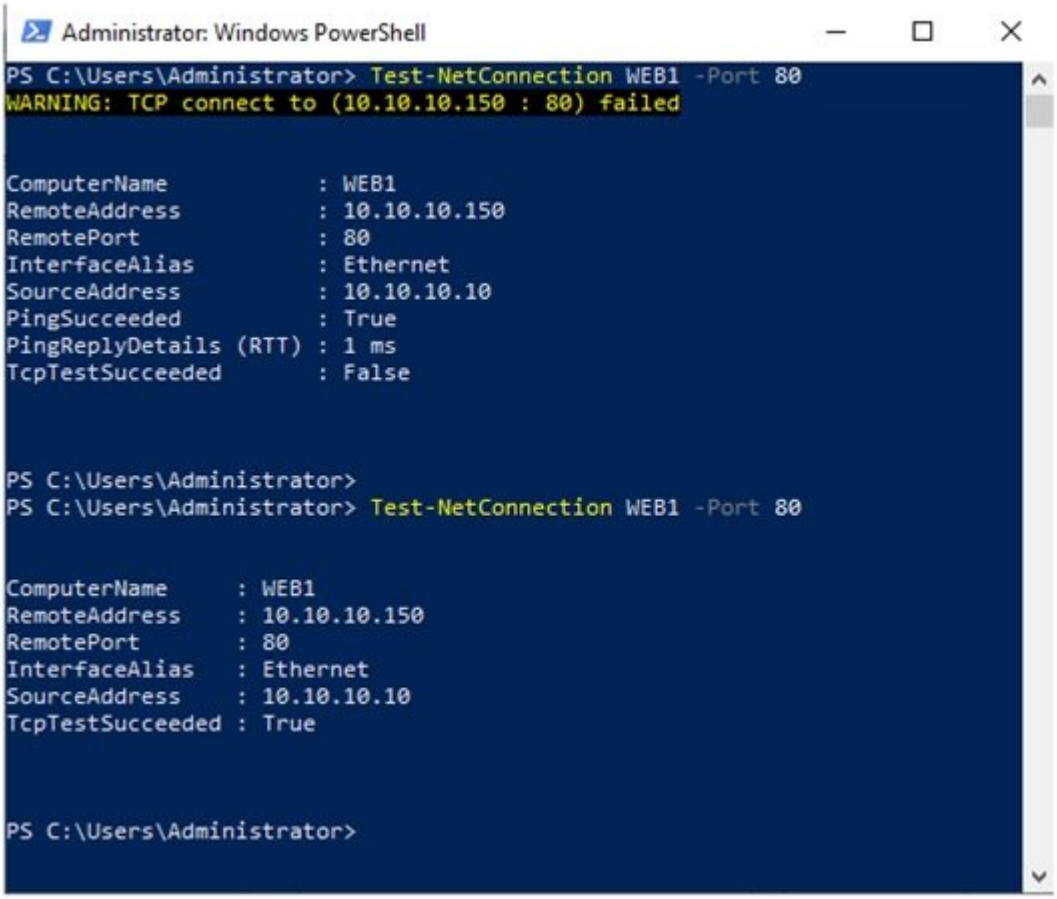
بیایید این موضوع را آزمایش کنیم و بار دیگر محاوره‌ای روی پورت 80 در WEB1 پیاده‌سازی کنیم.. در تصویر زیر مشاهده می‌کنید که من دو بار دستور را اجرا کرده‌ام. اولین بار وب‌سایت در WEB1 غیرفعال شد و اتصال من به درگاه 80 با موفقیت همراه نبود. بار دوم، وب‌سایت را دوباره فعال کردم و اکنون ارتباط موفقی دریافت کردم.

```
Test-NetConnection WEB1 -Port 80
```

مسیریابی بسته‌ها با Wireshark یا Message Analyzer

در نهایت، شاید لازم باشد که برخی اوقات به شکل عمیق‌تری به بسته‌های شبکه خود نگاه کنید. به‌کارگیری ابزارهای خط فرمان برای بررسی وضعیت سرورها و سرویس‌های بسیار مفید است، اما گاهی اوقات ممکن است کافی نباشد. به‌عنوان مثال، شما یک برنامه کلاینت دارید که به سرور برنامه وصل نمی‌شود، اما نمی دانید چرا این اتفاق رخ می‌دهد. برنامه‌های کاربردی مانند پینگ و حتی telnet ممکن است بتوانند با موفقیت به هم وصل شوند و نشان دهند که مسیریابی شبکه به درستی تنظیم شده است، اما برنامه‌ها قادر به برقراری اتصال نیستند. اگر گزارش‌های مربوط به رویداد برنامه به شما کمک نمی‌کند تا آن‌چه را که اتفاق می‌افتد، عیب‌یابی کنید، ممکن است بخواهید نگاهی عمیق‌تر به درون بسته‌های شبکه بیندازید که برنامه در تلاش است تا به سمت سرور ارسال کند.

Wireshark و Message Analyzer ابزارهای رایگان و در دسترسی که اساسا عملکردهای یکسانی دارند. آن‌ها به گونه‌ای طراحی شده‌اند که ترافیک وارد و خارج شونده به/از شبکه و اطلاعاتی که درون بسته‌ها وجود دارد را ضبط کنند تا بتوانید نگاهی عمیق‌تر به آن‌چه اتفاق می‌افتد داشته باشید. به‌طور مثال، برنامه ما قادر به برقراری اتصال نیست، شما م توانید یکی از این ابزارها را روی کامپیوتر کلاینت اجرا کنید تا ترافیک خروجی را مشاهده کنید. همچنین در برنامه در حال اجرا روی سرور ترافیک ورودی از کلاینت را مشاهده کنید.



هر ابزاری ویژگی‌های خاص خود را دارد و این امکان وجود ندارد تا جزییات هر ابزار را نشان دهیم. برای اطلاعات بیشتر به آدرس‌های زیر مراجعه کنید.

Wireshark: https://www.wireshark.org/download.html

Microsoft Message Analyzer: https://www.microsoft.com/en-us/download/details.aspx?id=44226

در شماره آینده آموزش رایگان ویندوز سرور 2019 مبحث فوق را ادامه خواهیم رفت.

برای مطالعه تمام بخش‌های آموزش ویندوز سرور 2019 روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
06 مهر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16055/%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D9%85%D8%B4%DA%A9%D9%84%D8%A7%D8%AA-%D8%AF%D8%B1-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%A8%D8%AA%D9%86%DB%8C-%D8%A8%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019