

برنامه نویسی:

سوال ۱: چرا این روند برعکس نیست. یعنی کلاینت یک پورت را باز نمی کند و آن را به سرور اطلاع دهد و سرور فایل را روی آن پورت برای کلاینت ارسال کند؟

پاسخ ۱: اگر روند برعکس باشد ممکن است چند کلاینت به طور همزمان به یک پورت درخواست بدهند که در اینصورت نمی توان به هر دو کلاینت سرویس داد.

اسکرین شات از خروجی های سرور:

```
Run: server client
C:\Users\Alireza\AppData\Local\Microsoft\WindowsApps\python3.9.exe C:/Users/Alireza/Desktop/Programming/My-FTP/server/server.py
Welcome to the FTP server

To get started, connect to a client
Server listening on 0.0.0.0: 2121

client "127.0.0.1" connected to port: 2121
Recieved instruction: HELP
Help ...
Help is sent

Recieved instruction: LIST
Listing files ...

file listing sent successfully

Recieved instruction: CD dir1
CD ...
Current Directory is set to "C:\Users\Alireza\Desktop\Programming\My-FTP\server\files\dir1"
New directory sent to client

Recieved instruction: DWLD bigFile.bin
Sending file...
File sent successfully
```

```
Recieved instruction: PWD
pwd ...
Current directory sent
```

اسکرین شات از خروجی های کلاینت:

```
Run: server x client x
C:\Users\Alireza\AppData\Local\Microsoft\WindowsApps\python3.9.exe C:/Users/Alireza/Desktop/Programming/My-FTP/client.py
Sending server request
Connected successfully

Welcome to the FTP client

Enter one of the following commands:

# HELP:          Show this help
# LIST:          List files
# DWLD "file_path": Download file
# PWD:          Show current dir
# CD "dir_name":  Change directory
# QUIT:          Exit

Enter Command: HELP
Getting help...
Enter one of the following commands:

# HELP:          Show this help
# LIST:          List files
# DWLD "file_path": Download file
# PWD:          Show current dir

# PWD:          Show current dir
# CD "dir_name": Change directory
# QUIT:          Exit

Enter Command: LIST
Requesting files...
> dir1 (13938842 B)
  hi.txt (0 B)

Total directory size: 13938842 Bytes

Enter Command: CD dir1
Changing dir to: dir1
Directory changed

Enter Command: DWLD bigFile.bin
File downloaded successfully
Enter Command: PWD
Requesting path...
\dir1\
Enter Command: |
```

سوال ۲: ورودی هایی برای دستورات CD و DWLD که باعث شود فایلی دانلود شود یا فولدري باز شود که در زیرشاخه اصلی سرور قرار ندارد.(مثل فایل های سیستم عامل) این حمله چه نام دارد؟

پاسخ ۲: این حمله، Directory Traversal Attacks نام دارد.

Properly controlling access to web content is crucial for running a secure web server. Directory traversal or Path Traversal is an HTTP

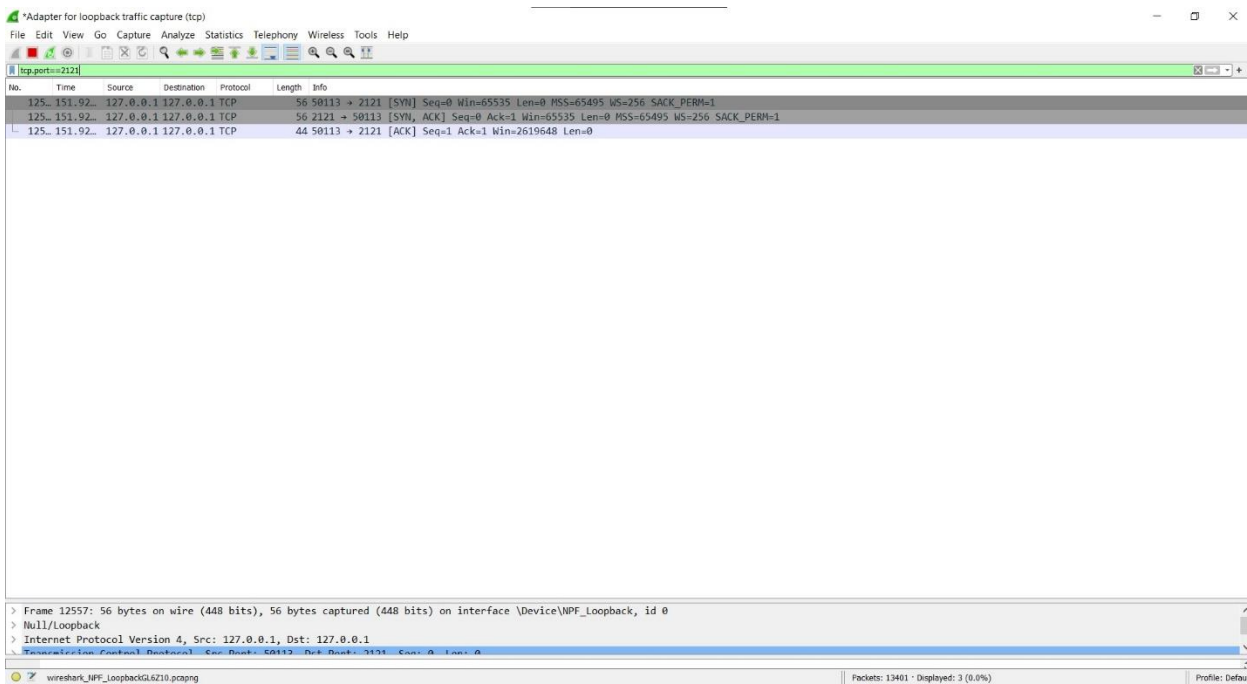
attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.

منبع: <https://www.acunetix.com/websitesecurity/directory-traversal/>

آشنایی و کار با Wireshark:

سوال ۱: وایرشارک را باز کرده و capture کردن بسته های loopback را آغاز کنید. سپس ابتدا سرور و سپس کلاینت را اجرا کنید. به وای شارک برگردید و از سه بسته ای که برای handshaking پروتکل TCP ارسال شده اسکرین شات بگیرید (برای این کار که فقط بسته های TCP را ببینید می توانید کلمه tcp را در نوار فیلتر وارد کنید). (۱۰ نمره)

پاسخ ۱:



سوال ۲: آیا TCP محدودیتی برای ارسال فایل ها دارد؟ فایل های بزرگ چگونه توسط

سوکت TCP ارسال می شوند؟

پاسخ ۲ آ: ماکزیمم طول پکت، ماکزیمم طول بسته های tcp هست. پس محدودیت طول

بسته دارد.

سوکت tcp مسئول این هست که اگر دیتایی با طول بیشتر بهش دادید خودش به پکت

های کوچک تر تقسیم و ارسال کند. در سمت گیرنده به صورت قطعه قطعه و به اندازه ی بافر

داده شده مثلا ۱۰۲۴ دریافت می شود تا کل فایل دریافت شود.

سوال ۲ ب: برای مشاهده عملی جواب قسمت قبل، ابتدا وایرشارک را روشن کنید و سپس

در کلاینت درخواست دانلود فایل bigFile.txt را بدهید. از نتایج وایرشارک اسکرین شات بگیرید.

TCP برای دانلود این فایل چند بسته فرستاده است؟ (۱۰ نمره)

پاسخ ۲ ب:

No.	Time	Source	Destination	Protocol	Length	Info
506.	640.84...	127.0.0.1	127.0.0.1	TCP	56	51977 → 31276 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 NS=256 SACK_PERM=1
506.	640.84...	127.0.0.1	127.0.0.1	TCP	56	31276 → 51977 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 NS=256 SACK_PERM=1
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	51977 → 31276 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=1 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=65496 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=138991 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=196480 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=261981 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=327476 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=392971 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=458466 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=523961 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=589456 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	51977 → 31276 [ACK] Seq=1 Ack=654951 Win=2095616 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=654951 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=728446 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=785941 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=851436 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	[TCP Window Update] 51977 → 31276 [ACK] Seq=1 Ack=654951 Win=2161152 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=916931 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	65539	31276 → 51977 [ACK] Seq=982426 Ack=1 Win=2619648 Len=65495
506.	640.84...	127.0.0.1	127.0.0.1	TCP	700	31276 → 51977 [PSH, ACK] Seq=1047921 Ack=1 Win=2619648 Len=656
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	51977 → 31276 [ACK] Seq=1 Ack=1048577 Win=1767680 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	31276 → 51977 [FIN, ACK] Seq=1048578 Ack=1 Win=2619648 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	51977 → 31276 [ACK] Seq=1 Ack=1048578 Win=1767680 Len=0
506.	640.84...	127.0.0.1	127.0.0.1	TCP	44	[TCP Window Update] 51977 → 31276 [ACK] Seq=1 Ack=1048578 Win=2225920 Len=0
506.	640.88...	127.0.0.1	127.0.0.1	TCP	44	[TCP Window Update] 51977 → 31276 [ACK] Seq=1 Ack=1048578 Win=2619648 Len=0
507.	641.07...	127.0.0.1	127.0.0.1	TCP	44	51977 → 31276 [FIN, ACK] Seq=1 Ack=1048578 Win=2619648 Len=0
507.	641.07...	127.0.0.1	127.0.0.1	TCP	44	31276 → 51977 [ACK] Seq=1048578 Ack=2 Win=2619648 Len=0

۱۷ بسته برای دانلود فرستاده است.(بسته های با طول ۶۵۵۳۹(به جز مورد آخر که ۷۰۰

است) که از پورت تصادفی ۳۱۲۷۶ تولید شده توسط برنامه به ۵۱۹۷۷ می روند)