Polecenia i Materiały

By otworzyć linię poleceń w systemie Windows, można: poszukać jej w Akcesoriach, bądz wybrać Menu Start, Uruchom i wpisać `cmd`.

Większość poleceń należy wykonać na maszynie `info3.meil.pw.edu.pl`, lecz niektóre można wykonać w lini poleceń Windows.

Materiały do tego laboratiorium można znaleść w katalogu `/home/zasoby/Info3/smsni` na serwerze `info3.meil.pw.edu.pl`. Całą zawartość katalogu można przegrać np. na pulpit za pomocą WinSCP, a na koniec zajęć skasować.

Serwery i porty

Standard TCP/IP mówi jak na na podstawowym poziomie działa Internet. W internecie są podłączone komputery i każdy z nich ma swój unikatowy numer IP. Ten numer to 4 bajty - zazwyczaj zapisuje się go w postaci 4 liczb oddzielonych kropkami (np. 127.0.0.1). Bajt to 8 bitów, wiec można w nim zapisać liczby od 0 do $2^8 - 1 = 255$. Tak więc wszystkich numerów IP jest 2^{32} więc ponad 4 miliardy. Jednak w internecie numery sa przydzielane grupami, wiec szybko się wyczerpały. W związku z tym wprowadzono nowy standard IPv6. Nie należy jednak sądzić że to 6 oznacza że teraz jest 6 liczb. Jest to poprostu wersja 6ta standardu - i numerów jest teraz 2^{128}, co daje prawie jeden septylion. Są pewne grupy numerów które są wyjątkowe.:

- 127.0.0.1 (localhost) – numer IP komputera na którym jesteśmy zalogowani – widoczny tylko z tego komputera
- 192.168.?.? – numery IP komputerów w sieci lokalnej – widoczne tylko wewnątrz tej sieci
- 192.168.0.1 – zwyczajowy adres bramy sieci (np routera w twoim domu) – widoczny tylko w tej sieci.

Standardową metodą komunikacji jest łączenie się jednego komputera z portem drugiego komputera. Każdy komputer ma wiele portów — tak by jeden komputer mógł obsługiwać wiele różnych funkcji. Komputer który łączy się nazywamy klientem, zaś komputer do którego się łączymy serwerem. Rozmawiają one przy pomocy zestawu ustalonych komend, które nazywamy protokołem. Żeby nie pomylić protokołów, przypisano im unikatowe porty. To oznacza, że dany port jest zwyczajowo używany do danego protokołu — ale fizycznie można by do tego użyć dowolnego innego.

Ćwiczenia

- Spróbuj dowiedzieć się jaki numer IP mają różne komputery używając np. komendy `ping google.com`
- Spróbuj to samo z nazwami `localhost` i `orange.meil.pw.edu.pl`
- Spróbuj dowiedzieć się coś wiecej o wybranej domenie `whois google.com` albo `whois onet.pl`

Telnet

Port: 23

Jednym z bardzo użytecznych programów jest `telnet`. Gdy uruchomimy `telnet google.com` program spróbuje połączyć się z komputerem google.com, na porcie 23. Gdyby udało mu sie połączyć, moglibyśmy z klawiatury wysyłać teksty do serwera, a na ekranie wyswietlała by się odpowiedz. Telnet służył do obsługi konsoli — tak jak SSH (putty) którego używasz. Jednak telnet nie był niczym zabezpieczony (nawet hasło było widoczne), dlatego nie jest teraz nigdzie używany. Jednak `telnet` jest użyteczny ponieważ możemy mu wskazać port na który ma się połączyć — i w ten sposób "oszukać" program i połączyć się z innym protokołem.

Ćwiczenia

W następnych ćwiczenia połączymy się na różnych portach z różnymi komputerami pisząc:

- `telnet info3.meil.pw.edu.pl`
- `telnet info3.meil.pw.edu.pl 22`
- `telnet localhost`
- `telnet google.com`
- `telnet google.com 80`

Hypertext Transfer Protocol (HTTP)

Port:80 **SSL**:443

HTTP to najczęściej używany protokół w internecie. Pozwala on na pobieranie stron z serwerów. W odróżnieniu od poprzednich, nie jest to protokół typu

instrukcja-odpowiedz. W tym protokole, wysyłamy zapytanie, zaś serwer wysyła nam odpowiedz i zamyka połączenie. Zapytanie wygląda następująco:

```
GET [ścieżka] HTTP/1.0
Host: [nazwa serwera]
[inna opcja]: [wartosc]
[pusta linia]
```

Po `GET` naprawdę nie trzeba pisać nic — lecz jeden serwer może obsługiwać strony gazeta.pl, tv.gazeta.pl i wiadomosci.gazeta.pl, gdybyśmy nie podali `Host:` serwer nie wiedziałby o którą stronę chodzi. Dla przykładu jeśli chcemy sciągnać stronę `http://m.google.com/index.html` wpiszemy:

```
GET /index.html HTTP/1.0
Host: m.google.com
```

Inne opcje to :

- `User-Agent:` – twoja przeglądarka
- `Accept:` – Jakie formaty umiesz przeczytać (html, txt) - można nadać im priorytety.
- `Accept-Language` – Jakie języki akceptujemy – też można nadać priorytety.

Ćwiczenia

- Spróbuj ściągnąć główną stronę “m.google.com”
- Spróbuj ściągnąć główną stronę “www.onet.pl”
- Spróbuj ściągnąć główną stronę do pliku
- Wyszukaj w tym pliku adresu jakiegoś obrazka i go ściągnij
- Napisz skrypt do ściągania plików z serwera HTTP. Z dwoma argumentami: nazwa serwera i ścieżka

HTTP over Secure Socket Layer (HTTPS)

Port:80 **SSL**:443

Do wielu usług warto łączyć się kanałem szyfrowanym. Po pierwszym użyciu w tym celu programu `telnet`, np łączac się z `telnet google.com 443`, widzimy że nie umiemy rozmawiać zaszyfrowanymi bajtami.

Do komunikacji z serwerem po szyfrowanym połączeniu możemy użyć program `openssl`. Dla przykładu:

```
openssl s_client -connect google.com:443
```

Ćwiczenia

- Spróbuj ściągnąć główną stronę “m.google.com” po protokole szyfrowanym
- Spróbuj dodać komentarz w serwisie `github.com` do dyskusji https://github.com/ccfd Użyj do tego zapytania do serwera `api.github.com` (skonstruuj je uprzednio w pliku tekstowym):

```
POST /repos/ccfd/courses/issues/12/comments HTTP/1.1
Host: api.github.com
Authorization: token [token]
User-Agent: Wget/1.9.1
Connection: close
Content-Type: application/json
Content-Length: 53

{"body":"To jest bardzo wazny komentarz\nBardzo\n"}
```

`[token]` możesz uzyskać logując się na GitHub i dodając token w menu “Settings”, “Personal access tokens”.

Simple Mail Transfer Protocol (SMTP)

Port:25 **TLS**:587 **SSL**:465

SMTP to protokół używany do wysyłania e-maili. Połączyć się z nim można pod portem nr 25. Jego postawowe instrukcje to:

- `HELO something` – przywitanie się z serwerem
- `MAIL From: something` – Od kogo jest e-mail
- `RCPT To: something` – Do kogo jest e-mail
- `DATA` – Po tej komendzie można napisać treść e-maila. Zakończyć trzeba [enter].[enter]
- `QUIT` – Kończy rozmowę z serwerem

Z szyfrowanym protokołem SMTP (typu TLS), można się połączyć za pomocą:

```
openssl s_client -connect [serwer]:25 -starttls smtp
```

Ćwiczenia

- Spróbuj wysłać ze swojego konta e-mail do kolegi obok
- Wyślij e-mail do na swoje prywatne konto i w domu obejrzyj jego nagłówek (poszukaj go w spam'ie).
- Spróbuj wysłać e-mail z konta "admin na swoje konto
- Napisz plik wejściowy, który po przekierowaniu do polecenia 'telnet' wyśle e-mail do kolegi
- Napisz skrypt z jednym argumentem który wyśle zawartość wybranego pliku do kolegi

Post Office Protocol version 3 (POP3)

Port:110 **SSL**:995

POP3 to protokół używany do odbierania e-maili ze skrzynki. Połączyć się z nim można pod portem nr 110. Jego podstawowe instrukcje to:

- `USER użytkownik` – ustawia użytkownika którego chcemy zalogować
- `PASS hasło` – loguje użytkownika
- `LIST` – Wypisuje listę e-maili w skrzynce w formacie [numer] [rozmiar]
- `RETR number` – pobiera e-mail
- `DELE number` – kasuje e-mail
- `TOP number` – pobiera pierwsze pare linii e-mail
- `QUIT` – Kończy rozmowę z serwerem

Do połączenia szyfrowanego użyj analogicznego polecenia jak w sekcji o HTTPS

Ćwiczenia

- Spróbuj odebrać swoje e-maile
- Spróbuj odebrać czyjeś e-maile
- Napisz plik wejściowy, który po przekierowaniu do polecenia `telnet` pobierze konkretnego e-maila. Jeśli telnet nie reaguje na wejściowy plik, jest to spowodowane tym, ze serwer nie nadąża z interpretowaniem komend. Napisz skrypt który co sekundę będzie wypisywał na ekran jedną linijkę z pliku - a następnie przekieruj z niego wyjście do telnet'u.
- Napisz skrypt z jednym argumentem, który odbierze e-mail o danym numerze.

Sniffing

Sniffing, czyli analiza pakietów (Packet Analysis) to najprostsza technika podsłuchu w internecie. Polega ona na przechwytywaniu pakietów na poziomie interface'u sieciowego i rozkodowywaniu ich do postaci czytelnej dla człowieka. W ten sposób możemy zobaczyć wszelkie połączenia TCP/IP (a także UDP). Analizując dane przesyłane pomiędzy klientami a serwerami, możemy nie tylko dowiedzieć się kto z kim się łączy ale:

- Zobaczyć adresy internetowe na które wchodzą użytkownicy
- Zobaczyć e-maile przesyłane przy pomocy SMTP i odbierane przez POP3, a nawet podejrzeć hasła
- Zobaczyć wpisywane hasła w kiepsko zabezpieczonych stronach HTTP
- Podsłuchiwać programy IM, takie jak: MSN, GG (szyfrowanie jest domyślnie wyłączone), stare wersje ICQ i IRC.

W materiałach można znaleść program `smsniff.exe`. Jest to typowy prosty sniffer pod Windows. Sieć w laboratorium jest oparta na dobrym switch'u, więc jedyne pakiety widoczne w sieci, to takie które idą od lub do danego komputera (oraz broadcast). Oznacza to, że nie da się podsłuchiwać innych studentów.

UWAGA: *Większość sieci (w tym praktycznie wszystkie WiFi) nie są zabezpieczone przed Sniffingiem! Pamiętaj, że to co właśnie robisz, może zrobić każdy!*

Ćwiczenia

- Podsłuchaj swoje połączenie przez SSH z orange'm (port 22)
- Podsłuchując wejdź w przeglądarce na http://meil.pw.edu.pl/
- Podsłuchując wejdź w przeglądarce na https://meil.pw.edu.pl/

Dla dociekliwych: Przekierowanie portu

Ta część jest dla osób które chcą się pobawić i pogrzebać - nie ma gwarancji że cokolwiek zadziała!

Porty można przekierować. Jeśli przekierujemy port x z serwera X do portu y serwera Y, to będzie to oznaczać, że jeśli połączymy się z portem x z serwerem X, to on przekaże całą komunikację do portu y serwera Y. Innymi słowy jeśli napiszemy:

```
telnet X x
```

to połączymy się z portem y na Y. Jest to wyjątkowo przydatne, jeśli my nie potrafimy połączyć się z komputerem Y. Dla przykłady gdy Y jest za firewall'em, albo jest w innej podsieci.

Ćwiczenia

- Uruchom putty. Wejdz w ustawienia „tunneling". Tam ustaw by port `80` był przekierowany na `google.com:80`. Następnie połącz się z maszyną `info3` jak zwykle.
- Spróbuj w przeglądarce otworzyć adres `http://localhost/`
- Zobacz co działa a co nie. Jeśli nie działa, to dlaczego?

Ćwiczenia SOCKS Proxy

- Uruchom putty. Wejdz w ustawienia "tunneling". Tam ustaw by port `12345` był przekierowaniem typu "Dynamic". Następnie połącz się z maszyną `info3` jak zwykle.
- Ustaw następnie w opcjach przeglądarki serwer SOCKS proxy na `localhost` i port `12345`
- wejdz na google.com
- *ciesz się internetem zza firewall'a*