

Problemy zabezpieczeń transmisji pakietów TCP/IP w sieciach komputerowych

1. Cel pracy.

Jako podstawowe założenie określiłem zapoznanie się z narzędziem „Microsoft Network Monitor” i za jego pomocą przechwycenie oraz przeanalizowanie pakietów danych wysyłanych/odbieranych przez hosta. Analiza pakietów przeprowadzona została w oparciu o standardowe usługi: WWW, FTP i inne.

2. Konfiguracja TCP/IP komputera.

Przez to pojęcie rozumiemy określenie wszystkich niezbędnych parametrów do prawidłowego działania sieci i wzajemnego komunikowania się komputerów. W sieci lokalnej z serwera DHCP parametry te zostają przydzielone automatycznie w zależności od aktualnie dostępnych zasobów sieciowych. Podgląd tych ustawień umożliwia nam komenda „ipconfig /all” wywołana z wiersza poleceń:

```
G:\>ipconfig /all

Windows 2000 - konfiguracja IP

Nazwa hosta . . . . . : komphigh
Sufiks podstawowej domeny DNS:
Typ węzła . . . . . : Hybrydowa
Routing IP włączony . . . . . : Nie
Serwer proxy WINS włączony. . . . . : Nie
Lista przeszukiwania sufiksów DNS : wel.tuniv.szczecin.pl tuniv.szczecin
.pl

Karta Ethernet Połączenie lokalne:

Sufiks DNS konkretnego połączenia:wel.tuniv.szczecin.pl tuniv.szczecin.p
l
Opis . . . . . : D-Link DFE-530TX PCI Fast Ethernet Adapter
<Rev A>
Adres fizyczny. . . . . : 00-50-B0-6F-57-5D
DHCP włączone . . . . . : Tak
Autokonfiguracja włączona . . . . . : Tak
Adres IP. . . . . : 213.155.162.182
Maska podsieci. . . . . : 255.255.254.0
Brana domyślna. . . . . : 213.155.162.1
Serwer DHCP . . . . . : 212.14.28.44
Serwery DNS . . . . . : 212.14.28.44
                          212.14.18.2
Podstawowy serwer WINS. . . . . : 212.14.28.34
NetBIOS przez TCP/IP: wyłączony.
Dzierżawa uzyskana. . . . . : 6 czerwca 2005 12:10:41
Dzierżawa wygasa . . . . . : 6 czerwca 2005 18:10:41

G:\>_
```

Powyższy obraz przedstawia parametry:

- adres sprzętowy (fizyczny) MAC - adres sprzętowy karty sieciowej, niezbędny do komunikacji sprzętowej w sieci
- adres IP hosta

- maskę podsieci - dzielącą sieć lokalną na podsieci, które ułatwiają przepływ informacji
- adres IP routera (bramy domyślnej)
- adresy serwera DHCP i DNS
- parametry dzierżawy adresu

Okresowe przeglądanie przydzielonych parametrów sieciowych może ustrzec użytkownika przed wymuszonym przydzieleniem ustawień przez pasożytniczy, nieautoryzowany serwer DHCP istniejący w sieci.

3. ARP i DNS

Nawiązanie połączenia nie byłoby możliwe, gdyby nie konwersja adresów: DNS-owego na adres IP oraz IP na adres sprzętowy MAC karty sieciowej. Odbywa się to w dwóch stadiach. Najpierw host wysyła do serwera DNS żądanie zdekodowania nazwy domeny na adres IP, a następnie w komputerze następuje proces ARP, polegający na rozwinięciu adresu IP na sprzętowy MAC karty sieciowej.

Elementarne połączenie sieciowe odbywa się pomiędzy dwiema kartami sieciowymi. W sieci rozległej obowiązuje jednak adres IP. Konieczne jest więc rozwiązanie tego adresu na adres MAC. Realizowane jest to przez protokół ARP warstwy internetowej (sieciowej modelu OSI). Ostatnio rozwiązane adresy IP i odpowiadające im adresy MAC zapisywane są następnie w pamięci podręcznej ARP naszego komputera. Komendą „arp -a(-d)” wywołaną z wiersza poleceń, możemy przeglądać i resetować tę pamięć.

```
G:\>arp -a
Interfejs: 213.155.162.182 on Interface 0x1000003
Adres internetowy      Adres Fizyczny      Typ
213.155.162.1         00-e0-b1-25-00-1f   dynamiczne
G:\>arp -d
G:\>arp -a
Nie znaleziono wpisów ARP
```

W momencie, kiedy posługujemy się nazwami domen internetowych (łatwiejszymi do przyswojenia przez użytkownika niż adresy IP) istnieje konieczność ich rozwiązania. Proces ten odbywa się w oparciu o istniejące w sieci serwery DNS oferujące usługę rozwiązywania nazw. Proces odbywa się w dwóch etapach. W pierwszym, host wysyła w sieć zapytanie odnośnie określonego adresu...

Ranka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
6	7.981476	LOCAL	PACKET25...	HTTP	POST Request (from client using port 1477)

.

.

Ramka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
1	1.371972	LOCAL	PACKET25...	DNS	0x3A:Std Qry for www.wp.pl. of type Host Ad...
2	1.371972	PACKET25...	LOCAL	DNS	0x3A:Std Qry Resp. Auth. NS is www.wp.pl. o...

```

+IP: ID = 0x42E6; Proto = UDP; Len: 55
+UDP: Src Port: Unknown, (1487); Dst Port: DNS (53); Length = 35 (0x23)
=DNS: 0x3A:Std Qry for www.wp.pl. of type Host Addr on class INET addr.
  DNS: Query Identifier = 58 (0x3A)
+DNS: DNS Flags = Query, OpCode - Std Qry, RD Bits Set, RCode - No error
  DNS: Question Entry Count = 1 (0x1)
  DNS: Answer Entry Count = 0 (0x0)
  DNS: Name Server Count = 0 (0x0)
  DNS: Additional Records Count = 0 (0x0)
+DNS: Question Section: www.wp.pl. of type Host Addr on class INET addr.

```

..., a w drugim, w odpowiedzi, otrzymuje z serwera DNS informację o IP odpowiadającym wybranej domenie...

Ramka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
1	1.371972	LOCAL	PACKET25...	DNS	0x3A:Std Qry for www.wp.pl. of type Host Ad...
2	1.371972	PACKET25...	LOCAL	DNS	0x3A:Std Qry Resp. Auth. NS is www.wp.pl. o...

```

+Frame: Base frame properties
+ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+IP: ID = 0x0; Proto = UDP; Len: 134
+UDP: Src Port: DNS, (53); Dst Port: Unknown (2188); Length = 114 (0x72)
=DNS: 0x74:Std Qry Resp. Auth. NS is www.wp.pl. of type Host Addr on class INET addr.
  DNS: Query Identifier = 116 (0x74)
+DNS: DNS Flags = Response, OpCode - Std Qry, RD RA Bits Set, RCode - No error
  DNS: Question Entry Count = 1 (0x1)
  DNS: Answer Entry Count = 1 (0x1)
  DNS: Name Server Count = 3 (0x3)
  DNS: Additional Records Count = 0 (0x0)
+DNS: Question Section: www.wp.pl. of type Host Addr on class INET addr.
=DNS: Answer section: www.wp.pl. of type Host Addr on class INET addr.
  DNS: Resource Name: www.wp.pl.
  DNS: Resource Type = Host Address
  DNS: Resource Class = Internet address class
  DNS: Time To Live = 521 (0x209)
  DNS: Resource Data Length = 4 (0x4)
  DNS: IP address = 212.77.100.101
+DNS: Authority Section: wp.pl. of type Auth. NS on class INET addr. (3 records present)

```

W rozwinięciu tej ramki znajduje się adres IP (widoczny powyżej) odpowiadający wywołanej przez użytkownika domenie. Widać także, że korzystamy z protokołu IP warstwy internetowej i z szybkiego protokołu UDP, warstwy transportowej modelu OSI.

4. Komenda PING.

Jednym z poleceń testujących sieć pod względem skuteczności transmisji danych jest PING. Komenda ta działa w oparciu o protokół testowy ICMP warstwy internetowej (sieciowej, modelu OSI). Działanie tej procedury testowej polega na czterokrotnym wysłaniu 32-bajtowego pakietu danych adresowanego do konkretnego odbiorcy posiadającego żądany adres IP i odbiorze odpowiedzi (nazywanej popularnie „PONG”, symbolizującego odbijanie piłeczki, czyli odpowiedź).

Procedurę PING uruchamiamy wpisując „ping <adres IP> (<nazwa domeny>)” w wierszu poleceń.

```
G:\>ping www.ps.pl

Badanie locutus.tuniv.szczecin.pl [212.14.28.45] z użyciem 32 bajtów danych:
Odpowiedź z 212.14.28.45: bajtów=32 czas=10ms TTL=254
Odpowiedź z 212.14.28.45: bajtów=32 czas<10ms TTL=254
Odpowiedź z 212.14.28.45: bajtów=32 czas<10ms TTL=254
Odpowiedź z 212.14.28.45: bajtów=32 czas<10ms TTL=254

Statystyka badania dla 212.14.28.45:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 0ms, Maksimum = 10ms, Średnia = 2ms
```

Poniżej widzimy rozwinięcie pakietu testującego, opartego na protokole ICMP.

Ranka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
2	4.614639	PACKET15...	LOCAL	ARP_RARP	ARP: Reply, Target IP: 213.155.162.182 Targ...
3	4.614639	PACKET25...	LOCAL	DNS	0x31:Std Qry for www.ps.pl. of type Host Ad...
4	4.614639	PACKET25...	LOCAL	DNS	0x31:Std Qry Resp. Auth. NS is www.ps.pl. o...
5	4.646682	PACKET25...	LOCAL	ICMP	Echo: From 213.155.162.182 To 212.14.28.45
6	4.654639	PACKET25...	LOCAL	ICMP	Echo Reply: To 213.155.162.182 From 212.14....
7	5.644639	PACKET15...	LOCAL	ICMP	Echo: From 213.155.162.182 To 212.14.28.45
8	5.644639	PACKET25...	LOCAL	ICMP	Echo Reply: To 213.155.162.182 From 212.14....
9	6.649562	PACKET25...	LOCAL	ICMP	Echo: From 213.155.162.182 To 212.14.28.45
10	6.649562	PACKET25...	LOCAL	ICMP	Echo Reply: To 213.155.162.182 From 212.14....
11	7.651002	PACKET25...	LOCAL	ICMP	Echo: From 213.155.162.182 To 212.14.28.45
12	7.651002	PACKET25...	LOCAL	ICMP	Echo Reply: To 213.155.162.182 From 212.14....

·
·
·

```

+ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
+IP: ID = 0x3D0F; Proto = ICMP; Len: 60
=ICMP: Echo: From 213.155.162.182 To 212.14.28.45
  ICMP: Packet Type = Echo
  ICMP: Echo Code = 0 (0x0)
  ICMP: Checksum = 0x395C
  ICMP: Identifier = 512 (0x200)
  ICMP: Sequence Number = 4608 (0x1200)
  ICMP: Data: Number of data bytes remaining = 32 (0x0020)

```

```

00000000  00  E0  B1  25  00  1F  00  50  BA  6F  00  00  00  45  00  .0 . . . P | oW | . E.
00000010  00  3C  3D  0F  00  00  80  01  95  24  00  00  00  00  00  . <=0 . 00H+NTs|dP
00000020  1C  2D  08  00  39  5C  02  00  12  00  61  62  63  64  65  66  L- . 9 \ @ . t . abcdef
00000030  67  68  69  6A  6B  6C  6D  6E  6F  70  71  72  73  74  75  76  ghijklmnopqrstuv
00000040  77  61  62  63  64  65  66  67  68  69  wabcdefghijklmnop

```

W momencie, gdy host docelowy jest niedostępny lub, gdy jest na nim zainstalowana usługa „FireWall”, nie zostanie odesłana żadna odpowiedź. Wysłane w sieć pakiety zostaną utracone, a działająca procedura spowoduje wyświetlenie się poniższego monitu:

```

G:\>ping 213.155.162.180

Badanie 213.155.162.180 z użyciem 32 bajtów danych:

Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.

Statystyka badania dla 213.155.162.180:
  Pakiety: Wysłane = 4, Odebrane = 0, Utracone = 4 (100% utraconych).
Szacunkowy czas błędzenia pakietów w milisekundach:
  Minimum = 0ms, Maksimum = 0ms, Średnia = 0ms

```

5. Wybrane usługi internetowe oraz bezpieczeństwo ich funkcjonowania.

Nie trzeba chyba nikogo przekonywać o tym, iż najbardziej rozpowszechnioną usługą internetową jest obecnie WWW, opierająca się na protokole HTTP. Różnorodność jej wykorzystania jest przeogromna, począwszy od dostępu do zredagowanych na stronach WWW dokumentów, a skończywszy na dostępie do poczty elektronicznej i usług bankowych poprzez formularze internetowe.

Korzyści idące z tak rozbudowanego narzędzia są niezmierzone. Powszechność tej usługi przyciąga jednak osoby postronne do nieautoryzowanego korzystania z zasobów innych użytkowników sieci. Podczas pisania owej pracy dowiodłem, że nawet przy użyciu standardowych narzędzi kontrolujących pracę sieci, jesteśmy w stanie wejść w posiadanie haseł, kodów dostępu i innych ważnych danych, ze strumienia ramek, płynących przez bezmiar Internetu. Jest to tym łatwiejsze, iż w większości przypadków informacje te nie są w żaden sposób chronione. Nawet mało doświadczony

użytkownik, jest w stanie wejść w posiadanie istotnych informacji. Poziom wiedzy na temat zabezpieczeń oraz krążenia informacji w sieci może być znikomy, ograniczając się do poznania obsługi oprogramowania ułatwiającego nielegalne rzemiosło.

Wykazałem to, na przykładzie dostępu do poczty elektronicznej poprzez formularz WWW (serwer poczty elektronicznej „Wirtualna polska”).

Ramka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
6	7.981476	LOCAL	PACKET25...	HTTP	POST Request (from client using port 1477)

000002D0	77 70 61 77 3D 41 30 32 42 32 31 44 31 36 46 30	wpaw=A02B21D16F0
000002E0	38 48 30 34 0D 0A 0D 0A 73 65 72 77 69 73 3D 6E	SH04J0J0serwis=n
000002F0	6F 77 61 5F 70 6F 63 7A 74 61 5F 77 70 26 75 72	owa_poczta_wp&ur
00000300	6C 3D 68 74 74 70 25 33 41 25 32 46 25 32 46 70	l=http%3A%2F%2Fp
00000310	6F 63 7A 74 61 2E 77 70 2E 70 6C 25 32 46 69 6E	oczta.wp.pl%2Fin
00000320	64 65 78 2E 68 74 6D 6C 26 74 72 79 4C 6F 67 69	dex.html&tryLogi
00000330	6E 3D 31 26 63 6F 75 6E 74 54 65 73 74 3D 33 26	n=1&accountTest=3&
00000340	6C 6F 67 69 6E 5F 75 73 65 72 6E 61 6D 65 3D 6C	login_username=1
00000350	6F 73 69 75 70 61 6E 74 68 65 72 26 6C 6F 67 69	osi%manther%logi
00000360	6E 5F 70 61 73 73 77 6F 72 64 3D 6B 75 70 61 26	password=kupa&
00000370	7A 61 6C 6F 67 75 6A 3D 5A 61 6C 6E 67 75 6B	&zaloguj=zaloguj

jawne: login i hasło

Możemy również dowiedzieć się, z jakiego oprogramowania korzysta serwer. Ułatwia to atak, gdyż programy posiadają błędy, które można skrzętnie wykorzystać, by zaszkodzić innym. Na rysunku poniżej widać z jakiego oprogramowania korzysta „Wirtualna Polska”.

```

⚡HTTP: Undocumented Header = Referer: http://profil.wp.pl/login.html
⚡HTTP: Undocumented Header = Accept-Language: pl
⚡HTTP: Undocumented Header = Content-Type: application/x-www-form-urlencoded
⚡HTTP: Undocumented Header = Accept-Encoding: gzip, deflate
⚡HTTP: Undocumented Header = User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
⚡HTTP: Undocumented Header = Host: profil.wp.pl
⚡HTTP: Undocumented Header = Content-Length: 151
⚡HTTP: Undocumented Header = Connection: Keep-Alive
⚡HTTP: Undocumented Header = Cookie: statid=213.155.162.182.261021068036222874685162; wpstick:
HTTP: Data: Number of data bytes remaining = 151 (0x0097)

```

Podobnie rzecz ma się z wieloma innymi usługami internetowymi. Dla przykładu przedstawimy inną popularną usługę, a mianowicie FTP.

```
G:\>ftp ftp.microsoft.com
Połączony z ftp.microsoft.com.
220 Microsoft FTP Service
Użytkownik (ftp.microsoft.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Hasło:
230-This is FTP.Microsoft.Com.
230 Anonymous user logged in.
ftp> quit
421 Timeout (30 seconds): closing control connection.
```

Tutaj również bez większego problemu przechwycić można hasło dostępu do zasobów serwera.

```
⊕TCP: .AP..., len: 27, seq:2929588872-2929588899
⊕FTP: Resp. to Port 1489, '220 Microsoft FTP Service'

⊕TCP: .AP..., len: 16, seq: 468356872
⊕FTP: Req. from Port 1489, 'USER anonymous'

⊕TCP: .AP..., len: 72, seq:2929588899-2929588971, ack: 468356888, win:17504
⊕FTP: Resp. to Port 1489, '331 Anonymous access allowed, send identity (e-mai'

⊕TCP: .AP..., len: 16, seq: 468356888-4683569
⊕FTP: Req. from Port 1489, 'PASS anonymous'

⊕TCP: .AP..., len: 32, seq:2929588971-2929589003
⊕FTP: Resp. to Port 1489, '230-This is FTP.Microsoft.Com.'

⊕TCP: .AP..., len: 31, seq:2929589003-2929589034
⊕FTP: Resp. to Port 1489, '230 Anonymous user logged in.'
```

Niektóre z aplikacji podają dane tego typu (login i hasło) wręcz w nagłówku ramki wysyłanej do sieci.

Jak nietrudno zauważyć użytkowanie zasobów sieciowych nie jest rzeczą bezpieczną. Samo podłączenie komputera do sieci może wielokrotnie wiązać się z zagrożeniem utraty danych, bezwiednego udostępnienia ich lub nawet sprzętowego uszkodzenia naszego komputera. Programy popularnie nazywane „trojanami”, bądź „końmi trojańskimi” są potężną bronią.

Kolejną rzeczą, o której warto wspomnieć w związku z niedawnymi atakami wirusów komputerowych typu „Mblast” jest sam sposób nawiązania połączenia. Na poniższym zrzucie ekranu widoczne są trzy ramki wysłane z użyciem protokołu TCP. Niebezpieczeństwo wiążące się z tego typu inicjacją transmisji polega na możliwości nawiązania znacznej liczby niepotwierdzonych połączeń, które rezydują w pamięci operacyjnej komputera wyczerpując jego zasoby. Host wysyła żądanie dostępu, a gdy otrzymuje odpowiedź, że dostęp jest możliwy, nie wysyła potwierdzenia, śląc od nowa zapytania.

Ranka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis
5	5.718222	LOCAL	PACKET25...	TCPS., len: 0, seq: 468356871-468356871...
6	5.958568	PACKET25...	LOCAL	TCP	.A..S., len: 0, seq: 2929588871-292958887...
7	5.958568	LOCAL	PACKET25...	TCP	.A...., len: 0, seq: 468356872-468356872...
8	6.198913	PACKET25...	PACKET25...	FTP	Resp. to Port 1489, '220 Microsoft FTP Serv...
9	6.329190	LOCAL	PACKET25...	TCP	.A...., len: 0, seq: 468356872-468356872...
10	17.174696	LOCAL	PACKET25...	FTP	Req. from Port 1489, 'USER anonymous'
11	17.435070	PACKET25...	LOCAL	FTP	Resp. to Port 1489, '331 Anonymous access a...
12	17.545228	LOCAL	PACKET25...	TCP	.A...., len: 0, seq: 468356888-468356888...
13	23.133264	LOCAL	PACKET25...	FTP	Req. from Port 1489, 'PASS anonymous'
14	23.393638	PACKET25...	LOCAL	FTP	Resp. to Port 1489, '230-This is FTP.Micros...
15	23.553868	LOCAL	PACKET25...	TCP	.A...., len: 0, seq: 468356904-468356904...
16	23.814243	PACKET25...	LOCAL	FTP	Resp. to Port 1489, '230 Anonymous user log...
17	23.954444	LOCAL	PACKET25...	TCP	.A...., len: 0, seq: 468356904-468356904...

trojstopniowe
nawiązywanie
połączenia

Na powyższym rysunku widać udane nawiązanie połączenia. Wysłaliśmy zapytanie, odesłana została odpowiedź twierdząca, następnie nasz komputer potwierdza chęć nawiązania połączenia.

6. Wnioski.

Powinniśmy jako użytkownicy być świadomi zagrożeń czyhających na nas w sieci. Powinniśmy chronić nasze dane (w miarę naszych potrzeb i możliwości) przed nieupoważnionym dostępem do nich. Ważne jest też zwrócenie uwagi na to, iż nie jest powiedziane, że im bardziej przyjazne i nowsze oprogramowanie, tym lepsze zabezpieczenie. Ślepe zaufanie może narazić nas na straty.