

Analiza w³amania od A do Z (czê¶æ 2)

Autor: Marek
23.01.2008.
Zmieniony 25.01.2008.

Zakończymy analizê skanuj±cego pakietu ¶ledz±cego (scan packet trace), aby zdobyæ wszystkie informacje na temat profilowania oraz rozpocz±æ atak na sieæ.

Czê¶æ pierwsz± skończyli¶my na przyjrzeniu siê pakietowej sekwencji otwieraj±cej wysy³anej przez Nmap. Wysy³ana sekwencja rozpoczyna³a siê od odpowiedzi typu „echo” ICMP, która ma ustaliæ czy komputer albo sieæ zosta³y przypisane do danego adresu IP. Ponadto byli¶my w stanie zgadn±æ, ¿e sieæ komputerowa ofiary posiada system Microsoft Windows, oparty na TTL w pakiecie „echo reply” ICMP, który zosta³ wysy³any z powrotem do atakuj±cego. To, co teraz zrobimy, to bêdzie dalsze przygl±danie siê pozosta³ym pakietom w Skanie Nmap oraz zdobyciu pozosta³ych informacji, które pozwol± nam sprofilowaæ sieæ ofiary.

Id±c dalej

```
10:52:59.078125 IP (tos 0x0, ttl 49, id 9808, offset 0, flags [none], proto: TCP (6), length: 40) 192.168.111.17.37668 >
192.168.111.23.80: ., cksum 0xfd46 (correct), ack 85042526 win 2048
```

```
0x0000: 4500 0028 2650 0000 3106 0407 c0a8 6f11 E..(&P..1.....o.
```

```
0x0010: c0a8 6f17 9324 0050 67d1 a55e 0511 a55e ..o.$Pg.^...^
```

```
0x0020: 5010 0800 fd46 0000 P....F..
```

```
10:52:59.078125 IP (tos 0x0, ttl 128, id 397, offset 0, flags [none], proto: TCP(6), length: 40) 192.168.111.23.80 >
192.168.111.17.37668: R, cksum 0x6813 (correct), 85042526:85042526(0)win 0
```

```
0x0000: 4500 0028 018d 0000 8006 d9c9 c0a8 6f17 E..(.....o.
```

```
0x0010: c0a8 6f11 0050 9324 0511 a55e 0511 a55e ..o..P.$...^...^
```

```
0x0020: 5004 0000 6813 0000 0000 0000 0000 P...h.....
```

Powy¿sze dwa pakiety przysz³y zaraz po tych opartych na ICMP, którym przygl±dali¶my siê w czê¶ci pierwszej. Nmap

wysłał pakiet ACK do IP 192.168.111.23 sieci ofiary na porcie 80. Pod względem profilowania informacji nie ma tu tego za dużo. Widzieliśmy, że pakiet ACK otrzymany od hakera uzyskał z powrotem pakiet RST, ponieważ ACK był niespodziewany. W istocie nie należał on do wcześniej ustalonego połączenia. Nadal mamy TTL o wartości 128, co odpowiada wartości TTL, jak widzieliśmy wcześniej.

```
10:52:59.296875 IP (tos 0x0, ttl 58, id 45125, offset 0, flags [none], proto: TCP (6), length: 40) 192.168.111.17.37644 >
192.168.111.23.21: S, cksum 0x37ce (correct), 2010644897:2010644897(0) win 3072
```

```
0x0000: 4500 0028 b045 0000 3a06 7111 c0a8 6f11 E..(E...:q...o.
```

```
0x0010: c0a8 6f17 930c 0015 77d8 01a1 0000 0000 ..o.....w.....
```

```
0x0020: 5002 0c00 37ce 0000 P...7...
```

```
10:52:59.296875 IP (tos 0x0, ttl 128, id 398, offset 0, flags [DF], proto: TCP (6), length: 44) 192.168.111.23.21 >
192.168.111.17.37644: S, cksum 0x4f58 (correct), 1685290308:1685290308(0) ack 2010644898 win 64240
```

```
0x0000: 4500 002c 018e 4000 8006 99c4 c0a8 6f17 E.....@.....o.
```

```
0x0010: c0a8 6f11 0015 930c 6473 7d44 77d8 01a2 ..o.....ds}Dw...
```

```
0x0020: 6012 faf0 4f58 0000 0204 05b4 0000 `...OX.....
```

```
10:52:59.296875 IP (tos 0x0, ttl 128, id 110, offset 0, flags [none], proto: TCP(6), length: 40) 192.168.111.17.37644 >
192.168.111.23.21: R, cksum 0xca50 (correct), 2010644898:2010644898(0) win 0
```

```
0x0000: 4500 0028 006e 0000 8006 dae8 c0a8 6f11 E..(n.....o.
```

```
0x0010: c0a8 6f17 930c 0015 77d8 01a2 77d8 01a2 ..o.....w...w...
```

```
0x0020: 5004 0000 ca50 0000 P....P..
```

Po wymianie pakietów ACK i RST widzimy teraz rzeczywisty pakiet SYN wysłany od hakera do sieci ofiary, co potwierdza się w pakiecie poprzez podświetlone S. Dzięki temu uzyskuje się pakiet powrotny SYN/ACK z sieci ofiary na porcie 21. Wymiana ta jest następnie finalizowana poprzez wysłanie z powrotem pakietu RST z komputera hakera do sieci ofiary. Te trzy pakiety zbierają teraz o wiele bogatsze plony pod względem profilowania informacji.

Mamy ten sam TTL o wartości 128 z komputera ofiary, lecz mamy też rozmiar okna 64240. Choć ta wartość nie znajduje się na liście, do której wcześniej odsyłałem, jest to naprawdę rozmiar okna, który widziałem wcześniej wiele razy w Win32 (32-bitowe wersje Microsoft Windows, takie jak Win NT, 2K, XP i 2K3). Inną funkcję pozwalającą na określenie komputera Microsoft Windows jest ta o możliwym do przewidzenia przyroście numerów IP ID. W tym przypadku mamy tylko wartość IP ID, tutaj akurat 398 w środkowym pakiecie powyżej. Potrzebowalibyśmy przynajmniej jeszcze jednego, zanim będziemy w stanie z większą pewnością powiedzieć, że ten komputer naprawdę działa pod systemem Windows. Aby to pokazać, przyglądnijmy się pozostałym pakietom ze skanu Nmap.

```
10:52:59.312500 IP (tos 0x0, ttl 59, id 54025, offset 0, flags [none], proto: TCP (6), length: 40) 192.168.111.17.37644 >
192.168.111.23.80: S, cksun 0x3393 (correct), 2010644897:2010644897(0) win 4096
```

```
0x0000: 4500 0028 d309 0000 3b06 4d4d c0a8 6f11 E..(.....;MM..o.
```

```
0x0010: c0a8 6f17 930c 0050 77d8 01a1 0000 0000 ..o....Pw.....
```

```
0x0020: 5002 1000 3393 0000 P...3...
```

```
10:52:59.312500 IP (tos 0x0, ttl 128, id 399, offset 0, flags [DF], proto: TCP (6), length: 44) 192.168.111.23.80 >
192.168.111.17.37644: S, cksun 0x7913 (correct), 1685345101:1685345101(0) ack 2010644898 win 64240
```

```
0x0000: 4500 002c 018f 4000 8006 99c3 c0a8 6f17 E....@.....o.
```

```
0x0010: c0a8 6f11 0050 930c 6474 534d 77d8 01a2 ..o..P..dtSMw...
```

```
0x0020: 6012 faf0 7913 0000 0204 05b4 0000 `...y.....
```

```
10:52:59.312500 IP (tos 0x0, ttl 128, id 111, offset 0, flags [none], proto: TCP(6), length: 40) 192.168.111.17.37644 >
192.168.111.23.80: R, cksun 0xca15 (correct), 2010644898:2010644898(0) win 0
```

```
0x0000: 4500 0028 006f 0000 8006 dae7 c0a8 6f11 E..(o.....o.
```

```
0x0010: c0a8 6f17 930c 0050 77d8 01a2 77d8 01a2 ..o....Pw...w...
```

```
0x0020: 5004 0000 ca15 0000 P.....
```

Pierwszą informacją, na którą patrzy haker jest sprawdzenie czy numer IP ID wzrasta do 399. Ta wartość IP ID wynosi właśnie 399, jak widać w środkowym pakiecie. Mając tę informację, haker jest raczej pewny, że ma do czynienia albo z NT, 2K, XP, albo 2K3. W tej sekwencji pakietu widać także, że port 80 w sieci ofiary wydaje się mieć usługę, co pokazuje SYN/ACK. Pakiet SYN/ACK jest ustalony dzięki weryfikacji pola flagi w nagłówku TCP, w tym przypadku

podkreślona szesnastkowa wartość 12 albo liczba dziesiętna 18. Wartość ta jest osiągnięta poprzez dodanie wartości 2 flagi SYN do wartości 16 flagi ACK.

I dalej do wyliczania

Skoro haker teraz wie, że oba porty 21 i 80 są otwarte, przechodzi do etapu wyliczania. To co musi wiedzieć, to pytanie jaki rodzaj serwera WWW oczekuje na połączenia. Byłoby bez sensu, gdyby użył do tego Apache exploit na serwerze IIS. Pamiętaj o tym, haker otwiera sesję cmd.exe i uruchamia program netcat.

```
C:\>nc.exe 192.168.111.23 80
```

```
GET s/s/s/s
```

```
HTTP/1.1 400 Bad Request
```

```
Server: Microsoft-IIS/5.0
```

```
Date: Mon, 06 Aug 2007 15:11:48 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 87
```

```
The parameter is incorrect.
```

```
C:\>
```

Powyżej widasz skądniê netcat lub nc.exe, który wpisuje do adresu IP ofiary, jak i numer portu 80. Gdy przyciśnie „enter”, wpisuje HTTP czasownika „GET”, a za nim jakiegokolwiek bzdury. Powoduje to, że serwer WWW ofiary wyśle z powrotem informacje systemowe, ponieważ nie rozumie próby. W istocie wylicza je sam :-). Tak więc haker wie teraz, że patrzy na Microsoft IIS 5.0. Tak naprawdę jest to wspaniała wiadomość, ponieważ ma on różnorodny exploit dla tej wersji IIS. Wszystko ładnie komponowane w Metasploit Framework.

Podsumowanie

Gdy haker przeskanowa³ sieæ ofiary przy u¿yciu narzêdzia Nmap, otrzyma³ istotn± seriê pakietów. W tych pakietach ukrytych by³o – jak zauwa¿yli¶my – wystarczaj±co du¿o informacji, aby haker móg³ w m±dry sposób zaatakowaæ system operacyjny, architekturê, a przy u¿yciu netcata tak¿e rodzaj serwera.

- Mieli¶my wzrastaj±cy numer IP ID, wskazuj±cy na MS Windows.
- Mieli¶my TTL o warto¶ci 128, co ponownie wskazuje na MS Windows.
- TTL o warto¶ci 128 wskazuje tak¿e na architekturê Intel x86 w miejsce – powiedzmy – SPARC.
- Nastêpnie poprzez netcat zobaczyli¶my, ¿e serwerem WWW by³ MS IIS 5.0.

W sumie niez³y zbiór informacji. Pozwoli³ on hakerowi sprofilowaæ host, architekturê oraz oferowan± us³ugê. Maj±c te informacje w d³oni, haker by³ gotowy, aby rozpocz±æ atak na serwery sieci ofiary. W czê¶ci trzeciej w³a¶nie temu siê przygl±dniemy. Do zobaczenia.

Źród³o: www.windowsecurity.com