helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

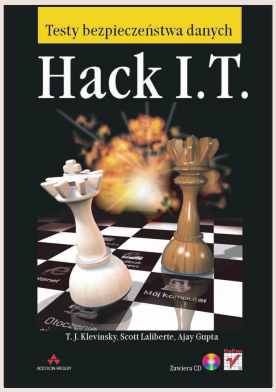
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Hack I.T. Testy bezpieczeństwa danych



Autorzy: T.J. Klevinsky, Scott Laliberte, Ajay Gupta
Tłumaczenie: Witold Kurylak, Przemysław Szeremiota
ISBN: 83-7361-232-7
Tytuł oryginału: Hack I.T. – Security Through Penetration Testing
Format: B5, stron: 462

Jeżeli w administrowanym przez Ciebie systemie znajduje się 10 słabych punktów, hakerowi wystarczy znalezienie jednego z nich, by Cię pokonać. Ty natomiast musisz załatać wszystkie luki w zabezpieczeniach. Ta gra jest tylko z pozoru nierówna, dysponując odpowiednimi narzędziami i wiedzą, możesz skutecznie przeciwdziałać włamaniom.

Książka „Hack I.T. Testy bezpieczeństwa danych" to kompendium wiedzy na temat testów penetracyjnych ujawniających słabe punkty w zabezpieczeniach. Jej autorami są specjaliści firmy Ernst&Young o wieloletnim doświadczeniu w tej dziedzinie. Dzięki tej książce dowiesz się gdzie szukać potencjalnych zagrożeń i jak się przed nimi bronić. Znajdziesz tu także wiele ciekawych informacji o pracy hakerów, o używanych przez nich narzędziach, wreszcie dowiesz się, jak wykorzystać te narzędzia we własnej obronie.

Książka przedstawia:

- Środowisko hakerów i mity o nich
- Metodologie prowadzenia testów penetracyjnych
- Najczęściej wykorzystywane luki w zabezpieczeniach i niebezpieczne protokoły
- Sposoby zbierania informacji o celu ataku
- Ataki przez internet i przez sieć telefoniczną
- Metody socjotechniczne
- Ataki na systemy Uniksowe i NT
- Zautomatyzowane narzędzia skanujące
- Programy do śledzenia ruchu w sieci, łamania haseł, włamywania się na serwery WWW
- Systemy wykrywania włamań
- Zapory sieciowe i metody ich omijania
- Ataki odmowy obsługi (DoS)

W książce znajdziesz także informacje o najgroźniejszych lukach w oprogramowaniu i najczęściej atakowanych portach. Dołączony do książki CD-ROM zawiera wiele cennych narzędzi, przydatnych do przeprowadzania testów penetracyjnych.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Słowo wstępne **11**

Przedmowa **13**

Wprowadzenie **19**

Rozdział 1. Włamania do systemów — stan na dzień dzisiejszy **23**

Rozdział 2. Określenie hakera **29**

2.1. Poziomy umiejętności hakerów 30
2.1.1. Hakerzy pierwszorzędni 30
2.1.2. Hakerzy drugorzędni 30
2.1.3. Hakerzy trzeciorzędni 31
2.2. Konsultanci do spraw zabezpieczeń 32
2.3. Mity o hakerach 33
2.4. Mity o zabezpieczaniu informacji 34

Rozdział 3. Penetracja na zamówienie **37**

3.1. Konsekwencje testów penetracyjnych 38
3.2. Wymagania stawiane niezależnemu konsultantowi 39
3.2.1. Umiejętności 39
3.2.2. Wiedza 39
3.2.3. Zestaw narzędzi 40
3.2.4. Sprzęt 40
3.2.5. Rejestrowanie działań 41
3.2.6. Etyka 41
3.3. Zapowiedziane i niezapowiedziane testy penetracyjne 42
3.3.1. Definicje 42
3.3.2. Wady i zalety obu rodzajów testów penetracyjnych 43
3.3.3. Dokumentowanie możliwości ataku 44

Rozdział 4. Niebezpieczne miejsca **45**

4.1. Luki w zabezpieczeniach aplikacji 47
4.2. Implementacje BIND (Berkeley Internet Name Domain) 48
4.3. Interfejs CGI (Common Gateway Interface) 48
4.4. Usługi tekstu otwartego 49
4.5. Konta domyślne 49

4.6. Usługa DNS 49
4.7. Uprawnienia do pliku 50
4.8. Protokół FTP i telnet 50
4.9. ICMP 51
4.10. IMAP i POP 51
4.11. Modemy 52
4.12. Brak monitoringu i wykrywania ataków 52
4.13. Architektura sieci 53
4.14. System plików NFS (Network File System) 54
4.15. Porty systemu NT 135 – 139 54
4.16. Połączenie null connection w systemie NT 55
4.17. Słabe hasło i identyfikator użytkownika 55
4.18. Usługi zdalnego administrowania 56
4.19. Zdalne wywołanie procedury (RPC) 57
4.20. Usługa sendmail 57
4.21. Usługi uruchamiane domyślnie 58
4.22. Protokół SMTP (Simple Mail Transport Protocol) 58
4.23. Łańcuch kontrolny protokołu SNMP (Simple Network Management Protocol) 59
4.24. Wirusy i ukryte kody 59
4.25. Przykładowe pliki serwera WWW 60
4.26. Ogólna podatność serwera WWW na atak 61
4.27. Monitorowanie luk w zabezpieczeniach 61

Rozdział 5. Penetracja przez internet 65
5.1. Tworzenie wykazu urządzeń w sieci 66
5.1.1. Polecenie Whois 66
5.1.2. Przesłanie informacji o strefie 68
5.1.3. Polecenie PING 69
5.1.4. Śledzenie trasy 70
5.2. Analiza podatności na atak 71
5.2.1. Rozpoznawanie systemów operacyjnych 72
5.2.2. Skanowanie portów 72
5.2.3. Wykaz aplikacji 74
5.2.4. Przeszukiwanie internetu 75
5.3. Wykorzystywanie słabych punktów 75
Studium przypadku: Komputery dołączone jednocześnie do dwóch sieci 77

Rozdział 6. Penetracja przez połączenie telefoniczne 81
6.1. Atak war dialing 81
6.2. Metoda war dialing 82
6.2.1. Wybieranie numeru 82
6.2.2. Rejestrowanie się 82
6.2.3. Ekrany logowania 83
6.3. Poszukiwanie numerów 84
6.4. Metody zapobiegawcze 85
6.5. Narzędzia do ataku war dialing 86
6.5.1. ToneLoc 86
6.5.2. THC-Scan 88
6.5.3. TeleSweep 91
6.5.4. PhoneSweep 92
Studium przypadku: War Dialing 92

Rozdział 7. Wewnętrzne testy penetracyjne 95
7.1. Scenariusze 96
7.2. Zbieranie informacji o sieci 97

7.3. Informacje o systemie NT ... 101
7.4. Unix ... 104
7.5. Poszukiwanie narzędzi ataku ... 105
7.6. Analiza ruchu w sieci ... 106
7.7. Zdalne instalowanie zestawu narzędzi ... 108
7.8. Skanowanie w poszukiwaniu słabych punktów ... 109
Studium przypadku: Sprawdzanie komputera stacjonarnego ... 109

Rozdział 8. Socjotechnika ... 111
8.1. Telefon ... 111
8.1.1. Obsługa techniczna ... 112
8.1.2. Niezadowolony klient ... 113
8.1.3. Prośba o pomoc w logowaniu ... 115
8.1.4. Metody dodatkowe ... 116
8.2. Grzebanie w śmieciach ... 116
8.3. Informacje z biurka ... 117
8.4. Typowe środki zaradcze ... 118

Rozdział 9. Metody uniksowe ... 121
9.1. Usługi w systemie Unix ... 122
9.1.1. Usługi inetd ... 123
9.1.2. Usługi zdalne ... 127
9.1.3. Usługi zdalnego wywołania procedury (RPC) ... 128
9.2. Ataki powodujące przepełnienie bufora ... 129
9.3. Zezwolenia do plików ... 130
9.4. Aplikacje ... 132
9.4.1. Serwery pocztowe ... 133
9.4.2. Serwery WWW ... 134
9.4.3. X Windows ... 135
9.4.4. Serwery DNS ... 136
9.5. Błędy w konfiguracji ... 137
9.6. Narzędzia uniksowe ... 138
9.6.1. Datapipe.c ... 138
9.6.2. QueSO ... 139
9.6.3. Cheops ... 139
9.6.4. NFSSHELL ... 142
9.6.5. XSCAN ... 143
Studium przypadku: Penetracja systemu Unix ... 144

Rozdział 10. Zestaw narzędzi ... 147
10.1. Sprzęt ... 147
10.2. Oprogramowanie ... 148
10.2.1. Stacja robocza Windows NT ... 149
10.2.2. Linux ... 149
10.3. VMware ... 150

Rozdział 11. Zautomatyzowane skanery luk ... 153
11.1. Definicja ... 153
11.2. Zastosowanie ... 154
11.3. Wady ... 154
11.4. Skanery zbierające dane z sieci i skanery monitorujące działalność komputera ... 155
11.5. Narzędzia ... 157
11.6. Skanery zbierające dane z sieci ... 158
11.6.1. Skaner Network Associates CyberCop ... 158
11.6.2. ISS Internet Scanner ... 161

11.6.3. Nessus ... 163
11.6.4. Symantec (uprzednio Axent Technologies) NetRecon ... 165
11.6.5. Bindview HackerShield (bv-control for Internet Security) ... 165
11.7. Skanery monitorujące działalność komputera ... 166
11.7.1. Symantec (uprzednio Axent Technologies) Enterprise Security Manager (ESM) ... 166
11.8. Pentasafe VigilEnt ... 168
11.9. Wnioski ... 169

Rozdział 12. Narzędzia do pozyskiwania informacji ... 171
12.1. WS_Ping ProPack ... 171
12.2. NetScanTools ... 180
12.3. Sam Spade ... 188
12.4. Rhino9 Pinger ... 201
12.5. VisualRoute ... 202
12.6. Nmap ... 205
12.7. What's running ... 207

Rozdział 13. Skanery portów ... 209
13.1. Nmap ... 209
13.2. 7th Sphere Port Scanner ... 215
13.3. Strobe ... 216
13.4. SuperScan ... 217

Rozdział 14. Programy do analizy ruchu w sieci ... 221
14.1. Dsniff ... 222
14.2. Linsniff ... 224
14.3. Tcpdump ... 224
14.4. BUTTSniffer ... 225
14.5. SessionWall-3 (obecnie eTrust Intrusion Detection) ... 227
14.6. AntiSniff ... 228

Rozdział 15. Łamacze haseł ... 233
15.1. L0phtCrack ... 233
15.2. pwdump2 ... 239
15.3. John the Ripper ... 240
15.4. Cain ... 242
15.5. ShowPass ... 243

Rozdział 16. Narzędzia dla Windows NT ... 245
16.1. NET USE ... 245
16.2. Połączenie zerowe ... 246
16.3. NET VIEW ... 247
16.4. NLTEST ... 249
16.5. NBTSTAT ... 250
16.6. EPDUMP ... 251
16.7. NETDOM ... 252
16.8. Getmac ... 253
16.9. Local administrators ... 253
16.10. Global ... 254
16.11. Usrstat ... 255
16.12. DumpSec ... 256
16.13. User2sid i sid2user ... 259
16.14. NetBIOS Auditing Tool (NAT) ... 260
16.15. SMBGrind ... 263
16.16. SRVCHECK ... 264

16.17. SRVINFO ... 265
16.18. AuditPol ... 266
16.19. REGDMP ... 267
16.20. Somarsoft DumpReg ... 268
16.21. Remote ... 270
16.22. Netcat ... 271
16.23. SC ... 273
16.24. AT ... 274
16.25. FPipe ... 275
Studium przypadku: Słabe hasła ... 276
Studium przypadku: Wewnętrzna penetracja systemu Windows ... 281

Rozdział 17. Narzędzia penetracji WWW ... 285
17.1. Whisker ... 286
17.2. SiteScan ... 288
17.3. THC Happy Browser ... 289
17.4. wwwhack ... 290
17.5. Web Cracker ... 292
17.6. Brutus ... 293
Studium przypadku: Luka w oprogramowaniu Compaq Insight Manager ... 295

Rozdział 18. Zdalne sterowanie systemem ... 299
18.1. PcAnywhere ... 300
18.2. Virtual Network Computing ... 304
18.3. NetBus ... 307
18.4. Back Orifice 2000 ... 311

Rozdział 19. Systemy wykrywania włamań ... 315
19.1. Definicja systemu wykrywania włamań ... 315
19.2. Unikanie wykrycia ... 317
19.2.1. Utajone skanowanie portów ... 320
19.2.2. Techniki agresywne ... 322
19.3. Pułapki ... 323
19.4. Cechy skutecznego systemu wykrywania włamań ... 323
19.5. Wybór systemu wykrywania włamań ... 329
19.5.1. RealSecure ... 329
19.5.2. NetProwler ... 330
19.5.3. Secure Intrusion Detection ... 330
19.5.4. eTrust Intrusion Detection ... 331
19.5.5. Network Flight Recorder ... 332
19.5.6. Dragon ... 332
19.5.7. Snort ... 333

Rozdział 20. Zapory sieciowe ... 335
20.1. Definicja ... 335
20.2. Monitorowanie ... 336
20.3. Konfiguracja ... 337
20.4. Nadzorowanie zmian ... 338
20.5. Rodzaje zapór sieciowych ... 338
20.5.1. Zapory sieciowe z filtrowaniem pakietów ... 339
20.5.2. Zapory sieciowe z kontrolą ładunku ... 340
20.5.3. Zapory sieciowe z serwerem pośredniczącym ... 340
20.6. Translacja adresów sieci wewnętrznej ... 341
20.7. Omijanie zapór sieciowych ... 341
20.8. Zapory sieciowe a wirtualne sieci prywatne ... 344
Studium przypadku: Atak na serwer IIS: MDAC ... 345

Rozdział 21. Ataki odmowy obsługi 349
21.1. Ataki wyczerpania zasobów 351
21.1.1. Papasmurf 351
21.1.2. Trash2 353
21.1.3. Igmpofdeath.c 353
21.1.4. Fawx 354
21.1.5. OBSD_fun 354
21.2. Zatykanie portów 355
21.2.1. Multilate 355
21.2.2. Pepsi5 356
21.3. Zalewanie pakietami SYN 356
21.3.1. Synful 357
21.3.2. Synk4 357
21.3.3. Naptha 358
21.4. Fragmentacja pakietów IP 358
21.4.1. Jolt2 359
21.4.2. Teardrop 360
21.4.3. Syndrop 360
21.4.4. Newtear 361
21.5. Rozproszone ataki odmowy obsługi 361
21.5.1. Tribe Flood Network 2000 363
21.5.2. Trin00 365
21.5.3. Stacheldraht 366
21.5.4. Obsługa sieci DDoS 368
21.6. Ataki odmowy obsługi wymierzone w aplikacje 369
21.6.1. Up Yours 370
21.6.2. Wingatecrash 372
21.6.3. WinNuke 372
21.6.4. BitchSlap 373
21.6.5. DOSNuke 373
21.6.6. Shutup 374
21.6.7. Ataki odmowy obsługi wymierzone w serwery WWW 374
21.7. Zbiorcze narzędzia ataków odmowy obsługi 375
21.7.1. CyberCop 376
21.7.2. ISS Internet Scanner 376
21.7.3. Toast 378
21.7.4. Spike.sh5.3 379
21.8. Podsumowanie 380

Rozdział 22. Podsumowanie 381
22.1. Profilaktyka 381
22.2. Aktualizacja 385
22.2.1. Witryny WWW 385
22.2.2. Listy dystrybucyjne poczty elektronicznej 386

Rozdział 23. Trendy i mody 393
23.1. Uwierzytelnianie 393
23.1.1. Uwierzytelnianie wieloelementowe 394
23.1.2. Metody biometryczne 394
23.1.3. Uwierzytelnianie z wykorzystaniem żetonów 395
23.1.4. Usługi katalogowe 396
23.2. Szyfrowanie 396
23.3. Infrastruktura klucza publicznego 397
23.4. Systemy rozproszone 398

23.5. Dochodzenia komputerowe ... 398
23.6. Regulacje prawne ... 399
23.7. Techniki włamań ... 400
23.8. Profilaktyka ... 401
23.9. Ubezpieczenia od skutków przestępstw komputerowych ... 401

Dodatek A Zawartość płyt CD-ROM ... 403

Dodatek B Dwadzieścia najgroźniejszych dla bezpieczeństwa internetu luk w oprogramowaniu ... 407

Skorowidz ... 449

Rozdział 5.
Penetracja przez internet

W tym rozdziale zaczniemy omawiać ogólne procesy, mające miejsce przy prowadzeniu testów penetracyjnych, jakie udało nam się opracować w trakcie naszych doświadczeń. Proponowane procedury nie są oczywiście jedynymi, jakie można stosować i stale pracujemy nad udoskonaleniem naszych metod, niemniej jednak chcielibyśmy tu podkreślić, że przedstawione techniki stanowią skuteczny środek prowadzący do infiltracji sieci i umożliwiający skuteczne zbadanie jej zabezpieczeń.

Przedstawiona tu metoda badania zabezpieczeń sieci na pewno nie jest jedyną możliwą i inni profesjonaliści mogą korzystać z metod odmiennych, również dających pozytywne wyniki. Możemy jednak zapewnić, że nasza metoda jest sprawdzona i skuteczna.

Korzystanie z dobrze określonej, spójnej metodyki pozwala na prowadzenie testów penetracyjnych z zachowaniem odpowiedniego poziomu dokładności. Zawodowi konsultanci, wynajmowani do przeprowadzania testów penetracyjnych, starają się włamać do badanej sieci w określonym czasie, zazwyczaj jest to kwestia tygodni lub nawet kilku dni. Inaczej sprawa przedstawia się w przypadku hakerów, którzy mogą poświęcić dowolną ilość czasu, starając się uzyskać dostęp administratora systemu. Dlatego też niezbędne jest używanie właściwych metod, pozwalających w określonym czasie systematycznie sprawdzać znane słabe punkty i wyszukiwać luki w zabezpieczeniach. Używanie tych samych metod ma jeszcze tę zaletę, że gwarantuje stały poziom wiarygodności wyników uzyskiwanych w różnych badaniach.

Przeprowadzanie testów penetracyjnych można podzielić na trzy etapy:

1. *Tworzenie wykazu urządzeń w sieci* — wyszukanie jak największej ilości informacji o celu ataku.
2. *Analiza podatności na atak* — określenie potencjalnych metod ataku.
3. *Wykorzystywanie słabych punktów* — próba włamania do sieci z zastosowaniem wyników analizy podatności na atak przy wykorzystaniu jak największej liczby sposobów atakowania, możliwych do użycia w określonym czasie.

W dalszej części rozdziału opiszemy również narzędzia najbardziej użyteczne w wykonywaniu przedstawionych zadań.

5.1. Tworzenie wykazu urządzeń w sieci

Zanim uda nam się uzyskać nieuprawniony dostęp do sieci, musimy zapoznać się z jej topologią. Każda informacja jest kolejnym elementem układanki. Zależy nam zwłaszcza na uzyskaniu takich informacji o sieci, jak: lista działających w niej komputerów centralnych, wygląd jej architektury oraz dopuszczalny rodzaj ruchu (na przykład TCP, UDP, IPX). Z wiadomości tych można później skorzystać przy określaniu sposobu ataku.

Proces zdobywania informacji nazywamy tworzeniem wykazu urządzeń w sieci; stanowi on pierwszy etap zewnętrznych testów penetracyjnych. Odbywa się zazwyczaj przez internet przy użyciu powszechnie stosowanego oprogramowania i ogólnie dostępnych zasobów informacji. Większość z uzyskiwanych na tym etapie wiadomości jest ogólnie dostępna, a ich pozyskiwanie jest legalne. Niemniej jednak, wiele przedsiębiorstw prowadzi monitoring i sprawdza, kto stara się uzyskać takie informacje, ponieważ może to świadczyć o potencjalnym ataku w przyszłości.

5.1.1. Polecenie Whois

Zanim rozpoczniemy skanowanie sieci, musimy określić nazwy domen i zakresy adresów IP badanej organizacji. Aby upozorować sytuację działania hakera atakującego z zewnątrz, na początku konsultant nie powinien dysponować żadnymi informacjami, dzięki czemu jego zadanie jest porównywalne z zadaniem stojącym przed hakerem. Jednak przed przejściem do drugiego etapu procesu wszystkie zidentyfikowane nazwy domen i adresy IP należy zweryfikować z rzeczywistymi, aby upewnić się, że stanowią one własność danej organizacji i mieszczą się w zakresie testów.

W celu określenia zakresu adresów IP, przynależnych danemu klientowi, korzystamy z polecenia `whois` uruchamianego przez internet. Polecenie można uruchomić bezpośrednio w większości środowisk uniksowych (zastosowanie polecenia i jego składnię dla określonej wersji Uniksa można sprawdzić pod `man whois`). W środowisku Windows do wykonywania polecenia `whois` można korzystać z dwóch narzędzi *Ws PingPro Pack* i *Sam Spade* (są one szerzej omówione w rozdziale 12.).

Z polecenia `whois` można również skorzystać za pośrednictwem witryn *www.arin.net* i *www.networksolutions.com* w sieci WWW. Na rysunku 5.1 przedstawiono przykład polecenia `whois` w witrynie Network Solutions (bez serwerów domeny) dla domeny *klevinsky.com*.

Polecenie `whois` umożliwia uzyskanie informacji o osobie lub jednostce administrującej siecią, o jednostce odpowiedzialnej za opłaty związane z rejestracją domeny oraz o adresie badanej sieci. Dwie pierwsze informacje mogą być przydatne przy przygotowywaniu ataku z użyciem socjotechniki (więcej na ten temat w rozdziale 8.).

W ten sposób uzyskujemy również zakresy adresów IP skojarzonych z wprowadzoną nazwą. W rezultacie możemy uzyskać również zakresy adresów, które należą do innej organizacji o podobnej nazwie. Przykładowo, w przypadku użycia polecenia `whois` dla



Rysunek 5.1. *Polecenie whois dla domeny klevinsky.com*

nazwy *company*, w częściowych rezultatach pojawią się zarejestrowane adresy IP dla różnych firm, w których nazwach występuje słowo *company*, natomiast może nie być w nich organizacji, która ma być celem ataku.

W przypadku, gdy dany klient dysponuje kilkoma zakresami adresów IP, część z nich może należeć do innego działu organizacji klienta i może znajdować się poza zakresem wyszukiwania. W takich sytuacjach należy odpowiednio zweryfikować kryteria wyszukiwania.

W wyniku zastosowania polecenia `whois` uzyskujemy tylko pierwszych 50 pozycji, które odpowiadają zadanym kryteriom. To ograniczenie jest wprowadzone przez centrum Internic w celu zminimalizowania czasu wyszukiwania. Wraz ze wzrostem domen internetowych, zadanie przeszukania wszystkich list i przedstawienia wszystkich możliwych odpowiednich rezultatów staje się coraz trudniejsze pod względem obliczeniowym.

Jeśli przedsiębiorstwo dysponuje większą liczbą interesujących nas listingów niż 50, trzeba podejść do wyszukiwania bardziej twórczo. Jedna z metod polega na podzieleniu nazwy przedsiębiorstwa albo na wyszukaniu zmodyfikowanych nazw lub nazw występujących w liczbie mnogiej. Można znaleźć nazwy organizacji zależnych od badanego przedsiębiorstwa (warto w tym celu sprawdzić informacje prasowe umieszczane na jego witrynie WWW) i wyszukać również te nazwy.

5.1.2. Przesłanie informacji o strefie

Dzięki poleceniu `whois` można uzyskać również listę serwerów nazw domeny, umożliwiających odwzorowanie nazwy komputera centralnego i adresu IP badanej sieci (te informacje, wraz z informacjami o kontakcie, można znaleźć, klikając towarzyszącą listingowi nazwę *Net Block*). W celu uzyskania listingu IP sieci musimy zastosować przesłanie informacji o strefie dla każdego systemu zidentyfikowanego jako serwer DNS. Polecenie przesłania informacji o strefie powoduje wyświetlenie pełnej listy adresów IP i nazw komputerów centralnych. Lista taka przechowywana jest wewnątrz DNS dla określonej domeny.

Przesłanie informacji o strefie można wykonać za pomocą polecenia nslookup, obsługiwanego zarówno przez platformę Unix, jak i Windows. W systemie operacyjnym Windows narzędzia *Sam Spade*, *Ws PingPro Pack* i *NetScan* udostępniają graficzny interfejs użytkownika, pomocny w przesłaniu informacji o strefie. W celu przesłania informacji o strefie należy skorzystać z serwera DNS, odpowiedzialnego za interesującą nas domenę, w związku z czym należy użyć serwerów nazw domeny wyszukanych w procesie `whois`. W rozdziale 12. omówimy metody wykonywania przesłania informacji o strefie.

Po przesłaniu informacji o strefie otrzymujemy listing adresów IP i odpowiadających im nazw komputerów. Przykładowy wydruk może wyglądać tak, jak przedstawiono poniżej:

```
ls -d abc.com
[server.abc.com]
 abc.com.                    SOA        server.abc.com
admin.abc.com.             (200000068 300 800 359100 4700)
 abc.com.                    A          10.10.10.30
 abc.com.                    NS         server.abc.com
 abc.com                     MX         10 mail.abc.com
 business                    A          10.10.10.11
 application                 A          10.10.10.32
 mailsweeper                 A          10.10.10.50
 mimesweeper                 CNAME      server4.abc.com
 server4                     A          10.10.10.40
 abc.com.                    SOA        server.abc.com
amin.abc.com.              (200000068 300 800 359100 4700)
```

Nazwy komputerów centralnych z reguły wskazują na pełnioną przez nie funkcję. Przykładowo, urządzenie służące w przedsiębiorstwie za zaporę sieciową zazwyczaj nazywane jest *firewall* lub nosi nazwę zgodną z nazwą działającej na nim zapory sieciowej, na przykład *Gauntlet* lub *Firewall1*. Podobnie jest w przypadku innych urządzeń — spotkaliśmy takie nazwy, jak *mail.nazwafirmy.com*, *smtp.nazwafirmy.com*, *ftp.nazwafirmy.com*, *dns01.nazwafirmy.com*, *ns01.nazwafirmy.com* czy *web03.nazwafirmy.com*. Nazwy te nie tylko informują o funkcji, ale również wskazują na obecność innych urządzeń. I tak na przykład, jeśli w danej sieci istnieje urządzenie *web03*, można przypuszczać, że będzie również *web01* i *web02*. Jeśli mamy urządzenie *ns01*, prawdopodobnie będzie też *ns* i *ns02*. W związku z powyższym, dobrym rozwiązaniem jest w tym przypadku wykorzystywanie nazw drużyn sportowych, nazwisk słynnych ludzi czy bohaterów kreskówek. Są łatwe do zapamiętania i nie ujawniają żadnych technicznych informacji.

Podczas wykonywania przesłania informacji o strefie należy pamiętać, że często serwer DNS nie posiada pełnego listingu wszystkich komputerów docelowej sieci. Kilka komputerów może korzystać z protokołu DHCP, a przedsiębiorstwo może używać odrębnych serwerów nazw domeny dla odrębnych domen. Dodatkowo, serwer DNS może nie obsługiwać żądań przesłania informacji o strefie od nieuwierzytelnionych komputerów, zezwalając na to tylko tym, które pochodzą z zapasowych serwerów nazw w danej organizacji. Dlatego też należy wykonywać przesłanie informacji o strefie dla wszystkich zidentyfikowanych serwerów nazw domeny sieci docelowej. Jeden z nich może przynajmniej udostępnić częściowy listing.

Spotkaliśmy również przedsiębiorstwa korzystające z zewnętrznej obsługi funkcji nazw domeny lub używające serwera DNS swego dostawcy usług internetowych. Z naszego doświadczenia wynika, że wykonywanie przesłania informacji o strefie wobec serwera DNS lub innego urządzenia, należącego do dostawcy usług internetowych lub strony niezależnej, zazwyczaj nie spotyka się ze zrozumieniem tej strony trzeciej. W takim przypadku najczęściej pomijamy ten etap, chyba że uzyskaliśmy pisemną zgodę zarówno badanej organizacji, jak i strony trzeciej. Jeśli taka sytuacja ma miejsce, należy upewnić się, że warunki prowadzenia testów penetracyjnych wyraźnie określają, czy takie systemy są objęte testowaniem.

Z drugiej strony, urządzenia DNS, które należą do organizacji klienta, ale nie mieszczą się w zakresie adresów IP, powinny być uwzględniane w zadaniu testowania (jeśli tylko istnieje jakaś szansa na to, że takie urządzenie DNS może udostępnić informacje o domenie będącej obiektem ataku), ponieważ są potencjalnym celem przesłania informacji o strefie. Penetracja z internetu bazuje bowiem na wykorzystaniu ogólnie dostępnych informacji.

Tak na ogół bywa, gdy cel ataku obejmuje jedną lub kilka domen w dużej organizacji. Główny serwer DNS tej organizacji prawdopodobnie będzie posiadał częściowy listing komputerów w docelowej domenie, nawet jeśli znajduje się poza tą domeną.

W przeciwieństwie do polecenia `whois`, żądanie przesłania informacji o strefie wyraźnie wskazuje na działanie hakera, gdyż przeciętnemu użytkownikowi takie wiadomości nie są do niczego potrzebne. Dlatego też osoba korzystająca z takiego polecenia może być od razu traktowana jak potencjalny włamywacz. Zalecane jest, aby przed rozpoczęciem tego typu działań dobrze ocenić sytuację, bo personel może odebrać to jak rozpoczęcie testów penetracyjnych.

5.1.3. Polecenie PING

Następnym krokiem jest sprawdzenie odnalezionych adresów IP za pomocą polecenia ping, aby określić, czy włączone są komputery o tych adresach. Istnieje szereg metod służących do wykonania tego zadania. Najczęściej używaną jest zastosowanie tradycyjnego ping ICMP (z żądaniem potwierdzenia), ale coraz bardziej popularny jest ping TCP (z pełnym lub częściowym negocjowaniem połączenia). Coraz więcej serwerów jest już zabezpieczanych przed tradycyjnym narzędziem ping przez ograniczenia w ruchu ICMP lub blokowanie ruchu na granicznej zaporze sieciowej i ruterze. Istnieje jednak szansa, że ping TCP może uzyskać dostęp do sieci.

W ostatnim czasie organizacje coraz skuteczniej blokują polecenie ping, a środki zaradcze są coraz powszechniejsze. Można z dużą dozą prawdopodobieństwa założyć, że komputer, wysyłający potwierdzenie na żądanie ICMP, jest czynny, jednak fakt, że komputer nie wysyła takiego potwierdzenia, wcale nie musi oznaczać, że jest wyłączony. Może być wyłączony, ale może mieć również miejsce filtrowanie ruchu ICMP do tego komputera i polecenie ping po prostu do niego nie dociera. Urządzenia zabezpieczające mogą również wysyłać fałszywe odpowiedzi na żądanie potwierdzenia.

W zależności od zakładanego stopnia wykorzystania narzędzia ping, można użyć różnych metod, aby fakt posługiwania się nim ukryć przed systemem wykrywania włamań, który może monitorować ruch w sieci. Metody te omówimy dokładnie w rozdziale 12., w części poświęconej narzędziu *Nmap*, warto jednak już teraz wspomnieć, że przydatne jest losowe wybieranie kolejności adresów IP, zmienianie czasu między wysyłaniem kolejnych pakietów ping, jak również dzielenie adresów IP na grupy (jest to najbardziej użyteczne w przypadku dużej liczby komputerów, powyżej 100).

Program *ping* można znaleźć w większości systemów operacyjnych i może być uruchamiany przy użyciu wielu narzędzi. Jednym z najpopularniejszych jest Nmap, w związku z jego konfiguracją, łatwością używania oraz szeregiem innych funkcji, jakie posiada (ping TCP, skanowanie portów, rozpoznawanie systemów operacyjnych). W środowisku Windows dobrymi narzędziami służącymi do tego celu są *Pinger* i *Ws PingPro Pack* (opracowywana jest również wersja *Nmap*). *Pinger* służy wyłącznie do wykonywania operacji *ping*, natomiast *Ws PingPro Pack* oferuje jeszcze dodatkowe funkcje.

Korzystanie z narzędzia ping zazwyczaj nie jest traktowane jako przejaw złych intencji, mających na celu włamanie do systemu. Jednak nadużywanie tego narzędzia może być bardzo irytujące lub nawet szkodliwe. Wystarczy wysyłać to polecenie do każdego urządzenia w sieci klasy C co 30 sekund przez 8 godzin, aby zobaczyć, jak bardzo wpływa to na przepustowość.

5.1.4. Śledzenie trasy

W celu określenia zarysu mapy architektury sieci, sprawdzamy trasy do kilku działających komputerów. Jest to dosyć żmudna praca, ale pomaga zidentyfikować rutery, zapory sieciowe, urządzenia wyrównywania obciążenia oraz inne urządzenia, znajdujące się na obrzeżu badanej sieci. Pozwala również rozpoznać komputery w odrębnych segmentach. Komputery w oddzielnych segmentach mogą być zarządzane przez różne osoby, a ich relacja zaufania może być wykorzystana do włamania się do systemu.

Śledzenie trasy pozwala na określenie drogi, jaką pokonują pakiety ICMP z komputera lokalnego (gdzie wykonywane jest polecenie) do komputera docelowego. Polecenie jest dostępne z wiersza poleceń zarówno w systemie Unix (`traceroute`), jak i Windows (`tracert`). Narzędzie *VisualRoute*, dostępne na platformie Windows, wykonuje tę samą usługę i dodatkowo odwzorowuje uzyskaną trasę na mapie świata (VisualRoute omawiamy w rozdziale 12.).

Przeprowadzamy śledzenie trasy na kilku adresach IP w tym samym bloku adresów klasy C, aby sprawdzić, czy wszystkie pakiety przebywają tę samą drogę. Interesują nas przeskoki mające miejsce bezpośrednio przed naszym celem. Takie przeskoki mogą

reprezentować rutery, zapory sieciowe lub inne bramy. Jeśli przed kilkoma komputerami występuje taki sam przeskok, prawdopodobnie oznacza to ruter lub zaporę. Jeśli za jakimś wspólnym komputerem pakiety ICMP nie są widoczne, także może to oznaczać istnienie zapory lub rutera filtrującego. Wspólny komputer przed zestawem serwerów WWW może być również urządzeniem wyrównywania obciążenia lub serwerem służącym do readresowania odwołań WWW.

Jeśli zauważymy, że niektóre pakiety podążają do pewnych komputerów inną drogą, może to oznaczać, że odkryliśmy nowe bramy do sieci. Dosyć często się zdarza, że segmenty sieci mają kilka połączeń z internetem — o czym nie wiedzą osoby zarządzające tą siecią. Połączenia mogły zostać utworzone przy testowaniu sieci lub dla jakiejś aplikacji, a potem o tym zapomniano. Takie ścieżki często są powodem infiltracji systemu.

5.2. Analiza podatności na atak

Analiza podatności na atak, zwana również wykrywaniem luk w systemach, polega na określeniu, jakie luki w zabezpieczeniach i inne słabe punkty mogą występować w danej sieci. W tym celu sprawdzamy w sieci rozpoznane urządzenia, wyszukując wszystkie otwarte porty i identyfikując działające w tym komputerze systemy operacyjne i aplikacje (razem z numerem wersji, poziomem poprawek — ang. *patch level* — i pakietem Service Pack). Ponadto, porównujemy uzyskane informacje z kilkoma internetowymi bazami danych, zawierającymi dane o słabych punktach, aby ocenić, które z nich mogą mieć zastosowanie w badanej sieci.

W związku z ograniczeniem czasowym, z jakim mamy zwykle do czynienia przy wykonywaniu zlecenia, oraz dużą liczbą komputerów, może okazać się niezbędne skoncentrowanie się tylko na komputerach o znaczeniu krytycznym. Niemniej jednak, jeśli ograniczenie listy jest konieczne, zazwyczaj jest to dokonywane podczas kolejnego etapu działań.



Uwaga: Należy pamiętać, że rezultaty uzyskane po zastosowaniu polecenia ping nie zawsze muszą oznaczać, że komputer jest wyłączony. Dlatego też, jeśli tylko zachodzi podejrzenie, że mamy do czynienia ze skutecznym filtrowaniem lub zabezpieczeniem przed narzędziem ping, zalecane jest przeprowadzenie skanowania portów. Należy raczej ograniczać liczbę skanowanych portów, ponieważ ta operacja zajmuje dużo czasu. Jeśli trzeba ją wykonać dla dużej liczby portów, najlepiej zrobić to w ciągu nocy.

Na zakończenie tej części naszego zadania powinniśmy utworzyć tabelę, zawierającą informacje o wszystkich komputerach, mogących być celem ataku (włączonych i nie), wraz z informacjami o systemie operacyjnym, adresie IP, działających aplikacjach, bannerze oraz znanych słabych punktach. Informacje te będą przydatne na etapie badania systemu, jak również przy prezentowaniu klientowi rezultatów naszej pracy.

5.2.1. Rozpoznawanie systemów operacyjnych

Rozpoznanie systemów operacyjnych pozwala przewidzieć, jakie usługi mogą działać w danym komputerze, a także pozwala dostosować do nich skanowanie portów. Najczęściej używanym narzędziem do rozpoznawania systemów operacyjnych jest *Nmap*. Narzędzie to służy do wykonywania analizy odpowiedzi otrzymywanych od stosu TCP na wysyłane przez nie pakiety. O tym, jak powinien zareagować stos TCP na żądanie, decydują różne dokumenty RFC, niemniej jednak szczegóły implementacji zależą już od dostawców. W związku z tym, różnice w obsłudze dokumentów RFC pozwalają na rozpoznanie dostawcy. Ta metoda nie jest doskonała, ale jest powszechnie uważana za wiarygodną. Zmiana sygnatury systemu operacyjnego w komputerze jest możliwa, ale nie jest sprawą prostą, a z doświadczenia wiemy, że firmy raczej nie korzystają z tej formy zabezpieczenia.

Rozpoznanie systemu operacyjnego stanowi duży krok w kierunku stworzenia wykazu urządzeń w sieci oraz przeprowadzenia skanowania luk. Poznanie systemu operacyjnego pozwala na stworzenie listy potencjalnych luk i słabych punktów — zazwyczaj na podstawie własnej witryny dostawcy. Jeśli wiemy na przykład, że w komputerze zainstalowany jest Windows NT, możemy sprawdzić, czy otwarty jest port TCP 139 i spróbować ustanowić połączenie null connection z udziałem IPC$. Jeśli rozpoznamy system Unix, możemy zacząć szukać portów X Windows (6000 – 6063).

5.2.2. Skanowanie portów

Celem tej operacji jest określenie, czy dany port oczekuje na sygnały, czyli czy jest otwarty. Istnieje szereg metod wykonywania skanowania portów. Przedstawimy tutaj tylko te z nich, które uznaliśmy za najbardziej użyteczne. Najbardziej popularną metodą jest TCP SYN; została ona szczegółowo opisana jest w rozdziale 13., w części poświęconej narzędziu *Nmap*.

Najwięcej informacji można uzyskać przez przeprowadzenie skanowania wszystkich możliwych portów (1 – 65535), ale jest to też działanie najbardziej czasochłonne i naraża nas na wykrycie. Z takiego skanowania korzystają zazwyczaj tylko początkujący hakerzy. Jeśli jednak zdecydujemy się na wykonanie tej czynności, należy robić to etapami, za każdym razem określając mały zakres portów. Z pełnego skanowania korzystamy często na zakończenie naszych prac, gdy już nie zależy nam na włamaniu. Pozwala to określić, jakich usług nie zauważyliśmy podczas skanowania wybranych portów.

Jeśli kwestia wykrycia nie jest tak istotna i chcemy po prostu zidentyfikować słabe punkty w systemie (na przykład gdy personel jest powiadomiony o testach), w takim przypadku można wykonywać skanowanie wszystkich portów naraz. Jednak zajmie to dużo czasu i lepiej jest, gdy możemy analizować wyniki, równocześnie przeprowadzając skanowanie nowych systemów.

Na szczęście jest kilka innych możliwości przeprowadzania skanowania. Można trzymać się tylko podstawowych znanych portów (1 – 1024) i dodać kilka innych (o których wiemy, że mają znaczenie dla klienta), takich jak porty X Windows (6000 – 6063) dla systemu Unix. Odpowiednią listę portów do skanowania w komputerze z systemem

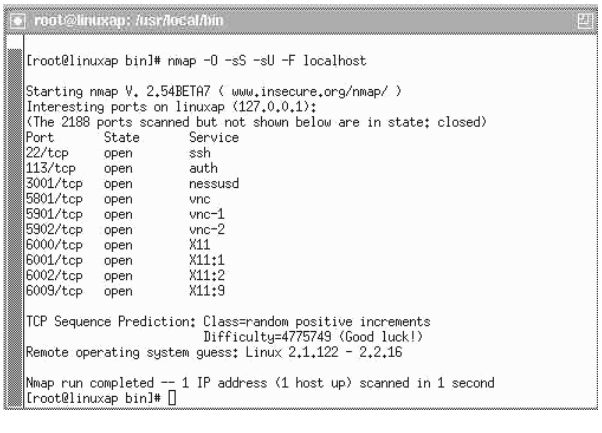
Unix można również uzyskać po przejrzeniu pliku */etc/services*. Można także stworzyć listę portów obsługujących aplikację, której słabe strony znamy i chcemy wykorzystać, na przykład FTP, telnet i RealSecure (odpowiednio: porty 21, 23 i 2998). Większość skanerów umożliwia skanowanie zarówno portów TCP, jak i UDP. Porty UDP są często ignorowane, ponieważ nie są tak powszechne, ale one również mogą być narażone na ataki. W związku z tym, że UDP jest protokołem bezpołączeniowym, wyniki skanowania tych portów są uważane za mniej wiarygodne.

Można także stworzyć listę portów, z których wygodnie korzysta się nam w różnych sieciach i modyfikować ją w sposób odpowiedni dla sieci, której skanowanie przewidujemy. Przykładowo, możemy utworzyć ogólną listę portów i w przypadku badania sieci Unix usunąć porty typowe dla NT. Nmap jest rozprowadzany z listą zawierającą kilka znanych portów, co może stanowić początek listy ogólnej (dodatkowe listy portów można znaleźć na różnych hakerskich witrynach — patrz rozdział 22.). Do listy ogólnej możemy następnie dodawać kolejne porty, w miarę jak dowiadujemy się, że są skojarzone z aplikacją posiadającą znane nam słabe miejsca lub lukę, z której możemy skorzystać. Z listy należy usunąć porty, które nie są związane ze słabymi punktami systemu, lukami czy zbieraniem informacji. Utrzymywanie takiej listy wymaga ciągłego testowania, jednak im więcej prób skanowania portów będziemy wykonywać, tym bardziej przydatne wiadomości uzyskamy.

Jak już wcześniej wspomnieliśmy, w środowisku uniksowym *Nmap* jest najlepszym narzędziem do skanowania portów, jak również wiarygodnym narzędziem do rozpoznawania systemów operacyjnych. Odpowiednimi skanerami portów w systemie NT są *SuperScan* i *7th Sphere*, ale nie umożliwiają rozpoznawania systemów operacyjnych (jak wspomnieliśmy, *Nmap* dla Windows jest w trakcie opracowywania).

W rozdziale 13. dokładnie omawiamy zastosowanie tych narzędzi, dlatego też nie będziemy się tu powtarzać. Przedstawimy jedynie wyniki uzyskane za pomocą narzędzia *Nmap* podczas skanowania portów TCP i UDP w pojedynczym komputerze z systemem Linux — rysunek 5.2.

Rysunek 5.2. *Przykładowe wyniki po użyciu narzędzia Nmap*



Zazwyczaj przed skanowaniem skanery portów wykonują polecenie ping i skanują tylko te komputery, które odpowiedzą na to polecenie. Jeśli mamy jakieś podejrzenia, dotyczące wyników funkcji ping, można ustawić skanery w takich sposób, aby skanowały również komputery, które nie reagują na ping. Skanowanie będzie jednak trwać dłużej.

Już od dawna kwestią dyskusyjną jest sprawa legalności wykonywania skanowania portów. Niektórzy profesjonaliści porównują skanowanie do jazdy ulicą i obserwowania, które okna są otwarte. Jednak skanowanie portów bez zezwolenia jest niewątpliwie działalnością nieetyczną i zawsze będzie odczytywane jako sygnał o zbliżającym się ataku.

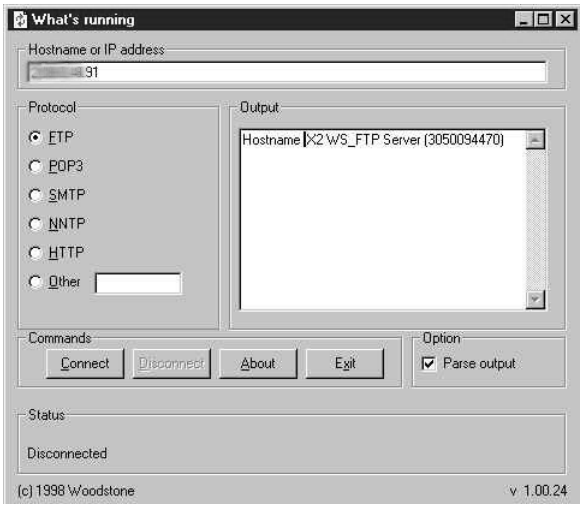
5.2.3. Wykaz aplikacji

Po skanowaniu portów otrzymujemy listę otwartych portów w badanych komputerach. To, że port jest otwarty, nie oznacza, że wskazuje, która usługa jest aktywna. Porty poniżej 1024 zostały przydzielone do różnych usług i jeśli są otwarte, z reguły wiadomo czemu służą. Niektóre aplikacje już od tak długiego czasu działają na określonych portach, że stało się to praktycznie standardem. Tak jest na przykład w przypadku portu 65301 dla *pcAnywhere* czy 26000 dla *Quake*. Oczywiście administratorzy mogą zmieniać porty w celu ukrycia usługi (jest to przykład zabezpieczenia przez niejawność). Dlatego też należy połączyć się z otwartym portem i przechwycić banner, aby sprawdzić działającą tam usługę.

Wiedza o tym, jakie aplikacje działają w komputerze, bardzo pomaga w dokonaniu analizy podatności systemu na atak. Podobnie jak w przypadku systemu operacyjnego, w internecie możemy odnaleźć listę znanych słabych punktów i narzędzi ataku dla żądanych aplikacji — często z witryn samych dostawców.

Z tworzeniem wykazu aplikacji wiąże się przechwytywanie bannera. Podczas uruchamiania niektórych aplikacji (między innymi telnetu, FTP, HTTP, SNMP i wielu innych) na ekranie logowania wyświetlane są informacje o ich wersji. Taka informacja zwana jest bannerem i jest bardzo przydatna w rozpoznawaniu działających aplikacji. Z reguły rejestrujemy wszystkie bannery, jakie napotkamy w trakcie przeprowadzania testów penetracyjnych. Można to zrobić za pomocą wielu aplikacji, takich jak *netcat*, która działa z wiersza poleceń systemu Unix czy Windows; telnet i *What's Running*, narzędzia bazującego na graficznym interfejsie użytkownika Windows. Narzędzie to przedstawione jest na rysunku 5.3. Szerzej opisano je w rozdziale 12.

Rysunek 5.3. *Okno programu What's Running*



Zaletą programu *What's Running* jest to, że banner jest umieszczany w oknie, z którego można go skopiować do pliku lub edytować.

5.2.4. Przeszukiwanie internetu

Gdy już znamy listę aplikacji, możemy przystąpić do jej sprawdzenia pod kątem istniejących słabych punktów aplikacji. W miarę przeprowadzania testów penetracyjnych, nabierzemy doświadczenia i poznamy pewne popularne luki w zabezpieczeniach, dzięki czemu będziemy mogli szybko określić, czy dana aplikacja jest podatna na ataki. Należy jednak pamiętać, że codziennie pojawiają się informacje o nowych lukach i powinniśmy sprawdzać w bazach danych, czy nie ma czegoś nowego, dotyczącego aplikacji, usługi czy systemu operacyjnego, objętego naszym aktualnym zleceniem.

W rozdziale 22. zamieściliśmy listę witryn internetowych, na których można znaleźć bazy danych ze słabymi punktami. Najpopularniejszymi listami są: Bugtraq, Packetstorm (*www.packetstormsecurity.org*) i SecurityFocus (*www.securityfocus.com*). Z czasem nabierzemy wprawy w korzystaniu z tych i innych witryn, umożliwiających szybkie wyszukiwanie słabych punktów. Niektóre zamieszczane tam informacje powielają się, jednak warto sprawdzać wiele witryn, ponieważ żadna z nich nie obejmuje wszystkiego w pełni. Każda witryna ma swoich użytkowników i informatorów, którzy uaktualniają bazy danych.

Po rozpoznaniu słabych punktów i umieszczeniu ich w tabeli, możemy pobrać kod programu, służącego do ataku (jeśli taki ma zastosowanie), aby skorzystać z tego kodu w następnej części testów penetracyjnych.

5.3. Wykorzystywanie słabych punktów

Następnym krokiem po określeniu listy słabych punktów jest przejście do ich wykorzystania w celu spróbowania uzyskania dostępu do badanego systemu z poziomu użytkownika root lub administratora.

Ogólna procedura jest częściowo wynikiem zbierania informacji i tworzenia wykazu. Sprawdzamy listę znanych słabych punktów i potencjalnych luk w zabezpieczeniach różnych komputerów i określamy, które z nich mogą być łatwym celem. Następnie staramy się je wykorzystać do uzyskania dostępu do badanego systemu z poziomu użytkownika root.

Pierwszymi celami ataku są otwarte porty i aplikacje podatne na ataki. Najpierw przeglądamy utworzoną poprzednio listę słabych punktów i układamy ją według prawdopodobieństwa odniesienia sukcesu oraz wyrządzenia ewentualnych szkód w sieci. Przykładowo, przepełnienie bufora lub atak DoS mogą być skuteczne, ale zarazem bardzo niebezpieczne dla systemu. Ataki DoS można wykonywać tylko wtedy, gdy w zleceniu wyraźnie jest zaznaczona potrzeba ich przeprowadzenia.

Bardzo popularną metodą jest przeprowadzanie ataku na serwer WWW. Jest to coraz powszechniej stosowana metoda przeniknięcia do atakowanej sieci. Jednym z często używanych narzędzi ataku jest Microsoft IIS MDAC/RDS, służące do wykorzystania serwera WWW IIS za pomocą pliku *msadc.cll* oraz usługi RDS (ang. *Remote Data Service*). Narzędzie to pozwala włamywaczowi na wykonanie w atakowanym komputerze pojedynczego polecenia. Z tego polecenia można skorzystać ponownie wówczas, kiedy chcemy zastosować serię pojedynczych poleceń, które razem mogą być użyte dla osiągnięcia różnych celów, takich jak pobranie poufnych plików z atakowanego komputera i ustanowienie połączenia z innymi komputerami. Użycie dodatkowo polecenia ntuser pozwala użytkownikowi na uzyskanie miejsca w lokalnej grupie administratorów.

Do zdalnego wykorzystania tego słabego miejsca może posłużyć powszechnie dostępny skrypt napisany w Perlu, *msdacExploit.pl* (plik ten nie jest jedynym, który do tego służy), kodowany przez hakera *rain-forest puppy*. Aby zastosować omawiany skrypt, wystarczy wydać następujące polecenie (nie musimy być na dysku C):

```
C:\> per; -x msdacExploit.pl -h <atakowany komputer>
```

Na ekranie naszego komputera powinien pojawić się znak zachęty wiersza poleceń atakowanego komputera. Znak ten umożliwia wykonanie jednego polecenia. Aby można było wykonać kilka poleceń, trzeba kilka razy uruchomić ten program.

Po uzyskaniu nieuprawnionego dostępu do systemu zdalnego, dzięki możliwości wydania polecenia w atakowanym komputerze bądź przez bezpośredni dostęp do rzeczywistego konta użytkownika, natychmiast musimy zapisać wszystkie istotne informacje, czyli nazwę komputera i katalogu lub udziału, do którego uzyskaliśmy dostęp, nazwę komputera, z którego uzyskaliśmy dostęp, datę i godzinę oraz poziom dostępu. Musimy również opisać lukę, przez którą udało nam się ten dostęp uzyskać. Następnie powinniśmy przekazać te informacje badanej organizacji. Służy to dwóm celom — po pierwsze, organizacja zostaje poinformowana o zidentyfikowanych lukach, dzięki czemu może zająć się tym problemem, a po drugie, zabezpieczamy się przed ewentualnymi konsekwencjami prawnymi. Nawet w przypadku niezapowiedzianych testów powinniśmy poinformować osobę, która wie o prowadzonych testach, że uzyskaliśmy dostęp, aby po wykryciu naszej działalności sprawa nie trafiła do sądu.

Uzyskanie dostępu do jednego komputera nie musi jeszcze oznaczać zakończenia testów penetracyjnych. Jeśli zakres zlecenia jest szerszy, możemy teraz zainstalować zestaw narzędzi, umożliwiających przeprowadzanie testów innych systemów z zaatakowanego komputera. Nasz zestaw narzędzi różni się od zestawu używanego przez hakerów. Zestaw hakerów służy do powtórnego włamania się do tego samego systemu w przyszłości (przez utworzenie tylnego wejścia lub pozostawienie konia trojańskiego) czy też do wykonania ataków na inne komputery, na przykład przez atak DDoS.

Zestaw narzędzi konsultanta jest dostosowany do systemu operacyjnego atakowanych komputerów, jakie możemy spotkać podczas testów penetracyjnych. Zazwyczaj zestaw ten obejmuje takie narzędzia jak *netcat*, programy do łamania haseł, oprogramowanie do zdalnego sterowania, sniffery i narzędzia do pozyskiwania informacji. Często, co wynika z charakteru połączenia, lepsze są narzędzia wiersza poleceń. Jeśli zainstalowany jest program zdalnego sterowania, na przykład *pcAnywhere* czy *Virtual Network Computing* (VNC), można korzystać z narzędzi graficznego interfejsu użytkownika. W przeciwnym

przypadku możemy mieć kłopoty, gdy badany komputer będzie odsyłał graficzny interfejs użytkownika do naszego komputera i interfejs zostanie zablokowany przez zaporę sieciową lub przez sam komputer. Badany komputer może ponadto czasami wyświetlać ten interfejs na ekranie i użytkownik będzie ostrzegany o naszych poczynaniach.

Zestaw narzędzi można skopiować za pomocą protokołu FTP lub TFTP. Po zainstalowaniu zestawu możemy rozpocząć testowanie kolejnych komputerów. Od tego momentu testowanie przebiega podobnie jak w przypadku testowania systemu od wewnątrz, ponieważ już znajdujemy się w badanej sieci. W rozdziale 7. zamieściliśmy więcej informacji o tym, jak postępować przy testowaniu dodatkowych systemów.

Wśród narzędzi, które powinniśmy umieścić w zestawie, są sniffery i narzędzia służące do odczytywania znaków wprowadzanych z klawiatury, pomocne w przechwytywaniu ruchu w sieci. Poszukujemy zwłaszcza nazw użytkowników i haseł, umożliwiających uzyskanie dostępu do innych komputerów, systemów modemowych i czekających na sygnał usług w sieci. Sniffery są szerzej opisane w rozdziale 14.

Warto wypróbować również narzędzia zdalnego sterowania, które mogą pomóc w sterowaniu systemem. Po przejęciu jednego komputera otwierają się przed nami rozległe możliwości dalszej penetracji sieci. Możemy przechwycić plik haseł Unix (wraz z zapasowym plikiem haseł) lub rejestr systemu Windows (często dzięki wersji przechowywanej w katalogu zawierającym informacje naprawcze) w celu uzyskania haseł wszystkich użytkowników urządzenia lub nawet konta administratora, co prawdopodobnie umożliwi nam uzyskanie dostępu do innych komputerów w sieci. Narzędzia zdalnego sterowania i ich zastosowanie zostały opisane w rozdziale 18.

Instalujemy zatem wszystkie narzędzia, które mogą nam być pomocne w wykorzystaniu zaatakowanego systemu jako platformy do atakowania innych systemów. Należy jednak pamiętać, co i gdzie umieszczamy, aby po zakończeniu testów można było przywrócić system do stanu wyjściowego.

Studium przypadku: Komputery dołączone jednocześnie do dwóch sieci

Jak już wspomnieliśmy w rozdziale 4., komputery dołączone jednocześnie do dwóch sieci mogą być przyczyną powstania poważnej luki w zabezpieczeniach sieci, ponieważ mogą pozwolić użytkownikom, posiadającym prawo dostępu i uprawnienia w jednej sieci lub domenie, na uzyskanie praw i uprawnień, jakich nie powinni mieć w innej domenie. Taka sytuacja może zaistnieć wówczas, gdy komputer stacjonarny jest podłączony do wewnętrznej sieci LAN i równocześnie połączony jest przez modem do lokalnego dostawcy usług internetowych. W przypadku takiej konfiguracji istnieje możliwość uzyskania dostępu do sieci przedsiębiorstwa z internetu przez połączenie telefoniczne. Ten rodzaj podatności na atak może jednak wystąpić również przy innych konfiguracjach.

Przykładowo, naszym klientem był kiedyś dostawca usług internetowych, który prowadził również serwery WWW dla kilku tysięcy przedsiębiorstw. Korzystał do tego z setek komputerów z systemem Unix, o identycznej konfiguracji, na których działały serwery Netscape.

Dostawca usług internetowych nie prowadził pełnego zarządzania, jego zadaniem była obsługa komputerów, natomiast serwerami WWW zarządzali sami klienci.

Pakiet usługi obejmował język skryptowy tcl, umożliwiający zdalne zarządzanie serwerami WWW. Dostawca usług internetowych nie zdawał sobie sprawy z tego, że wykorzystując język skryptowy tcl, dobrze zorientowani klienci, a nawet osoby odwiedzające witryny WWW, mogą prowadzić działalność, do której z pewnością nie powinny być uprawnione. Wykorzystanie serwera WWW, działającego z uprawnieniami użytkownika root, umożliwiało uzyskanie dostępu z takimi uprawnieniami do komputerów za pomocą różnych specjalnie opracowanych adresów URL. Jest to przykład ataku na serwer WWW, polegający na wykorzystaniu niepełnej lub niewłaściwej weryfikacji wprowadzanych danych.

Taki układ doprowadził do infiltracji komputera centralnego. Podobne skutki może wywołać nieodpowiednie skonfigurowanie serwera Microsoft IIS.

Okazało się jednak, że wyżej opisana możliwość infiltracji komputera nie była największą luką w badanej sieci.

Po udanym ataku na komputer w sieci zawierającej serwery WWW (na przykład po uzyskaniu dostępu użytkownika root) można było zainstalować w tym komputerze odpowiedni zestaw narzędzi, a wśród nich narzędzia do łamania haseł. Gdy już uzyskaliśmy dostęp użytkownika root w jednym komputerze, mogliśmy zaobserwować, że sieć była połączona z inną siecią, używaną do obsługi różnych systemów handlowych przedsiębiorstwa dostawcy usług internetowych. Co więcej, odkryliśmy, że niektórzy użytkownicy sieci z serwerami WWW mieli konta również w tej drugiej sieci i korzystali z tych samych haseł.

W tym momencie nie było żadnych problemów z uzyskaniem dostępu do drugiej sieci, ponieważ istniały konta z tą samą nazwą użytkownika i tym samym hasłem w obu sieciach, dzięki czemu można było ponownie skopiować i zainstalować zestaw narzędzi.

Następnie odkryliśmy, że jeden z komputerów w tej drugiej sieci był połączony z trzecią siecią. Była to sieć wewnętrzna, używana do obsługi księgowości, utrzymywania bazy danych klientów i innych bardzo cennych informacji. Ta sieć miała funkcjonować jako niezależna sieć wewnętrzna. Przez pomyłkę był do niej podłączony jeden komputer. Udało się go odnaleźć dzięki odkryciu, że miał dwie karty NIC z adresami IP należącymi do dwóch różnych zakresów adresów. Dlatego też konta użytkownika (i konto użytkownika root) tego komputera uprawniały do działania w obu sieciach. Jak można się było spodziewać, konto użytkownika root miało to samo hasło we wszystkich komputerach drugiej sieci, w związku z czym uzyskaliśmy dostęp użytkownika root do wewnętrznej, głównej sieci organizacji.

Podsumowując, możliwe było uzyskanie dostępu użytkownika root do komputera w sieci, zawierającej serwery WWW, przy wykorzystaniu oprogramowania istniejącego na samych tych serwerach. Możliwe było również przejście do drugiej sieci przez konta użytkownika, posiadające te same nazwy i hasła. Odkrycie podwójnego połączenia pozwoliło uzyskać nieuprawniony dostęp do wewnętrznej sieci przedsiębiorstwa. Można powiedzieć, że w związku z uzyskaniem ważnego prawa dostępu, dostęp ten nie był już nieuprawniony, ponieważ mechanizm kontroli dostępu nie wstrzymał go lub nie rozpoznał jako nieuprawniony.

W momencie, gdy członkowie zarządu przedsiębiorstwa zorientowali się, że jeden z komputerów w prywatnej sieci wewnętrznej był podłączony do sieci, która była połączona ze światem zewnętrznym, rujnując w ten sposób integralność i poufność krytycznych dla przedsiębiorstwa danych i informacji o klientach, byli, co zrozumiałe, wstrząśnięci i zażenowani.

Wniosek

Niejednokrotnie spotkaliśmy się z sytuacjami, w których pewne organizacje nie były świadome tego, że istniały w nich komputery podłączone do dwóch sieci lub że celowo używano podwójnego połączenia jako łatwego rozwiązania, pozwalającego uniknąć kłopotów z komunikacją (realizowaną przez zapory sieciowe) między pewnymi aplikacjami. Z opisanego powyżej przykładu wyraźnie widać, że należy bardzo dokładnie sprawdzać architekturę sieci. Po projektowaniu i wdrażaniu bezpiecznej architektury, obejmującej zarówno konfigurację komputerów, jak i całościową topologię sieci, wszelkie wprowadzane zmiany muszą być kontrolowane przez odpowiedni mechanizm, aby uniknąć powstawania takich błędów, jak istnienie komputerów o podwójnym połączeniu, umożliwiających włamanie się do sieci.