

ポートスキャン実習

2002年9月19日

修士1年

兼子 譲

牧之内研究室「インターネット実習」Webページ
<http://www.db.is.kyushu-u.ac.jp/rinkou/internet/>

ポートスキャンとは

- メッセージを送った際の応答を元にコンピュータが提供しているネットワークサービスを探査
 - ネットワークサービスの稼動有無
 - 稼動しているネットワークサービスサーバのバージョン確認
- サーバ内で動作しているアプリケーションソフトやOSの種類を調べ、侵入口となりうる脆弱なポートがないかどうか調べる行為

ポートスキャン実験用のソースプログラム

(<http://kane/rinkou/scan/portscan.c>)

```
#include <sys/types.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

#define SERV_HOST_ADDR "192.168.33.33" ← 対象サーバのIPアドレス
#define MAXPORT 1024
#define BUFLen 1024
#define SBUFLen 256

int main(int argc, char **argv)
{
    struct sockaddr_in addr;
    struct servent *serv;
    int fd, i, j, rtn, n;
    char buf[BUFLen];

    for (i = 1; i < MAXPORT; i++) {
        /* ソケットの準備 */
        fd = socket(AF_INET, SOCK_STREAM, 0);

        memset((char *)&addr, 0, sizeof(addr));
        addr.sin_family = AF_INET;
        addr.sin_addr.s_addr = inet_addr(SERV_HOST_ADDR);
        addr.sin_port = htons((short)i);

        /* サーバとの接続 */
        if ((rtn = connect(fd, (struct sockaddr *)&addr, sizeof(addr))) == -1) {
            //printf("e");
            close(fd);
            continue;
        }
        /* サービス名の取得 */
        if ((serv = getservbyport(htons(i), "tcp")) == NULL) {
            printf("unknown service (port %d) is available.\n", i);
        } else {
            printf("%s\tservice (port %d) is available.\n", serv->s_name, i);
        }
        close(fd);
    }
}
```

telnetコマンドによる実験(1)

FTPサービスへのアクセス例

```
%telnet lana 21 "21"はFTPのポート番号
Trying 192.168.33.33...
Connected to lana.4f.db.is.kyushu-u.ac.jp.
Escape character is '^]'.
220 lana FTP server (SunOS 5.8) ready.
quit
221 Goodbye.
Connection closed by foreign host.
%
```

telnetコマンドによる実験(2)

HTTPサービスへのアクセス例

```
%telnet hatsune 80      "80"はHTTPのポート番号
Trying 133.5.18.167...
Connected to hatsune.db.is.kyushu-u.ac.jp.
Escape character is '^]'.
GET / HTTP/1.0
[ENTER]
HTTP/1.1 200 OK
Date: Wed, 18 Sep 2002 05:41:36 GMT
Server: Apache/1.3.26 (Unix)
Last-Modified: Wed, 08 May 2002 10:44:00 GMT
ETag: "18b4d1-bef-3cd94a0d"
Accept-Ranges: bytes
Content-Length: 3055
Connection: close
Content-Type: text/html
(省略)
Connection closed by foreign host.
%
```

実習

- ポートスキャンプログラムを実行
 - ソースは/u/kane/rinkou/scan/portscan.c
 - 研究室外のマシンにポートスキャンを試みることは**マナー違反**となるので、研究室内のマシンに対してのみ実験
- 稼動しているサービスに対してtelnetでアクセスしてみる(ただし、アクセスする前にそのプロトコルがどのようなものかを調べておく)

ポートスキャン(Nmap)

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 843. 844. 845. 846. 847. 848. 849. 850. 851. 852. 853. 854. 855. 856. 857. 858. 859. 860. 861. 862. 863. 864. 865. 866. 867. 868. 869. 870. 871. 872. 873. 874. 875. 876. 877. 878. 879. 880. 881. 882. 883. 884. 885. 886. 887. 888. 889. 890. 891. 892. 893. 894. 895. 896. 897. 898. 899. 900. 901. 902. 903. 904. 905. 906. 907. 908. 909. 910. 911. 912. 913. 914. 915. 916. 917. 918. 919. 920. 921. 922. 923. 924. 925. 926. 927. 928. 929. 930. 931. 932. 933. 934. 935. 936. 937. 938. 939. 940. 941. 942. 943. 944. 945. 946. 947. 948. 949. 950. 951. 952. 953. 954. 955. 956. 957. 958. 959. 960. 961. 962. 963. 964. 965. 966. 967. 968. 969. 970. 971. 972. 973. 974. 975. 976. 977. 978. 979. 980. 981. 982. 983. 984. 985. 986. 987. 988. 989. 990. 991. 992. 993. 994. 995. 996. 997. 998. 999. 1000.

Nmapとは

- ポートスキャンをするプログラム
- insecure.orgが提供している

Nmapの使用方法

- # nmap [Scan Type(s)] [Options] <host or net list>
 - Scan Type
 - -sT :TCPスキャン
 - -sU :UDPスキャン
 - Options
 - -O :OSを調べる
 - -p :ポート番号の指定
 - -v :スキャン中の様子を表示

- オプションによってはrootでしか実行できない

Nmapの使用例

- # nmap -sU -O ami
 - amiのUDPポートをスキャンする
 - OSを調べる

- # nmap -p 20-25 '192.168.33.*'
 - 20番から25番までのTCPポートをスキャンする
 - 192.168.33のネットワーク全体のコンピュータをスキャンする

実行結果

```
tei# nmap -O ami.db.is.kyushu-u.ac.jp

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on ami.db.is.kyushu-u.ac.jp (133.5.18.197):
(The 1545 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open   ftp
22/tcp    open   ssh
23/tcp    filtered telnet
53/tcp    open   domain
111/tcp   open   sunrpc
139/tcp   open   netbios-ssn
1021/tcp  open   unknown
1022/tcp  open   unknown
1023/tcp  open   unknown
1024/tcp  open   kdm
6000/tcp  open   X11
Remote operating system guess: FreeBSD 4.3 - 4.4-RELEASE

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
tei#
```

Nmapのインストール方法

- 以下のページからファイルをダウンロードする
 - http://www.insecure.org/nmap/nmap_download.html
- FreeBSDではportsが用意されています
 - `cd /usr/ports/security/nmap`
 - `make install`

実習上の注意点

- ポートスキャンはサーバに対する攻撃方法の1つ
- ポートスキャンされた側はポートスキャンを行ったホストを悪意のあるホストとして認識する可能性がある
- 必ず**研究室内のマシンに対してのみ**実験を行う