3T-5

TCP のフラグを用いたポートスキャンの検出法

鈴木和明　岡部吉彦　後藤滋樹
早稲田大学大学院 理工学研究科 情報・ネットワーク専攻

概要

ポートスキャンとは、あるホストのポートが使用されているかどうかを調べる行為である。管理者がそれをを管理目的で行うことは容認される。クラッカー（攻撃者）がポートスキャンを行うのは不正な行為であり、不正侵入の事前行為であることが多い。クラッカーは開いているポートを見つけ、そのポートに対して攻撃・侵入を試みる。従ってポートスキャンを検知することは侵入を事前に察知することに役に立つ。本研究は、観測対象をネットワークの応答パケット、さらにその TCP フラグに絞る。この方法によって軽量な侵入検出を実現することができる。ポートスキャンを効率的にいち早く検出することは、侵入・攻撃を未然に防ぐことにつながる。

1　ポートスキャンの検出

1.1　データ収集

本論文では、早稲田大学の対外接続点において 2004 年 1 月 17 日に収集したデータを対象に分析を行った。時間帯を 4 つに分け、各時間帯それぞれ 2 時間ずつ収集し解析を行った。

1.2　検出法

本論文では UDP ではなく TCP によるポートスキャンの検出を行う。学内のネットワークを対象としているために、学外から学内に対するポートスキャンを検出の対象とする。TCP ポートスキャンでは、標的ポートが閉じている場合一般的に RST（リセット) フラグがオンになったパケットが標的ホストから返される。一方、ポートが開いている場合には、SYN パケットに対して SYN/ACK が標的ホストから返される。ポートスキャンをする側（スキャナー）はこれらの応答によってポートの状態を調べる。TCP ポートスキャンには様々な方法がある。しかしどのポートスキャン方法においても標的ホストの反応として次のことが共通している。開いたポートに SYN パケットが来た場合は SYN/ACK を返す。それ以外のパケットが来た場合は何も返さないか、RST フラグがオンになったパケットを返す。

本研究では 2 つの方法によりポートスキャンを検出する。1 つ目は、IDS として有名な Snort[8] によるものである。このポートスキャンの検出法は、あるホスト (学外) からあるネットワーク (学内) に対して

「S 秒間に N 個以上のポートにアクセス」

があったものをポートスキャンとするものである。これを本論文では方法 1 とする。ここで N 個以上のポートという点に注意が必要である。例えばホスト A の 80 番ポートとホスト B の 80 番ポートは、同じ 80 番ポートでも別のものとして数える。これは以下の方法 2 においても同様である。

本論文における検出法（方法 2）では、標的ホストからの RST と SYN/ACK パケットに注目し、あるネットワーク (学内) からあるホスト (学外) に対して

「S 秒間に N 個以上のポートから RST または SYN/ACK」

が返されたものをポートスキャンの候補とする。S, N の値は自分で設定する。SYN/ACK も含む理由は、開いているポートに対してポートスキャンが行われた場合も考慮するためである。しかしこれだけでは通常の通信もポートスキャンとして検出してしまう場合がある。以下のような条件を付け加える。

1. 学外ホストへのすべてのパケットは RST を含む
2. 学外ホストのポート番号がウェルノウンポートである
3. 学内ホストのポート番号がウェルノウンポートでない

この 3 つすべてを満たす事象はポートスキャンとして検出する必要がないため除外する。方法 2 では以上の条件に合致するものをポートスキャンとして検出する。

2　実験結果

表 1: 3 秒間に 4 ポート以上

	9–11 時	13–15 時	18–20 時	2–4 時
方法 1	8	16	17	13
方法 2	14	26	25	12
応答なし	3	4	1	3
方法 1 と方法 2 の一致	5	12	16	10
方法 1 − 応答なし	5	12	16	10

$S = 3$, $N = (4, 5, 6)$ として実験を行った結果を示す。表中の数字は、ポートスキャンとして検知した数を表す。方法 1 と方法 2 の一致とは、それぞれがともに検出したポートスキャンの数である。表中の「応答なし」とは、方法 1 で検出されたポートスキャンのうち、学内からの応答がなかった、あるいは、応答があったとしても、閾値 N を超えなかったものである。これらは、ファイアウォールによっ

表 2: 3 秒間に 5 ポート以上

	9–11 時	13–15 時	18–20 時	2–4 時
方法 1	4	12	15	11
方法 2	7	11	16	9
応答なし	1	2	1	3
方法 1 と方法 2 の一致	3	10	14	8
方法 1 − 応答なし	3	10	14	8

表 3: 3 秒間に 6 ポート以上

	9–11 時	13–15 時	18–20 時	2–4 時
方法 1	3	11	14	10
方法 2	3	10	15	7
応答なし	1	1	1	3
方法 1 と方法 2 の一致	2	10	13	7
方法 1 − 応答なし	2	10	13	7

てフィルタされた、あるいは受け取ったホストが何も返さなかったといった原因が考えられる。したがって方法 2 では検出不能である。そこで、この数を方法 1 から引いた数字を表中に載せてある。

表 4中の内、外はそれぞれ学内、学外を表す。また S/A は SYN/ACK の意味である。

3 評価

本実験では、比較評価の対象として Snort を用いた。Snort は監視するネットワークに入ってくるパケットを処理する。今回のポイントは、より少ないパケットでポートスキャンを検出することである。方法 2 で対象とするパケット数は、学外へ出て行くすべての TCP パケットをさらに絞り込んだ RST+SYN/ACK パケットである。表 4より、それらのパケット数が非常に少なくて済むのがわかる。方法 2 では、応答パケットを見ているために、応答がない、あるいはそれが閾値 N を超えないスキャンは検出することができない。しかしそれらを方法 1 から除外したポートスキャンはすべて方法 2 でも検出できる。

S 秒間に N 個以上のアクセスがあったポートスキャンについては、応答パケット (RST+SYN/ACK) のみを処理することでも検出できている。しかし、表 1からわかるとおり、方法 2 は方法 1 よりも多く検出している。これは応答パケットとして RST だけではなく SYN/ACK も同じように扱ったことが原因である。つまり 3 秒間に 4 ポート以上から SYN/ACK が返されるということは、通常の TCP 通信の中で起こりうる。これは RST と SYN/ACK の応答パケットのみをみているために開いたポートにスキャンをしてきた場合と区別することができなかった。

表 4: 対象としたパケット数

パケット	9–11 時	13–15 時	18–20 時	2–4 時
TCP (外→内)	12,957,400	38,918,093	20,105,859	31,150,049
TCP (内→外)	14,124,509	36,054,079	19,634,578	29,088,381
RST (内→外)	72,045	131,370	109,651	52,525
S/A (内→外)	114,997	162,372	171,217	91,069

4 まとめ

本研究による方法では検出できなかったポートスキャンがあり、さらにわずかながら誤検知があった。このように従来の方法よりも劣る点はあるものの、全く違った方法かつ少ないパケット数でここまで検出できることがわかった。ポートスキャンは今回扱った典型的なパターンだけとは限らない。あらゆる種類のポートスキャンの検出を検討する必要がある。また、ポートスキャンの検出は、IDS における機能の 1 つに過ぎない。IDS の負荷および不正侵入の検知に対し、今後も様々なアプローチ方法を検討したい。

参考文献

[1] 岡部 吉彦: 『ICMP を用いた侵入検知システムの負荷軽減』, 早稲田大学理工学部 2002 年度卒業論文, 2003

[2] W・ Richard Stevens 著, 橘 康雄 訳, 井上 尚司 監訳: 『詳解 TCP/IP Vol.1』, ピアソン・エジュケーション, 2000.

[3] W・ Richard Stevens 著, 徳田 英幸 訳, 戸辺 義人 監訳: 『詳解 TCP/IP Vol.2』, ピアソン・エジュケーション, 2000.

[4] W・ Richard Stevens 著, 篠田 陽一 訳: 『UNIX ネットワークプログラミング』, Prentice Hall, 1996.

[5] David Tansley 著, 服部由美子 訳:『Linux & UNIX Shell Programing』, ピアソン・エデュケーション, 2003.

[6] CERT, “the CERT Coordination Center (CERT/CC) “, http://www.cert.org/

[7] CERT, “JPCERT コーディネーションセンター “, http://www.jpcert.or.jp/

[8] Snort.org, “open source network intrusion detection system”, http://www.snort.org/

[9] Jon Postel, “Transmission Control Protocol”, RFC793, September 1981.

[10] Insecure.org, “Nmap Security Scanner”, http://www.insecure.org/nmap/

[11] SANS, “The Trusted Source for Computer Security Training, Certification and Research”, http://www.sans.org/

[12] Fyodor, “The Art of Port Scannig”, http://www.insecure.org/nmap/nmap_doc.html