

IDS検知能力検証

1. 検証IDSスペック

IDS製品名		Snort 1.8.3
開発元		snort.org
Hardware	ハードウェア名称	HP NetServer Ip1000r(PIII/1000モデル)
	プロセッサ(種別/搭載個数)	Intel Pentium-III 1GHz (x1)
	2次キャッシュ	256KB
	搭載メモリ	256+256MB(合計512MB)
	HDD (容量/転送形式)	Ultra3 SCSI HDD 18.2GB (x1)
	FD	3.5inch 2モード(740KB, 1.44MB対応)(x1)
	CD-ROM	最大24倍速 IDE (x1)
	NIC1 (攻撃検出用ポート)	Intel pro/1000XT (100Mbps動作)
	NIC2 (コントロール用ポート)	内蔵 Intel 82559 10/100TX (100Mbps動作)
	その他の特記事項	特になし
Software	オペレーションシステム	Kondara Linux 2.1 (Kernel 2.4.18)
	IDSソフトウェア	Snort 1.8.3
	検知ポート用NIC ドライバー等	汎用(libpcap)デフォルトインストール
	シグネチャデータベース	上記付属
	有効な設定シグネチャ数及び判断	シグネチャ数として977個が有効になっていることを確認
	その他備考	TCPフラグメントとIPフラグメントに対応するように設定を変更 (frag2とstream4プリプロセッサを有効化)。その他のパラメータ等は特に変更なし(インストール時のデフォルト)。

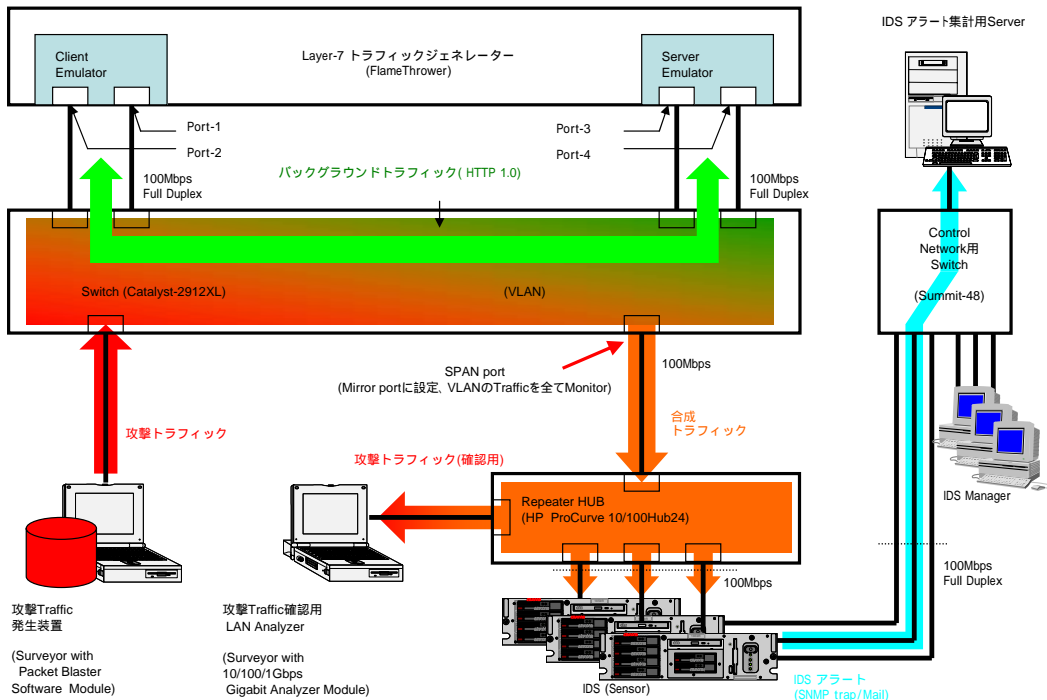
2. バックグラウンドトラフィックジェネレーター (FlameThrower)の設定パラメーター

Emulateする機能	パラメーター	内容	
HTTP Client	FrameThrowerポート	Port -1*注	Port -2*注
	使用MAC アドレス	機器Default MAC アドレス(固定)	機器Default MAC アドレス(固定)
	使用IP アドレス	192.168.3.131 ~ 192.168.3.167 (ラウンドロビン方式で変動)	192.168.3.192 ~ 192.168.3.223 (ラウンドロビン方式で変動)
	アプリケーションプロトコル	HTTP 1.0	HTTP 1.0
	使用Port	tcp/1024 ~ tcp/65535 (ラウンドロビン方式で変動)	tcp/1024 ~ tcp/65535 (ラウンドロビン方式で変動)
	HTTP Request先アドレス	192.168.3.2	192.168.3.7
	HTTP Request 速度	3.HTTP Request速度の項を参照	3.HTTP Request速度の項を参照
HTTP Server	FrameThrowerポート	Port -3*注	Port -4*注
	使用MAC アドレス	機器Default MAC アドレス(固定)	機器Default MAC アドレス(固定)
	使用IP アドレス	192.168.3.2(固定)	192.168.3.7(固定)
	アプリケーションプロトコル	HTTP 1.0	HTTP 1.0
	使用Port	tcp/80(固定)	tcp/80(固定)
	ClientダウンロードHTMLファイルの 大きさ・内容	機器Defaultの32KByte ランダムキャラクターファイル	機器Defaultの32KByte ランダムキャラクターファイル

*注)テストベンチ構成図参照

3. HTTP Request速度(バックグラウンドトラフィック速度)

No.	HTTP Request 速度(Request/sec)			バックグラウンドトラフィック速度 (Mbps)
	Port-1 to Port-3	Port-2 to Port-4	合計	
0	2	2	4	1.2
1	8	8	16	5
2	15	15	30	10
3	33	33	66	20
4	50	50	100	30
5	65	65	130	40
6	83	83	166	50
7	100	100	200	60



参考図: テストベンチ構成図

4. Snort 1.8.3 定性検証結果

- 出展 1 Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Thomas H.Ptacek, Timothy N.Newsham, Secure Networks, Inc. January, 1998
 2 SideStepによるEVASIONテスト(<http://www.robertgraham.com/tmp/sidestep.html>)
 3 その他

出展	No	テスト名称	操作の概要	本検証におけるIDSの動作期待値	検証結果	出展	No	テスト名称	操作の概要	本検証におけるIDSの動作期待値	検証結果
1	1	baseline-1	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。	検知	検知 *注1)	1	21	tcbc-1	TCP 3WHは完了させないが、あたかもある任意のTCP 3WHが完了したかの様に、連続した1バイト単位に分割されたTCPデータセグメントを送出する。	非検知	非検知
1	2	baseline-2	TCPの3WH終了後、テストストリングを1キリャクター単位のTCPデータセグメントに分割し、順番に送出する。	検知	検知	1	22	tcbc-2	TCPの3WH終了後、同一パラメータを持つSYNパケットを挿入した、1バイト単位に分割された連続したTCPデータセグメントを送出する。	検知	検知
1	3	frag-1	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを8バイト単位に分割し、IPフラグメントパケットとして順番に送出する。	検知	検知	1	23	tcbc-3	TCP 3WHは完了させず、ランダムなSequence番号をもつ任意のデータストリームを送出。その後同じコネクションパラメータを使用した正しい接続を行う。	検知	検知
1	4	frag-2	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを24バイト単位に分割し、IPフラグメントパケットとして順番に送出する。	検知	検知	1	24	tcbt-1	TCPの3WH終了後、すぐさまRSTパケットによってコネクションを終了させる。その後Sequence No.を急激に変えて(最初の3WHと同じパラメータで接続し、連続した1バイト単位に分割されたTCPデータセグメントを送出する)。	検知	検知
1	5	frag-3	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを8バイト単位に分割し、IPフラグメントパケットとして送出する。但し、この時IPフラグメントパケットの1つを順番に逆にする。	検知	検知	1	25	tcbt-2	TCPの3WH終了後、1バイト単位に分割されたTCPデータセグメントを送出する。但し送信中にRSTパケットを送信し、コネクションを切断する(但し、残りのデータを送り続ける)。	非検知	非検知
1	6	frag-4	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを8バイト単位に分割し、IPフラグメントパケットとして順番に送出する。但し、この時1つの重複したIPフラグメントパケットを混入する。	検知	検知	1	26	insert-1	TCPの3WH終了後、1バイト単位に分割された連続したTCPデータセグメントを送出する。但しこれらのIP checksum値は不正な値とする。	非検知	非検知
1	7	frag-5	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを8バイト単位に分割し、IPフラグメントパケットとして送出する。但し、この時送出はランダムにし、かつ1つの重複したIPフラグメントパケットを混入する。	検知	検知	1	27	insert-2	TCPの3WH終了後、1バイト単位に分割された連続したTCPデータセグメントを送出する。但しこれらのTCP checksum値は不正な値とする。	非検知	非検知
1	8	frag-6	TCPの3WH終了後、テストストリングを含むTCPデータセグメントを8バイト単位に分割し、最初に最後のIPフラグメントであるビットを立てたパケットを送信。その後それ以前に送られるべきIPフラグメントパケットを送出する。	検知	検知	1	28	insert-3	TCPの3WH終了後、1バイト単位に分割された連続したTCPデータセグメントを送出する。但しこれらのAck Bitはセットされていないものとする。	検知 *注5)	検知 *注5)
1	9	frag-7	TCPの3WH終了後、8byteの無関係なデータストリングを送信。その後、そのデータストリングをForward-Over lapするテストストリングを含む1byteのデータを送信する。	検知 *注2)	非検知 *注2)	3	29	apbase-1	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する(baseline-1とは別のパターン・Web evade用)。	検知	検知 *注6)
1	10	tcp-1	TCPの3WH終了後、対象ホストが一時的ネットワークから切断されている状態をSimulateする。その後、テストストリングを含むTCPデータセグメントを1バイト単位で送付する。	状況による *注3)	全て非検知 *注4)	3	31	appevade-2	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合のコンテンツはUnicodeエンコードされたものとする。	検知	検知
1	11	tcp-2	TCPの3WH終了後、SequenceNo.を0に戻すセグメントを含む、1バイト単位のTCPデータセグメントを送出する。	検知	非検知	3	30	appevade-3	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合のコンテンツは、不正な方法でUnicodeエンコードされたものを使用する。	検知	検知
1	12	tcp-3	TCPの3WH終了後、重複したデータセグメントを含む、1バイト単位に分割されたTCPデータセグメントを送出する。	検知	検知	3	32	appevade-4	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合冗長な"/"を付加する。	検知	*注7)
1	13	tcp-4	TCPの3WH終了後、重複したデータセグメントを含む、1バイト単位に分割されたTCPデータセグメントを送出する。但しこの場合の重複したセグメントの内容は異なるものとする。	検知	検知	3	33	appevade-5	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合"/"を付加する。	検知	非検知
1	14	tcp-4-1	TCPの3WH終了後、重複したデータセグメントを含む、1バイト単位に分割されたTCPデータセグメントを送出する。但しこの場合の重複したセグメントの内容は異なるものとする(tcp-4の逆検証)。	非検知	非検知	3	34	appevade-6	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合のデータストリングのDirectory表記は"/"を含むものとする。	検知	非検知
1	15	tcp-5	TCPの3WH終了後、"h"を"x"で置換したデータセグメントを送出。その後"x"を"ph"でForward over lapする。	検知 *注2)	非検知 *注2)	3	35	appevade-7	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合のデータストリングは大文字を含めて送信する。	検知	検知
1	16	tcp-6	TCPの3WH終了後、1バイト単位に分割されたTCPデータセグメントを送信する。但し送信中にSequence No.を1000増加させる。	非検知	非検知	3	36	appevade-8	TCPの3WH終了後、単一のTCPデータセグメントでテストストリングを送出する。但しこの場合のデータストリングは".//XXX//."等とする(XXXは任意)。	検知	検知
1	17	tcp-7	TCPの3WH終了後、1バイト単位に分割されたTCPデータセグメントを送出する。但し送信中にSequenceNo.を急激に変化させた(不正な)同じコネクションを挿入する。	検知	検知	2	37	appevade-R1	RPC Requestを複数のRcord Fragmentに分割して送信する(RPC protocol LevelのEvasion)	検知	*注8)
1	18	tcp-8	TCPの3WH終了後、1バイト単位に分割された連続したTCPデータセグメントを送出する。但し送信中に順番のくるったセグメントを一つ挿入する。	検知	検知	2	38	appevade-F1	FTP requestに制御用文字を挿入して送信する(FTP Protocol LevelのEvasion)	検知	検知
1	19	tcp-9	TCPの3WH終了後、1バイト単位に分割された連続したTCPデータセグメントを送出する。但しセグメントは完全にランダムな順番で送信する。	検知	検知	2	39	appevade-D1	DNSのVersion Bind リクエストにオフセットを指定したCompression Nameを使用する(DNS protocol levelのEvasion)	検知	非検知
3	20	tcp-10	TCPの3WH進行中にRSTパケットを送信するが、その後連続した1バイト単位に分割されたTCPデータセグメントを送出する。	検知	検知	2	40	appevade-S1	SNMP Query に不正マスクを使用する(SNMP protocol levelのEvasion)	検知	非検知

*注1) "Web-CGI.php access"として検知

*注2) 本検証では後着データが優先されるOSを使用して、実際に攻撃が成立したトラフィックを使用した為"検知"としてある。但し、本検証はIDSの設定(先着データ優先/後着データ優先)に設定されているかに依存するものである。

*注3) オリジナルの論文では"非検知"であるが、その評価は考慮を必要とする

*注4) 当該攻撃を特定回数繰り返し、全て検知しなかった

*注5) オリジナルの論文では"非検知"となっているが、本検証では実際にサーバに対する攻撃が成功している為"検知"とした。本検証項目の結果の妥当性については検討が必要である。

*注6) "WEB-MISC /etc/passwd"として検知

*注7) "Web CGI Scriptaris Attack"として規定回数検出。"WEB-MISC /etc/passwd"として検知はしなかった。

*注8) "RPC Portmap listing"として検出。但し、この結果のみではEvasionに対応しているのかは判断不可能であった。

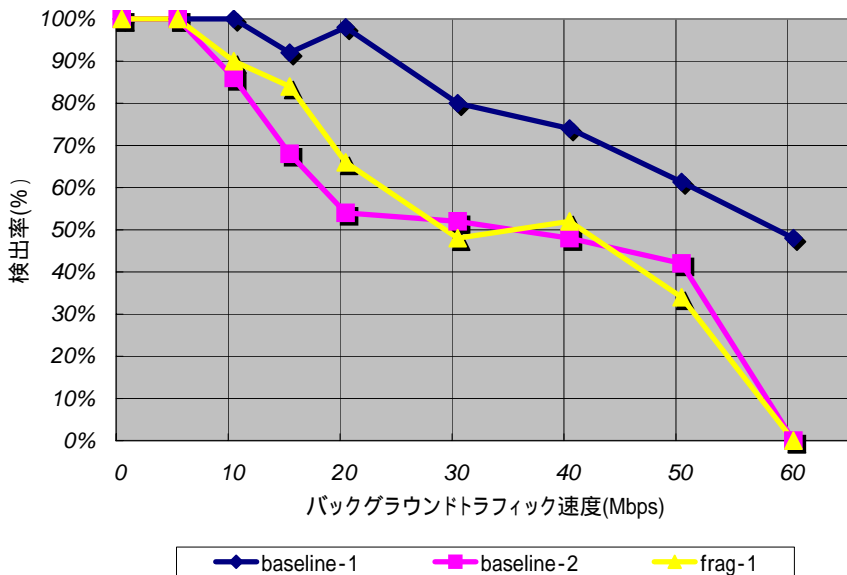


5. Snort 1.8.3 定量検証結果

*定量検証の実施方法:

1. 攻撃トラフィックは定性検証において使用した、各々のトラフィックを使用した。
2. 各テストにおいて62秒間隔で、同一攻撃トラフィックを25回送信、IDSにて検知した回数を測定した。

No	検証速度 (Mbps)	検証結果	baseline-1			baseline-2			frag-1		
			検出数	有効 攻撃回数	%	検出数	有効 攻撃回数	%	検出数	有効 攻撃回数	%
1	0Mbps (負荷なし)	Test 1	25	25	100.0%	25	25	100.0%	25	25	100.0%
		Tset 2									
		Test 3									
		合計	25	25	100.0%	25	25	100.0%	25	25	100.0%
2	5Mbps	Test 1	25	25	100.0%	25	25	100.0%	25	25	100.0%
		Tset 2									
		Test 3									
		合計	25	25	100.0%	25	25	100.0%	25	25	100.0%
3	10Mbps	Test 1	25	25	100.0%	21	25	84.0%	22	25	88.0%
		Tset 2	25	25	100.0%	22	25	88.0%	23	25	92.0%
		Test 3									
		合計	50	50	100.0%	43	50	86.0%	45	50	90.0%
4	15Mbps	Test 1	23	25	92.0%	17	25	68.0%	21	25	84.0%
		Tset 2									
		Test 3									
		合計	23	25	92.0%	17	25	68.0%	21	25	84.0%
5	20Mbps	Test 1	25	25	100.0%	11	25	44.0%	15	25	60.0%
		Tset 2	24	25	96.0%	16	25	64.0%	18	25	72.0%
		Test 3									
		合計	49	50	98.0%	27	50	54.0%	33	50	66.0%
6	30Mbps	Test 1	21	25	84.0%	13	25	52.0%	10	25	40.0%
		Tset 2	19	25	76.0%	13	25	52.0%	14	25	56.0%
		Test 3									
		合計	40	50	80.0%	26	50	52.0%	24	50	48.0%
7	40Mbps	Test 1	20	25	80.0%	10	25	40.0%	12	25	48.0%
		Tset 2	17	25	68.0%	14	25	56.0%	14	25	56.0%
		Test 3									
		合計	37	50	74.0%	24	50	48.0%	26	50	52.0%
8	50Mbps	Test 1	16	25	64.0%	11	25	44.0%	11	25	44.0%
		Tset 2	16	25	64.0%	10	25	40.0%	6	25	24.0%
		Test 3	14	25	56.0%						
		合計	46	75	61.3%	21	50	42.0%	17	50	34.0%
9	60Mbps	Test 1	12	25	48.0%	0	25	0.0%	0	25	0.0%
		Tset 2									
		Test 3									
		合計	12	25	48.0%	0	25	0.0%	0	25	0.0%



バックグラウンド トラフィック 速度(Mbps)	baseline- 1 検出率 (%)	baseline- 2 検出率 (%)	frag-1 検出率 (%)
0	100.0%	100.0%	100.0%
5	100.0%	100.0%	100.0%
10	100.0%	86.0%	90.0%
15	92.0%	68.0%	84.0%
20	98.0%	54.0%	66.0%
30	80.0%	52.0%	48.0%
40	74.0%	48.0%	52.0%
50	61.3%	42.0%	34.0%
60	48.0%	0.0%	0.0%