2007－CSEC－37 (11)
2007／5／25

不正PCを検出・無力化するシステムについての検討

猿田 智勇† 大西 克実†† 中野 秀男††

企業ネットワークのセキュリティ侵害は,その多くが内部の人間により行われている.
本稿では,不正なホストを検出するシステムと,無力化するシステムを組み合わせ,検疫ネットワークに準ずるシステムを安価に構成する検討を行った.

Study of Detection and Inactivation System for illegal PC.

Toshio Saruta† Katsumi Onishi†† Hideo Nakano††

Almost security violation were cause by right user in his consciousness/inconsciousness.
In this research, we exermine the net system based on open-source software,
that detect and inactivate the illegal PCs in low cost.

1.はじめに

この数年,外部からのセキュリティ侵害より,むしろ内部からの侵害が問題となっている.その対策としてUTM,(総合脅威管理)アプライアンス等の機器を用いたゲートウェイ近辺での検知や,ホストベースファイアウォールの適用を強制する方法がある.その一方で,セキュリティ侵害には様々な要因が考えられ,自宅PCの持ち込みのような意図的な侵害の他,SSL経由や,暗号化アーカイブファイルの取得のような,検出や保護が困難なものが増加している.

また,セキュリティリスクの顕在化から実際のインシデント発生までの時間差が短くなり,セキュリティパッチのリリースよりしばしば先に攻撃コードが到着・感染を広げるゼロデイアタックが時々発生している.

セキュリティ対策方法として,検疫ネットワークは有力な選択肢の一つである.しかし,その導入に当たっては,ネットワーク・システム構成を大幅に更新する必要がある.また,現在運用LANに既に接続されているが,IDSやFirewallをすりぬけたウィルス/ワームや,USBメモリ等で人為的に持ち込まれたウィルス/ワームの侵入を防ぐことは困難であるため.ネットワークの挙動によって異常を振り分ける,「ビヘイビア型アクセス制御」について各種検討が行われているが,発展途上である.[1][2][3]

前回の発表[4]では,ARP spoofingを利用したPCの無力化について検討を行い,標的となったホストを速やかに無力化する方法を確立した.続いて本稿では,既存の,オープンソースプロダクトを中心とした検知システムを用い,安価で,ネットワーク・システム構成を変更することなく導入できるシステムの設計・試験を行った.

2.検討したシステム

今回検討したシステムは,オープンソースソフトウェアで構成した検出系に,同じくオープンソースソフトウェアのARP spoofingによるホスト無力化を組み合わせたものであり,セキュリティ侵害の発生後,二次被害を予防することを主目的としている.

2.1 システム構成

本システムは,以下のホスト・ネットワークにより構成される.(図1)

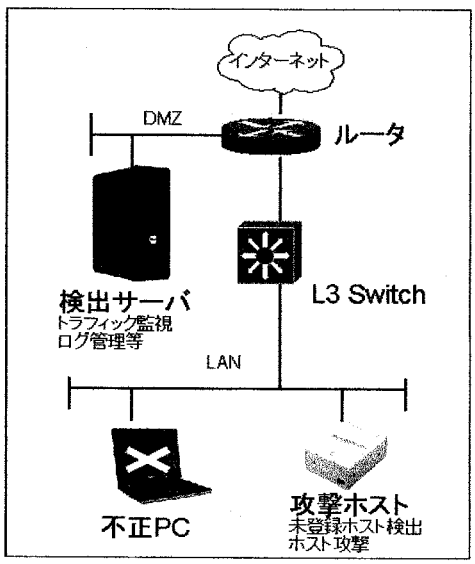

図1 システム構成
Fig.1 System overview

○ 検出サーバ
DMZに配置する.IDSによるネットワークトラフィック監視およびログ管理を行う.
また,攻撃ホストに対する攻撃指示を行う.

○ 攻撃ホスト
LANごとに配置する.登録外PCの検出・無力化を行い,検出サーバからの指示によりホスト無力化を行う.

○ 不正PC
各種セキュリティリスクを有するPC.
不正の検知・無力化の対象となる.

○ ルータ/L3スイッチ
試験環境でDMZとLANを分離する.

2.2 防御ポリシー

本システムで検出する対象は以下の通りとする.

表1 検出・無力化ポリシー
Table1 Detection/Inactivation policy

観測対象	検出方法
未登録PCの無許可での接続 / ARPspoof・ARP cache poisoning対策	未登録IPアドレス:MACアドレスの検出・無力化
セキュリティホール検出 問題のあるアプリケーションの利用	脆弱性診断(VA*) ホストベースIDS**(HIDS) ネットワークIDS(NIDS)
ネットワークトラフィック異常検出 ウィルス・ワーム感染	ネットワークIDS(NIDS)

* VA(Vulnerability Assessment)
** IDS(Intrusion Detection System)
***試験環境構成
○ 検出サーバ
DELL PowerEdge SC430
(Celeron 2.66GHz/Memory 512MB)
OS CentOS4
○ 攻撃ホスト
自作PC (Celeron 1.1AMHz/Memory 512MB)
OS FreeBSD6.2
○ 不正PC
Victor Interlink xv631
(MobileCeleron 866MHz/Memory 768MB
OS Windows XP Home

2.3 問題検出時の対応

問題を検出した場合,攻撃ホストは不正PCに対し,ARP spoofing攻撃を行う.

ARP spoofingには,適宜2種類のツールを利用する.

未登録ホストを検出した場合IP Sentinelを利用し,IDS等により検出された場合はarpspoofを利用する.攻撃の内容はログとして検出サーバに送られ,管理者に通達される.

管理者は,ログから状況を確認し,状況確認の上,問題となったホストをネットワークより切り離し,対応を行う.

3.試験環境

図1に準じたシステムを構築し,以下の各種ツールを導入した.

表2に,各種ツールの概略を示す.

表2 利用ツール一覧
Table2. List of illegal PC detection tools

ツール名(導入箇所)	概略
Nessus [6] (検出サーバ)	オープンソースVAツール.ネットワーク内部をポーリングし,ポリシーに従ってセキュリティホールを有するホストを検知する.
OSSEC [7] (検出サーバ)	オープンソースのホストベースIDS. PCにエージェントを導入することで,詳細な分析を行う.
Snort [8] (検出サーバ)	オープンソースのネットワークIDS. シグネチャ検出および異常値検出を行う.
IP Sentinel [9] (攻撃ホスト)	MACアドレス/IPアドレスの登録情報に従い,未登録のMACアドレスに対して無力化を行う.
Arpspoof (dsniff)[10] (攻撃ホスト)	セキュリティツールキットdsniff[10]の1アプリケーション.コマンドにて,標的となるIPアドレス/MACアドレスに対してARP spoofing攻撃を行う.

検出サーバでは,トラフィックを監視する一方でログサーバを動作させ,攻撃ホストからの情報を取得した.

3.1 試験1:未登録ホストの接続

IP Sentinelが参照するMACアドレス:IPアドレスの対比表一覧に該当しないPCをネットワークに接続し,挙動を確認する.

3.2 試験2:ARP Spoofingによるなりすまし検出

PCにてARP Spoofingを利用してルータのIPアドレスを偽装し,ネットワークトラフィックのスニフィングを試みた際,ルータのMACアドレスが書き換わったKernel Messageを監視して,攻撃元ホストに対する無力化を確認した.

3.3 試験3:セキュリティパッチ未適用ホストの接続

特定のセキュリティパッチを外したPCをネットワークに接続し,Nessusによる検出および,攻撃ホストによる無力化を確認した.

脆弱性持つ Windows PC のモデルとして，Windows2000 Professional ホストより Security Rollup Package を除外した PC を準備した．

モデル PC のセキュリティホールをスキャンした結果,セキュリティホールが発見された場合は無力化を行うこととした．

また,Snort の設定は,以下の Web サイトを参考にした．[11][12]

3.4 試験 4:不正アプリケーション利用ホスト

クライアント PC による不正アプリケーションの利用を検出し,無力化を行った．

不正アプリケーション利用のモデルとしてポートスキャンツールおよび Winny について調査を行った．

3.5 試験 5:Mass Mailing Worm

Mass Mailing Worm 感染のモデルを作成し,トラフィック監視による感染 PC の検出および攻撃ホストによる無力化を確認した．

Mass Mailing Worm は一般的に活動時に大量の DNS クエリーを発生させることが知られているため[5],本調査ではモデル系として,DNS および SMTP に対して急激に負荷をかけた．

4. 試験結果

4.1 試験 1 未登録ホストの接続

前回の調査にて報告したように,未登録の MAC アドレスを持つ PC が接続された時点で,速やかに無力化された．

これは IP Sentinel の基本機能であり,5 回の試行で,それぞれ 1 秒未満で無効化されたことを確認した．

4.2 試験 2 ARP spoofing によるなりすまし検出

ARP spoofing による ARP テーブルの変化を IP-sentinel が検出し,無力化した．

以下にその際のログを示す．

IP アドレス 192.168.0.10 の PC の ARP に対して架空の MAC アドレスを返答している．

```
@40000000463e7b541a85fa60:
192.168.0.10/aa:aa:aa:aa:aa:aa                    >-
192.168.0.10/0:0:0:0:0:0 [1:80:c2:0:0:1]
```

図 2 ARP spoofing によりホストを無効化したログ
Fig.2 Detection and Inactivation by ARP spoofing

4.3 試験 3 セキュリティパッチ未適用ホストの接続

Nessus による完全テスト実施時の所要時間は,1 ホストあたり 3 分～4 分であった．

以下に,Windows PC に対する試験にて検出された脆弱性の一覧を示す．

```
-bash-2.05b$ cat results.txt |grep Vulner
. Vulnerability found on port epmap (135/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port microsoft-ds (445/tcp) :
. Vulnerability found on port blackjack (1025/tcp) :
. Vulnerability found on port epmap (135/udp) :
```

図 3 検出された脆弱性
Fig.3 Detected vulnerability of Windows PC

検出後,速やかに標的ホストは無力化された．

4.4 試験 4: 不正アプリケーション利用ホスト

不正 PC からポートスキャン実行時,Snort(IDS)が異常を検出した.以下にログの一部を示す.不正 PC192.168.0.10 のランダムなポートから,192.168.0.254 の各種ポートに対してスキャンを行っている状況が確認されている．

```
May  7 06:37:52 192.168.0.10:2332 -> 192.168.0.254:1297 SYN ******S*
May  7 06:37:52 192.168.0.10:2333 -> 192.168.0.254:1296 SYN ******S*
May  7 06:37:52 192.168.0.10:2335 -> 192.168.0.254:1423 SYN ******S*
May  7 06:37:52 192.168.0.10:2336 -> 192.168.0.254:1428 SYN ******S*
May  7 06:37:52 192.168.0.10:2337 -> 192.168.0.254:1234 SYN ******S*
May  7 06:37:52 192.168.0.10:2338 -> 192.168.0.254:1236 SYN ******S*
May  7 06:37:52 192.168.0.10:2339 -> 192.168.0.254:1231 SYN ******S*
May  7 06:37:52 192.168.0.10:2340 -> 192.168.0.254:1235 SYN ******S*
May  7 06:37:52 192.168.0.10:2341 -> 192.168.0.254:1291 SYN ******S*
May  7 06:37:52 192.168.0.10:2334 -> 192.168.0.254:1294 SYN ******S*
```

図 4 Snort のポートスキャン検出ログ
Fig.4 Portscan detection log of Snort

4.5 試験 5: Mass Mailing Worm

試験 4 と同様,Snort が DNS トラフィックの異常を検出した．

以上の結果を,試験別にまとめたものが表 3 である．

試験 1,2,4,5 は,すみやかに異常を検知し,無力化を行った.試験 3 はセキュリティホール対応であり,他のセキュリティ問題と比較して,比較的緊急度は低いため,十分な能力を持っていると考えられた．

表 3 結果
Table3 Results

試験別	時間	検出ツール
試験 1	1 秒未満	IP Sentinel
試験 2	1 秒未満	IP Sentinel
試験 3	3 分～4 分	Nessus
試験 4	1 秒～5 秒	Snort/OSSEC
試験 5	1 秒未満	Snort

5.まとめ

オープンソースソフトウェアを利用したIDS,VAによるネットワーク監視システムを構築し,ARP spoofing攻撃ツールと組み合わせることで,検疫ネットワークに準ずる形式の,比較的セキュアな環境を構築し,試験を行った.その 結果,試験環境レベルでは各種セキュリティ侵害に対抗する能力を有することを確認した.

実際に運用を想定した場合,IP Sentinel,OSSECはネットワークに常駐させておき,Nessusを定期的に実行することが好ましいと考えられる.

また,PCはOSSECエージェントを導入することで,安全性を高められると考えられた.

今後,実用システムを想定した運用環境を構築する場合には,IDSポリシーのカスタマイズ,LAN内のネットワークノード台数が増加した際の挙動変化,ARP spoofingパケットの最適値等,環境と規模に応じたポリシーの調整が必要となると考えられた.

また,今回は試験の範囲外であったが,複数のネットワークのうちのひとつにウィルス・ワーム等の大量感染が発生した場合は,ルータに対する無力化も行うことで,ゼロデイ攻撃時でも大量感染や,外部に対する二次被害を防ぐことが可能と考えられた.

参考文献

[1]瀬林克啓,明石修, 丸山充:集約したユーザポリシを用いた攻撃防御方法の提案, 信学技報 2006, 113-118

[2]八木毅, 大倉一浩, 田邉正雄, 村山純一,外山勝保:信学技報 2006, p119-124

[3]寺田真敏, 枝村和茂, 高橋正和, 有村浩一:2007CSEC-36, p89-93

[4]猿田 智勇, 大西 克実,中野 秀男: ネットワークポリシーに従わないPCの無力化に関する検討, コンピューターセキュリティシンポジウム2006 p311-314

[5] 武蔵 泰雄,杉谷 賢一,松葉 龍一: Mass Mailing Wormと DNS/SMTPトラフィック解析,情報処理学会研究報告, 2002-CSEC-19, pp19-24 (2002)

[6]Nessus
http://www.nessus.org/

[7]OSSEC
http://www.ossec.net/

[8]Snort
http://www.snort.org/

[9]IP Sentinel
http://www.nongnu.org/ip-sentinel

[10]arpspoof (dsniff)
http://www.monkey.org/~dugsong/dsniff/

[11]Snortで侵入検出
http://www.hawkeye.ac/micky/network/snort.html

[12]日本Snortユーザ会
http://www.snort.gr.jp/