

IPネットワーク機器の脆弱性を検査し、  
モニタ、レポート可能なサービスアナライザ

# Mu-8000

企業にとって、提供しているサービスの可用性は非常に大きな問題です。しかし、サービスは常にDDoS攻撃、ゼロディアタックなどを含む多種多様な攻撃に晒されているため、可用性を維持するためのコストは増大し続けています。Mu-8000はそうした多種多様な攻撃を擬似し、独自に生成することで脆弱性を発見し、サービスを維持するために必要な対策を行うための情報をレポートします。

## 特徴

- 独自に開発された機器攻撃パケット生成エンジンが、バッファオーバーフローなど潜在的な脆弱性を900万を超える攻撃パターンで検証
- DDoS攻撃を生成し、DDoS攻撃環境下でのサービスの可用性を検証
- 公開されたパッチなどの正常性を確認するため、問題の攻撃パターンをダウンロードしての検証が可能
- TELNET,SSH,コンソール,SNMP,電源のコントロールなどを利用し、試験対象装置を自動設定、動作をロギング
- 全試験を通じて、問題のあった時点のキャプチャデータ、応答時間を含む統合的なレポート機能
- インターネット経由での最新攻撃パターの自動更新のサポート

Mu-8000には大きく以下の4つの機能があります

### SLTV (Service Level Traffic Variation) アナリシス

・バッファオーバーフロー、パースエラーなどを引き起こす900万通りの攻撃パケットを生成、対象機器に攻撃を行い、レポートを作成します。

### DDoS攻撃

・DDoS攻撃をシミュレートし、攻撃環境下でのサービスの応答時間をレポートします。

### PVA (Published Vulnerability Attack)

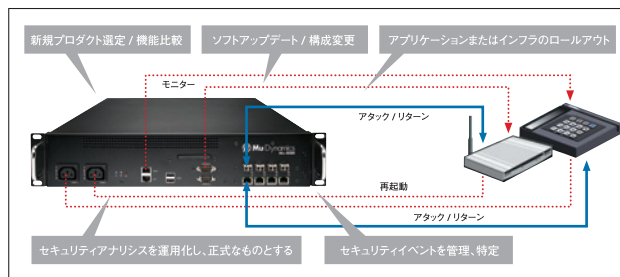
・既知の脆弱性に対するパッチの確認を行います。

### シナリオ攻撃

・Mu Studioでパケットキャプチャファイルを元に作成したシナリオを使用して攻撃パケットを生成、対象機器に攻撃を行い、レポートを作成します。

## SLTV (Service Level Traffic Variation) アナリシス

独自の生成エンジンによる攻撃パターンを利用し、潜在的な脆弱性を検証します。バッファオーバーフロー、エスケープ文字、2バイトコード、各要素の有無など様々な潜在的脆弱性の存在をプロトコル毎に検証を行います。そのパターン数は、プロトコル毎に数万通りに及び、Mu8000全体では約900万通りもの攻撃パターンをサポートします。新しい機器の開発、導入時のみならず、ソフトウェア更新時などに試験を自動化し脆弱性をレポートします。

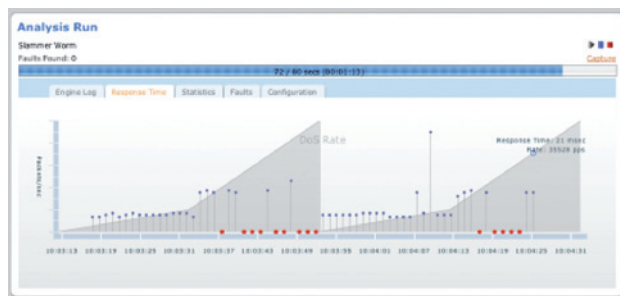


### SLTV アナリシスサポートプロトコル

ARP	IMAP	POP3	SSL/TLS
BGP	IPv4	Portmap	SUNRPC
BOOTP	IPv6	PPPoE	SUNRPC-Portmapper
CDP	IS-IS	RADIUS	SUNRPC-STATd
CIFS	ISAKMP	RADIUS-Cisco	RADIUS-Microsoft
DHCP	LDAP	RADIUS-JuniperNetworks	TACACS+
DHCPv6	LDP	RIPng	TCP
DNP3	LLDP	RIPv1	TELNET
FTP	MGCP	RIPv2	TFTP
H.323	MMS	RTSP	UDP
HTTP	MODBUS/TCP	SMTP	
ICMPv4	MOUNT	SNMP	
ICMPv6	OSPFv2	SNMPTRAP	
IEEE802.1X	OSPFv3	SSDP	
IGMP	PIM-SM/DM	SSH	

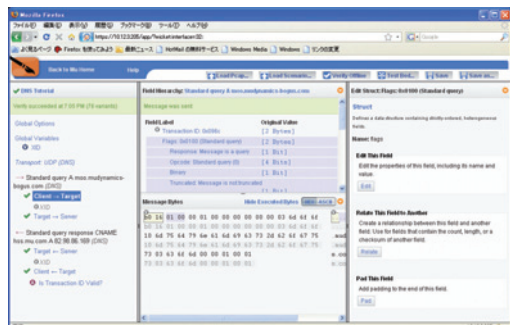
## DDoS 攻撃

攻撃パターのデータをキャプチャデータを元にIPアドレス、ユーザIDなどの内部の一部データを変更しながら再生することで、DDoS攻撃を擬似することが可能です。Mu-8000では、DDoS攻撃を行うのみでなく攻撃トラフィックの負荷パターンを変えながら正常なパケットへの応答時間も合わせて確認することでサービスの可用性に対する検証を行うことが可能です。



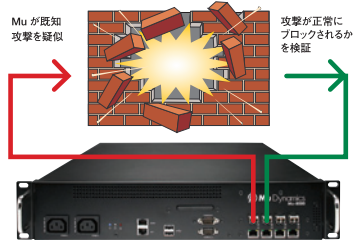
## シナリオ 攻撃

Mu Studioを使用することで、パケットキャプチャ (pcap) ファイルを元に新規のシナリオを作成することができます。作成したシナリオを使用して、SLTVアナリシスと同じように独自の生成エンジンによる攻撃パターンを利用した攻撃を行い脆弱性を検証します。カスタマイズされたシナリオを作成することで、幅広い環境に対応した試験を行うことが可能です。



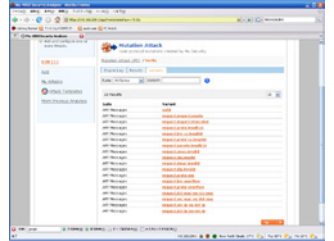
## ■ PVA (Published Vulnerability Attack)

PVAでは、すでに公開されている脆弱性への攻撃パターンを再生することで、ファイアウォール、IPS、IDSなどのセキュリティ機器が正常に攻撃パケットを検出、ブロックできるかどうかを検証します。攻撃パターンはほぼ1月に一度の周期で更新され最新のパッチが正常に動作しているかどうか、セキュリティ機器が新しい攻撃をブロックできるかどうかを検証することができます。



## ■ レポート

Muでの攻撃の結果は、レポートとして統合的に出力され、同時に攻撃時に発見された問題点は攻撃時のキャプチャデータのみならず、Linux上で動作する攻撃パターン再生プログラムとしても出力されます。



## ■ Mu Dynamics 構成部品リスト

### 1: プラットフォーム & モジュール

パートNo.	品名
SYS-M80-V1	Mu-8000 シャーシ 8GbE (4copper + 4SFP) ベースMuOSライセンス + プロトコルライセンス (CDP, VRRP, IPv4, TCP, UDP, ICMP, TFTP, DHCP, IEEE 802.1Q and ARP)
SW-MUOS-V20-DOS	Denial of Service モジュール
SUBS-MUST-M-1Y	Mu Studio

### 2: プロトコル

全プロトコルライセンス	
SW-T123-FULL-1Y	全プロトコルライセンス (Tier 1 & Tier 2 プロトコル全て)
プロトコル・アラカルト (Tier 1 & 2 リスト参照)	
SW-T1-1PK-1Y	1 × Tier 1 プロトコル
SW-T2-1PK-1Y	1 × Tier 2 プロトコル
SW-T3-1PK-1Y	1 × Tier 3 プロトコル
プロトコル・ソリューション・パッケージ	
SW-SOLN-VOIP1-1Y	VOIP-1 (SIP, MGCP, RTP/RTCP)
SW-SOLN-VOIP2-1Y	VOIP-2 (SIP, MGCP, RTP/RTCP, H248, H323)
SW-SOLN-IMS1-1Y	IMS-1 (SIP, IKEv2, H248, RTP/RTCP, HTTP)
SW-SOLN-IPTV1-1Y	IPTV-1 (IGMPv3, PIMSM/DM, RTSP, SIP, HTTP)
SW-SOLN-INDC1-1Y	インダストリアル・コントロール (DNP-3, MODBUS, IEC 61850)
SW-SOLN-STOR1-1Y	ストレージ-1 (CIFS, NFS, FTP, IKEv2, ISAKMP)
SW-SOLN-RTNG1-1Y	ルーティング-1 (BGP, OSPF, VRRP, Static MPLS, LDP, IS-IS)
SW-SOLN-ADM1-1Y	管理-1 (SNMP, SSH, HTTP, Telnet, SSL/TLS)
SW-SOLN-DAT1-1Y	データサービス (VPLS, MPLS, BGP, LDP)

### 3: Published Vulnerability Analysis

SW-MUOS-PVA-1Y	PVA (Published Vulnerability Analysis)
----------------	----------------------------------------

- プラットフォーム及び各種プロトコルライセンスのレンタル (各月単位) も可能です。

■ 記載の内容および仕様は予告なしに変更されることがあります。

### 4: プロトコル & Tiers

Tier 1 プロトコル:
•Cisco Discovery Protocol (CDP)
•File Transfer Protocol (FTP)
•HyperText Transfer Protocol (HTTP)
•IEEE 802.1X
•Internet Group Management Protocol (IGMP) v1, v2, v3
•Internet Message Access Protocol (IMAP)
•Label Distribution Protocol (LDP)
•Link Layer Discovery Protocol (LLDP - IEEE 802.1AB)
•Media Gateway Control Protocol (MGCP)
•MODBUS/TCP
•Post Office Protocol (POP3) v3
•PPP over Ethernet (PPPoE)
•Protocol Independent Multicast (PIM) - SM and DM
•RADIUS
•Routing Information Protocol (RIP) v1, v2 and ng
•Simple Mail Transfer Protocol (SMTP)
•Simple Network Management Protocol (SNMP) v1, v2c, v3 and SNMP Trap
•Stream Control Transfer Protocol (SCTP)
•Simple Service Discovery Protocol (SSDP)
•TACACS+
•Virtual Router Redundancy Protocol (VRRP)
•Telnet
•MPLS (Static LSPs)
Tier 2 プロトコル:
•Border Gateway Protocol (BGP) v4
•Common Internet File System (CIFS)
•Distributed Network Protocol (DNP-3)
•Diameter
•H.248
•H.323
•IEC 61850 Protocol for sub-station automation
•Intermediate System to Intermediate System Protocol (IS-IS)
•Internet Security Association and Key Management Protocol (ISAKMP)
•IKEv2
•IP Version 6 with TCP6, UDP6, ICMP6 and ND
•Lightweight Directory Access Protocol (LDAP)
•Manufacturing Message Specification (MMS)
•Network File System (NFS) v2, v3 - Portmapper, Mount, NFS
•Open Shortest Path First (OSPF) v2, v3
•Real Time Streaming Protocol (RTSP)
•Real Time Protocol/Real Time Control Protocol (RTP/RTCP)
•Secure Shell (SSH)
•Secure Sockets Layer (SSL) v3/Transport Layer Security (TLS) v1
Tier 3 プロトコル:
•Session Initiation Protocol (SIP)
ベースプラットフォームに含まれるプロトコル:
•IEEE 802.1Q •IPv4 •TCP •UDP •ICMP •ARP •TFTP •DHCP

## ■ 販売代理店



エンピレックス株式会社  
コミュニケーション・プロダクツ・グループ

〒150-0021 東京都渋谷区恵比寿西1-10-11 フジワラビルディング 7F  
Tel: 03-5457-2342 Fax: 03-5457-0541  
E-mail: Hammerjapan@empirix.com URL: www.empirix.co.jp

※Mu-8000は Mu Dynamics™社の製品です。  
※記載されている社名・製品名は各社の商標または商品登録です。  
© 2009 Empirix. All rights reserved. 2009.05