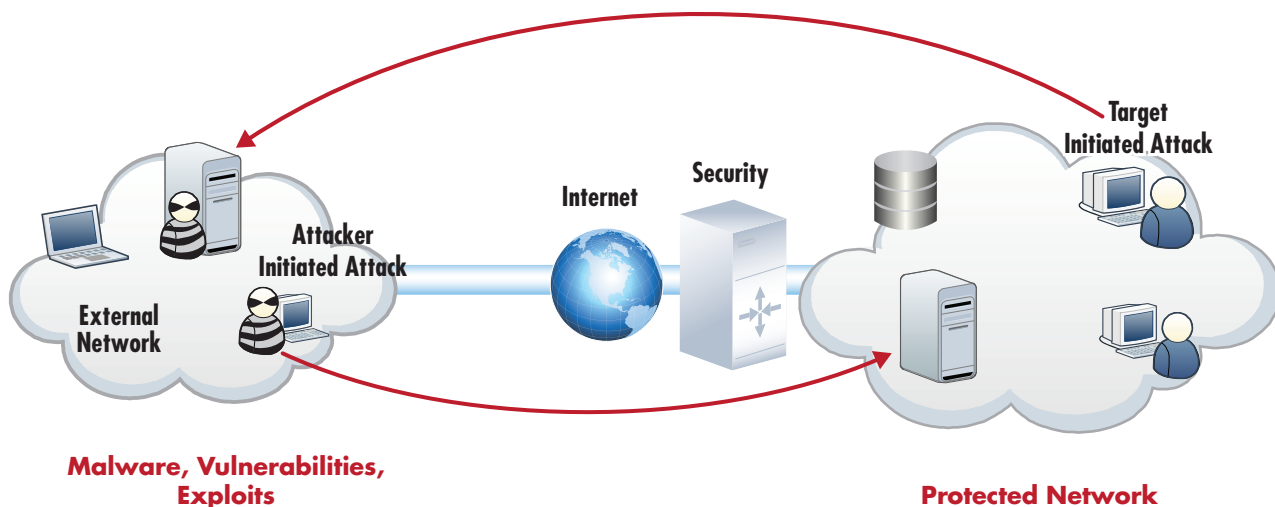




IxLoad-Attack



IxLoad-Attackは、使い易さで高い評価を頂いているL4-L7プロトコルエミュレーションツールであるIxLoadに実装したセキュリティデバイス向けのテストソリューションです。

約6,000種類の攻撃パターンを標準で搭載し、テストポート間で様々な攻撃をシュミレーションします。フルレートでのDDoSアタックもサポートしており、これらを組み合わせることによって、様々なネットワークデバイスの脆弱性を簡単にテストすることができます。

また、IxLoad-Attackでは、週単位で最新の攻撃パターンを追加する定義ファイルの自動更新機能が使用できます。これにより、ファイアウォールやIDS/IPS、VPNゲートウェイなど、ネットワークセキュリティの要となるデバイスは、常に最新の防御機能を備えることが可能になります。

その他にも、IxLoadでエミュレーションできる通常のアプリケーショントラフィックと共に、攻撃をシュミレーションすることも可能です。これにより、攻撃系トラフィックと正常系トラフィックの混在環境も容易に構築でき、より実環境に近いネットワークトラフィックを使用したテストが可能になります。

更にはVPNトンネル上でも疑似攻撃を生成する機能を保持し、外部だけでなく内部からの攻撃に対するセキュリティテストもIxLoadのみで実現可能です。

特徴：

- 標準で6,000種類の攻撃トラフィックをシミュレーション可能
- 攻撃パターンを自由にカスタム可能なMultiple Evasion技術
- 1GbE/10GbE ラインレートでのDDoSアタックを実現
- 通常のアプリケーショントラフィックとの組み合わせにより、実環境に近いネットワークを再現
- 同じポートで正常系および攻撃系トラフィックの混在が可能
- 脅威時のセキュリティー効果、パフォーマンス、サービス性能を測定
- VPNトンネル上にも攻撃トラフィックを生成可能
- 新たな脅威にも対応できる定義ファイルの更新サービス



IxLoad-Attack Features

Feature	Options
Published Vulnerabilities and Malware	<ul style="list-style-type: none"> • 6,000+ vulnerabilities and malware • Highest coverage of Microsoft vulnerabilities • Subscription service with online and offline malware and vulnerabilities updates • Measures security effectiveness • Emulates attacks over IPv4 and IPsec • Comprehensive attack metadata • Multiple attack evasions • Packet capture using IxLoad's embedded Analyzer • Attacker/server-initiated attacks • Target/client initiated attacks (client based attacks)
Multiplay Voice, Video, Data and Wirelss Protocol Support	<ul style="list-style-type: none"> • Internet: HTTP, P2P, FTP, SMTP, POP3, DNS, and CIFS • Video: IGMP, RTSP, Adobe Flash Player™, Microsoft Silverlight™, Apple HLS, MPEG2, and H.264/AVC • Voice: SIP, MGCP, H.323, H.248, Cisco Skinny™, FAX over IP, video conferencing and PSTN • Wireless: 3GPP packet core protocols used by GGSNs
Distributed Denial of Service	<ul style="list-style-type: none"> • Both IPv4 and IPv6 • Botnet and target emulation • Attacks against live servers • Attacks against intermediate devices • Emulation of large botnets with millions of unique IP addresses • Line rate attacks over 1GE and 10GE interfaces • Mix of voice, data, video and DDoS traffic on same port • Mix multiple attack patterns on same port • Attacks initiated from spoofed IPs or real IPs • Attack rate and attack throughput test objectives • Attacks: ARP, ICMP, UDP, TCP, IP and IGMP

IxLoad-Attack Statistics

Feature	Statistics
Distributed Denial of Service	<ul style="list-style-type: none"> • Attack counters (Attacks Sent/Received/Not Received) • Attack rates (Attacks per second Sent/Received/Not Received) • Attack throughput (Attack Throughput Sent/Received) • Per attack counters (Attacks Sent/Received/Not Received) • Per attack rates (Attacks per second Sent/Received/Not Received) • Per attack throughput (Attack Throughput Sent/Received) • Drill down per port, attack, and network
Published Vulnerabilities & Malware	<ul style="list-style-type: none"> • Attack counters (Attacks Sent/Received/Not Received) • Attack rates (Attacks per second Sent/Received/Not Received) • Attack packet counters (Attacks Packets Sent/Received/ Not Received) • Attack packet rates (Packets per second Sent/Received/Not Received) • Attack throughput (Attack Throughput Sent/Received) • Per attack counters (Attacks Sent/Received/Not Received) • Attacks - distribution by year, vendor, severity, category, type, evasion class (Attacks Sent/Received/Not Received) • Drill down per port, attack, and network

For more information see http://www.ixiacom.com/solutions/testing_security/index.php.

This material is for informational purposes only and subject to change without notice. It describes Ixia's present plans to develop and make available to its customers certain products, features and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.



イクシアコミュニケーションズ株式会社
〒160-0023 東京都新宿区西新宿6-24-1
西新宿三井ビル11F
TEL : 03-5326-1948
FAX : 03-3348-7733
E-mail: salesjapan@ixiacom.com