TEST METHODOLOGY

Breach Prevention Systems

September 12, 2019

v2.95 Request for Comments DRAFT

Table of Contents

1 Introduction

1.1 The Need for Breach Prevention Systems

Enterprises, both public and private, find themselves in a world of ever-increasing cyber risk. Threat actors with various motivations and skill levels are constantly launching attacks, both targeted and opportunistic. To properly defend the enterprise, point products such as firewalls or endpoint products in and of themselves are insufficient. Enterprises need visibility, and the ability to interdict, in all phases of the Cyber Kill Chain[1]. Enter the breach prevention system (BPS), an integrated solution that provides both comprehensive protection and alerting and reporting.

1.2 About This Test Methodology

The Breach Prevention System Test Methodology describes a new approach to testing the efficacy of security solutions. The BPS will be assessed as an integrated system, rather than an aggregation of point products. Scenario-based, goals-oriented testing will be performed to determine the real-world effectiveness of the system under test in an environment that emulates an enterprise network.

During the evaluation, numerous scenarios will be run. These scenarios cover all steps of the Cyber Kill Chain. Each step can be defined in terms of the MITRE ATT&CK Framework.[2] One or more techniques will be used in each of these steps.

Testing will be performed in a red team fashion. This testing is adversarial in nature; however, it is not threat actor simulation. No specific threat actor (e.g., APT1) will be simulated during a scenario, but each scenario will leverage tools, techniques, and procedures leveraged by various threat acting groups.

To conduct the test, a mix of off-the-shelf and custom techniques and payloads will be used. For any given technique, multiple different tools may be used. If a BPS is found to block one tool, the evaluators may adapt to attempt to evade the defenses and fulfill the mission in the scenario as a threat actor would.

At a high level, scenario testing will cover:

- False positives
- Targeted attacks
- Opportunistic attacks
- Insider threats

Any vector for attack or exfiltration for which there is an enumerated ATT&CK technique ID is in scope. This includes physical access and removable media.

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[2] https://attack.mitre.org/matrices/enterprise/

1.3 Inclusion Criteria

The only required component of the breach prevention system is a network-based appliance that is capable of being deployed in line and taking prevention or blocking actions against malicious traffic or traffic containing malicious binaries. This can be a firewall, IPS, or similar type device.

Other optional components may include but are not limited to:

- Endpoint agents
- Endpoint management systems (on premises or in the cloud)
- Sandboxes (on premises or in the cloud)

While these components are optional, solutions that do not include some or all of these components will have reduced introspection and interdiction abilities, potentially leaving them blind to various threat vectors.

It is also important to note that while, in many scenarios, the goal of the threat actor will be to attain potentially sensitive information from the "enterprise," this is not a DLP test in that NSS is not explicitly testing capabilities such as marking and classification of information.

Because the BPS test is a systems-level test, granular assessment of point product components will not be conducted. For assessments such as evasions coverage, network throughput, etc. the component such as the next generation firewall (NGFW) or endpoint agent should have been assessed in NSS Labs' NGFW or Advanced Endpoint Protection (AEP) group tests. The most recent report for that component will be referenced rather than rehashing discrete control tests.

1.4 Deployment

The network components of a BPS are, at a minimum, placed in line with the main north-south traffic of an enterprise, preferably at the ingress/egress of the private network. Some systems may themselves function as the edge routing/firewall device, but this is by no means required. The system under test will be assessed on its ability to provide protection against server- and client-side exploits, including phishing attacks. The system under test will not be assessed on its ability to provide stateful firewalling.

The network appliance may also be deployed at various internal segmentation points within the network, typically at Layer 3 boundaries, to provide visibility and control for east-west traffic and prevent pivoting within the environment.

The test harness for BPS 3.0 will provide a segmented network with multiple VLANs and subnets. Systems that function as a gateway firewall will be configured with an equivalent rule set for traffic flow and routing. Network segments simulating internal servers and desktop workstations will be NATed from the outside "attack" network. However, there will be a "DMZ" in the swim lane to support public-facing servers that may be directly attacked.

The swim lane will contain a mix of Windows and Linux endpoints. These will include both servers and workstations. An Active Directory domain will be present, and workstations and Windows servers will be attached to the domain. A VPN connector will also be present in the swim lane.

While cloud services such as file sharing and email may be incorporated into various scenarios, there will be no hybrid cloud component to the swim lane, and the ability of the BPS to provide protection for public, private, or

hybrid cloud services will not be assessed by this test. Please refer to NSS' Cloud Workload Protection group test for products covering the cloud.

Figure 1 provides a cursory overview of the breach prevention topology. The "A" designations represent egress points, via typical WAN, via end user VPN terminal access, and via socks laterally from inside the domain.

Typical enterprise office servers and applications are deployed within the DMZ, additional files and services are deployed on internal domain servers. Clients are divided into representative groups, which are discretely segmented by network, and a range of software is run on the clients to reflect a typical enterprise office stack of productivity applications (Microsoft Office, browsers, etc.)

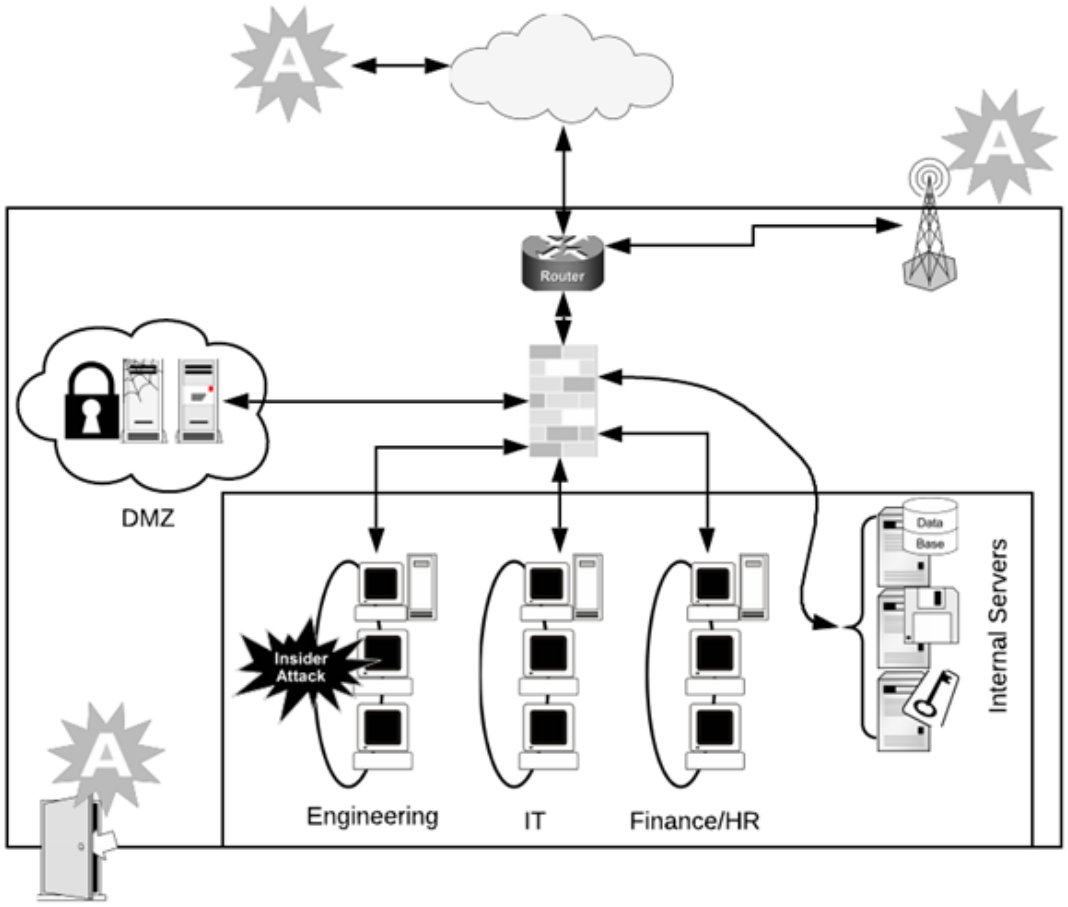

Figure 1 – Overview of Breach Prevention Topology

2 Security Effectiveness

Security effectiveness in the BPS 3.0 Group Test will be determined by the ability of a BPS to perform kill chain interdiction during an adversarial engagement. Ultimately what matters is the BPS' ability to prevent the attacker from exfiltrating sensitive information. NSS' testing will be:

- Goals-oriented
- Scenario-based
- Adversarial

During execution of a scenario, all steps taken will build on each other, illustrating the entire kill chain. Each scenario will have a goal (e.g., theft/destruction of data, establishing persistence, etc.) that reflects the motivation of the attacker. The attacker motivations are as described in the MEECES framework[3] developed by Max Kilger:

- Money
- Ego
- Entertainment
- Cause (including espionage, cyberwarfare, or hacktivism)
- Entrance to a social group
- Status

Example threat scenarios that will be executed are listed for each section. All scenarios executed during public testing will be in the test reports.

2.1 False Positive Handling

For the purposes of the BPS 3.0 Group Test, a false positive is defined as any block or alert generated for non-malicious activity, which presents itself as security relevant. Any time spent by an analyst running incident response playbooks for issues that are not real distracts from the ability to identify and remediate real issues. Additionally, because of the assumption that the BPS can automatically block traffic, a high false-positive rate could have a negative impact on the stability and usability of the network.

To assess the BPS' tendency towards false positives, NSS will run false-positive scenarios that involve non-malicious behavior or items likely to trigger either block or detect signatures in some component of the BPS.

[3] Kilger, Max. (2010). Social Dynamics and the Future of Technology-Driven Crime. 10.4018/978-1-61692-805-6.ch011.

False-positive scenarios can also be described in terms of MITRE ATT&CK technique IDs. For instance, a false-positive test wherein a user repeatedly fails to log in due to fat-fingering a password, then proceeds to mount and browse a network drive before copying files from the network share to a local location would reference the following MITRE technique IDs:

FP Action	Associated Technique ID	Associated Technique Description
Failed logins	T1078, T1110	Valid accounts, brute force
Browsing network file share	T1083	File and directory discovery
Copying file to local host	T1039	Data from network shared drive

2.2 Insider Threats

For today's enterprise, the risk of an insider threat is all too real. While it may not be feasible for a BPS to prevent an ill-intentioned user from accessing files that he or she has legitimate access to, there are times when the insider threat may engage in overtly malicious actions. Scenarios testing the ability of the system under test to identify and prevent the insider threat from succeeding will be presented.

For example: A malicious insider who is motivated by financial gain attempts to steal financial data. The user leverages a local privilege escalation exploit in order to dump credentials from a shared machine and succeeds in gathering administrator credentials. These credentials are used to mount a network drive and steal financial data, which can then be exfiltrated to a remote server.

Technique ID	Description
T1078	Valid accounts
T1068	Exploitation for privilege escalation
T1135	Network share discovery
T1083	File and directory discovery
T1074	Data staged
T1002	Data compressed
T1048	Exfiltration over alternative protocol

2.3 Targeted External Attacker

For most enterprises, the targeted, external attacker, often described as the advanced persistent threat (APT) is the great fear, and BPS vendors spend a lot of time addressing this. Such attackers want something that only a given enterprise has, and they are willing to spend a great deal of effort obtaining it. Enterprises may expect to see custom malware, implants, and C2 infrastructure, which is used solely to target them and never re-used. Payloads may be designed, after considerable reconnaissance, so that they only execute in a target environment in order to prevent leakage and reduce the likelihood of detection.

Many scenarios presented to the system under test will be of this nature.

For example: A targeted attacker sends a phishing message to a system administrator. The attacker can gain valid login credentials and drop malware on the user's workstation. The user runs the payload, which has been crafted specifically for the target environment, and gives the attacker an initial foothold. The attacker uses that access to establish further persistence with an implant kit. The user's credentials are used to perform further internal reconnaissance and move laterally within the system. Sensitive data is exfiltrated, but persistence remains in the environment.

Technique ID	Description
T1192	Spear phishing link
T1056	Input capture
T1480	Execution guardrails
T1204	User execution
T1059	Command line interface
T1086	PowerShell
T1078	Valid accounts
T1050	New service
T1032	Standard cryptographic protocol
T1104	Multi-stage channels
T1135	Network share discovery
T1083	File and directory discovery
T1039	Data from network shared drive
T1074	Data staged
T1002	Data compressed
T1048	Exfiltration over alternative protocol

2.4 Opportunistic Attacker

By far the highest volume of attacks experienced by enterprises are those of opportunity. These non-targeted attacks may be conducted by threat actors with varying degrees of skill and differing motivations. Financially motivated attacks by criminal organizations, such as ransomware attacks, fall into this category, as do opportunistic attacks by less skilled threat actors looking to boost their own egos by taking advantage of unpatched systems discovered via scanning tools such as Shodan.[4]

Scenarios simulating opportunistic attacks will not involve payloads that take into consideration the target environment. These scenarios may involve data theft but can also involve data destruction or defacement.

[4] https://www.shodan.io/

For example: A user browses to a website currently serving as a watering hole attack vector. A payload is delivered, which launches ransomware that encrypts all sensitive documents the user has access to while securely deleting the original. A ransom note is left with instructions on how to negotiate for the release of the decryption key and tool.

Technique ID	Description
T1189	Drive-by compromise
T1135	Network share discovery
T1083	File and directory discovery
T1026	Multi-band communication
T1032	Standard cryptographic protocol
T1071	Standard application layer protocol
T1486	Data encrypted for impact

2.5 Scenarios Requiring Physical Access

Today, the enterprise perimeter is increasingly porous. Telecommuting and virtual private networks (VPNs) have led to more and more workers operating from outside the corporate environment, putting assets such as laptops, tablets, and phones within the physical reach of attackers (e.g., the "evil maid"[5] attack or related vectors). Long the provenance of intelligence agencies, commercially available hardware tools[6] put this type of attack well within the reach of even the most budget-conscious operations. This, combined with the reality of insider threats, presents additional concerns for enterprises.

These scenarios will not have a separate category within the test but instead will be spread across the targeted attacker and insider-threat scenarios. Physical access primarily reflects vectors for initial exploitation, establishing persistence, or exfiltrating data. Assessed techniques may include:

Technique ID	Description
T1091	Replication via removable media
T1200	Hardware additions
T1109	Component firmware
T1052	Exfiltration over physical medium

[5] https://en.wikipedia.org/wiki/Evil_maid_attack

[6] https://shop.hak5.org/

3 Reporting and Visibility

Given that a BPS comprises many different, distributed technologies, and given that these technologies are able to take proactive action and block traffic, the need for a single coherent, centralized "pane of glass" for enterprise defenders to refer to should be apparent. All event data from sensors, sandboxes, end point agents, etc. should be collected in as few management consoles as possible.

Even in this case, many enterprises will desire or require that the product be capable of offloading logs to a security information and event management (SIEM) system for manageability and for preservation of the logs in a forensically sound location. To facilitate this, the BPS components should be able to stream logs to a centralized collector. At a minimum, this should be via Syslog. Ideally the Syslog connection will be made over TLS or some other trusted channel.

4 Performance

The various components of the BPS will have differing effects on the performance of the network and systems on which it is deployed. These can range from additional overhead on endpoints created by agents to reduced throughput at various chokepoints in the network due to processing by in-line sensors.

Because this test does not dictate how the BPS is to be implemented, providing one-to-one comparisons would be difficult. Instead, the relevant public test results for the components of the BPS (e.g., NGFW, NGIPS, AEP) will be referenced.

5 Total Cost of Ownership and Value

Implementation of security solutions can be complex, with several factors affecting the overall cost of development, maintenance, and upkeep. All of these should be considered over the course of the useful life of the product.

- **Product Purchase** – The cost of acquisition
- **Product Maintenance** - The fees paid to the vendor (including software and hardware support, maintenance, and updates)
- **Installation** – The time required to take the technology out of the box(es), configure it, deploy it in the network, apply updates and patches, perform initial tuning, and set up desired logging and reporting
- **Upkeep** – The time required to apply periodic updates from vendors, including hardware, software, and firmware updates

6 Appendix A: Change Log

Version 2.95 (3.0) – September 2019

- Revised security effectiveness test cases to capture threat scenarios
  - Removed volumetric testing of exploits, malware.
  - Test cases structure linked to MITRE ATT&CK techniques and the Cyber Kill Chain concepts
- Added new section 3, reporting and visibility
- Removed performance test cases in section 4 (formerly section 3)

Version 2.0 – January 2018

- Renamed section 2.2.2 to "Malware"
- Modified section 2.3
- Added sections:
  - 2.3: Physical Access and Malicious Insider Attacks
  - 2.4: Data Exfiltration
  - 2.5: Advanced attacks against hardware systems
- Removed 3.6: HTTP Capacity with Transaction Delays
- Removed 3.8.1: "Real World" Protocol Mix (Enterprise Perimeter)
- Removed 3.8.2: "Real World" Protocol Mix (Education)
- Added sections:
  - 3.7.1: Single Application SIP Flow
  - 3.7.2: Single Application SMTP Flow
  - 3.7.3: Single Application SMB Flow
  - 3.7.4: Single Application RDP Flow
  - 3.7.5: Single Application YouTube Flow
  - 3.7.6: Single Application WebEx Flow
  - 3.7.7: Single Application BitTorrent Flow
  - 3.7.8: Single Application Netflix Flow
  - 3.7.9: Single Application SSH Flow
- RPC Fragmentation removed from evasions section
- Removed 4.4: Protocol Fuzzing and Mutation
- Changes to wording in the following sections:
  - 1.1: The Need for Breach Prevention
  - 1.4: Deployment
  - 2.1: False Positive Testing
  - 2.2: Detection and Prevention Engine
  - 2.2.2: Malware
- Updated contact information with office address

Version 1.1 – April 2017

- Section 2.3.1: Removed polymorphism and metamorphism from Binary Obfuscation
- Section 2.3.7: HTML Obfuscation: Removed HTTP Evader

- Removed Section 3.3.6: Maximum SSL Handshakes per Second
- Removed Section 3.8: HTTPS Capacity with No Transaction Delay (HTTP Persistent Connections)
- Section 3.9: Replaced Financial Traffic Mix with Education Traffic Mix
- Combined sections 4.5 (Power Failure) and 4.6 (Persistence of Data)

7 Contact Information

NSS Labs, Inc.
3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com