

Micro-Deployment • Overview

We realize that not every company's network is the same. Moreover, we know that, due to issues ranging from complexity to disparity, not all organizations can deploy NetBait Enterprise over their entire network. In these instances, we offer several options to deploy NetBait on particular network segments or sub-networks and to utilize NetBait's infrastructure to execute highly specific functions within the network security superstructure of your organization.

Although NetBait allows for multiple configurations and deployments, there are three specific types of micro-deployments that we will discuss here. These are:

- Security Monitoring -- NetBait Sensor
- Stable Security Configuration -- NetBait OS Defender
- Security testing and analysis -- NetBait Lab

NetBait Sensor

We offer four distinct implementations of NetBait Sensor on networks over which you need control, from which you want to collect relevant data, and to which you might want to provide additional security. These Sensors are data, service and risk-free distributions of NetBait Linux and have minimal hardware and support requirements (i386+ PC, 8MB of RAM, and floppy drive).

Passive Sensor

You can utilize NetBait infrastructure to create passive log writing sensors that will capture all incoming traffic and provide specific message responses to every network connection. Implementation of such sensors provides you with a real-time picture of the hack-related activity on any local or remote network. What's more, you have multiple distribution options for Passive Sensors, including web interface, manual (in *.bin file format), and many others.



Active Sensor

With Active Sensor, you can create specific modules for specific "missions." Once installed, Active Sensors are transparent to the host network and act as "Passive Sensors." However, at any moment, you can re-deploy any all of them for a particular task, including network security penetration tests, traffic sniffing or custom network routing. These Sensors are seamlessly "activated" by uploading custom commands (scripts) to specific modules from a centralized administration point.

Once a task is completed, involved Active Sensors unload their mission scripts and deliver results back to a specified destination (log server, IDS or even workstation). When the mission is complete, they switch back to their passive mode. This logic allows you to maintain a distributed and secure infrastructure for remote security management, troubleshooting and auditing.

Production Sensor

If you want to deploy a subterfuge on certain network segments, can use the NetBait Enterprise infrastructure to create active targets for a given local or remote network segment. In addition, you can change the segment's overall "picture" by adding hundreds of "fake" NetBait Nodes to it. Since you control the NetBait infrastructure, you are allowed the choice of installing any services and operational systems, as well as an "open book" capability to create data patterns and behavior options for installed targets. All hacker activity is captured and reports delivered are delivered to a designated administrator.

Production Sever allow you to provide your clients or partners with new ways to protect important data and to gain knowledge of their network intrusions. At the same time, you can employ Production Sensor without having to conform the entirety of your global network to a new object schema.

Split Sensor

Split Sensor acts much like Production Sensor, with the exception that, instead of delivering filtered reports, it writes raw logs to a specified log server. These logs give you the ability to merge data from multiple networks and create profiles of a specific intruder.

NetBait OS Defender

Protection

NetBait Enterprise can be used to create a proxy-like system that protects mission-critical objects on any given network. OS Defender directs all "production" traffic (http for example) to a specified port on a designed system (web server), while redirecting all other traffic and intrusion attempts to another system within NetBait Server Farm. This logic enables you to present OS Defender as a single production server and reduce the security risks (both yours and those of your partners) that are inherent in providing any type of IT service.

Policy Enforcer

With Policy Enforcer, you can configure any of your existing stand-alone systems (such as a firewall, web server, DNS or any other) to provide static network services of any kind based on a set of specific rules (firewall, web server, gateway, proxy). This real system would then be delivered to any one of your network segments along with other NetBait Nodes.

As the result, you reduce risk of the systems' compromise by having a permanently configured service that has no "write" functionality and cannot be changed or re-configured anywhere other than within the NetBait Enterprise infrastructure.

NetBait Lab

Want to test your intrusion detection and prevention systems? NetBait Lab can serve as your research platform. You can employ NetBait to create networks of objects configured in various implementations. These networks are protected by existing IDS or firewall tools and then "artificially" attacked in a controlled environment. Subsequent reports generated by IDS or firewalls would be compared to reports from NetBait objects/networks to reveal the current state of IDS or firewall functionality.

A Platform for Enterprise Security

NetBait Enterprise is more than just a security solution. In truth, it provides a platform from which you can deploy multiple security applications. It's flexibility and centralized architecture are what set it apart from the pack. These are just a few examples of possible micro-deployments; there are many more. To learn more about the NetBait platform and specific micro-deployments for your organization's needs, visit <http://www.NetBaitInc.com>.

Or call us at 1 866 NETBAIT.