



MDD's New Password Bouncer Automates Enhanced Security Policy

For Windows NT/2000 system and security administrators concerned about unauthorized access to user accounts, MDD's Password Bouncer is a centralized management console for preventing vulnerable passwords from being used by employees and contractors. Unlike existing security products, Password Bouncer defeats hackers by using their own methods in the on-going battle to protect your network.

ARE YOUR EMPLOYEES UNWITTINGLY LEAVING YOUR ENTERPRISE OPEN TO AN ATTACK?

The security industry has determined that 70% of all deployed firewalls are not effectively protecting the networks behind them. More telling is that 70% of all network compromises occur behind the firewall by a user or hacker attacking other user accounts.

Most users are prone to selecting simple, easy-to-remember passwords containing only letters or digits. Simple human behavior innocently reduces the effort required to compromise a password. A smart hacker can simply apply guesswork to gain unauthorized network access using spouse and child names, birthdays, anniversaries, etc.

More insidious are freely available utilities that automate what is commonly known as a Dictionary attack. These programs compare common words from several dictionaries to compromise a user's password. Should a hacker gain access to an administrative password and the Domain Controller's SAM, *all* passwords on the network are threatened -- from the mailroom to the boardroom.

Using these methods, the hacker can crack virtually any password given enough processing power and time. The key is to *harden* the password, so that by the time it can be compromised, it has already changed due to proper, globally enforced password policy.

PASSWORD BOUNCER – ENHANCED PASSWORD POLICY MANAGEMENT AND AUTOMATED ENFORCEMENT

Security on the network is of paramount importance requiring the cooperation of everyone from the CEO to the temporary employee. Although organizations establish and publish strong password standards that disallow common words and names, they face specific challenges when executing these policies:

1. Native tools in today's Windows NT/2000 environment do not provide the ability to enforce *truly strong* password policy on the level required to effectively protect the network
2. Automated systems to compare and validate passwords against illegal wordlists do not exist

Password Bouncer is the first solution that streamlines and automates the process of centrally managing and automatically enforcing enhanced password security policy:

- Reject passwords that contain common words using a 300,000-word English wordlist
- Reject passwords that contain common names using a 4,000-word proper name wordlist
- Reject passwords that contain specific names or phrases using a custom wordlist that includes wildcard support
- Enforce the use of upper and lower cases characters (mixed case)
- Enforce the use and position of special characters
- Enforce the use and position of numeric characters
- Reject passwords that contain palindromes (i.e. radar or bob)
- Enforce Password length, minimum and maximum
- Reject passwords with repeating sequences

By asserting control over the weakest link in your security policy, the user password, Password Bouncer is the single most effective measure that can be taken to improve internal Windows NT/2000 security. Get ahead of the hackers and beat them at their own game in the race to compromise your network – put Password Bouncer to work today.