

PORT KNOCKING: STEALTH AUTHENTICATION ON CLOSED PORTS

Client is a small enterprise having small offices at various locations. Company is maintaining several servers which need to be accessible from remote locations at all times. Client is looking for a solution which enhances the security of these servers which are critical for infrastructure management.

CHALLENGE

These servers are not running any public services like SMTP or HTTP, but accessibility from remote locations for SSH service is required in order to allow IT administrators to access company network and carry out their responsibilities. Client also understands that keeping SSH service open on these servers shall also invite random attempts on these servers by worms and viruses trying to exploit any known vulnerabilities. SSH servers in such a setup shall always be vulnerable to zero-day attacks.

SOLUTION

Newgen proposed a relatively new concept of "Port Knocking" to provide stealth protection to such these SSH servers. A port knocking daemon was implemented such that all the ports on the SSH server shall be closed while the port knocking daemon listens for all the connection attempts. When an authentic port-knocking sequence is detected, the daemon shall open a port for receiving one SSH connection only from the source of successful port-knock. If connection is not received within configured time, the opened port is closed again. The implementation also made use of MD5 hashed and knock tags to provide protection from replay attacks. Port knocking client was also developed in this implementation.

BENEFITS

- ✘ Stealth protection against port scans. It is difficult to break a reasonably sized port knock sequence.
- ✘ Even when services are known, possible vulnerabilities in the server code can not be exploited.
- ✘ IT administrators have a safe window to patch the service even when new vulnerabilities are known.
- ✘ Brute force password attacks are rendered ineffective.
- ✘ Protection against replay attacks.
- ✘ Simple setup and almost no performance issues for network connections.
- ✘ No change is required in the services being protected.

TECHNOLOGIES

- ✘ Port knock daemon and client implementation in C
- ✘ Sockets and pcap interface
- ✘ Scripts for iptables manipulation

PROJECT TEAM

- ✘ 6 person months
- ✘ Duration - 3 months

SOFTWARE ENGINEERING SERVICES AT NEWGEN

Newgen is a specialized provider of Software Engineering Outsourcing services. Over the last decade, Newgen has provided services to leading global packaged software product and enterprise software product companies.

Services provided include:

- ✘ Product Strategy and Conceptualization
- ✘ New Product development
- ✘ Product Extension
- ✘ Product Maintenance and Support
- ✘ Testing & Quality Assurance
- ✘ Porting / Migration
- ✘ Internationalization and Localization
- ✘ SaaS Enablement
- ✘ Professional Services