CASE STUDY

Automated Pentesting for Strengthening the Cybersecurity of Police Department

Ridge Security Technology Inc. www.ridgesecurity.ai

Customer

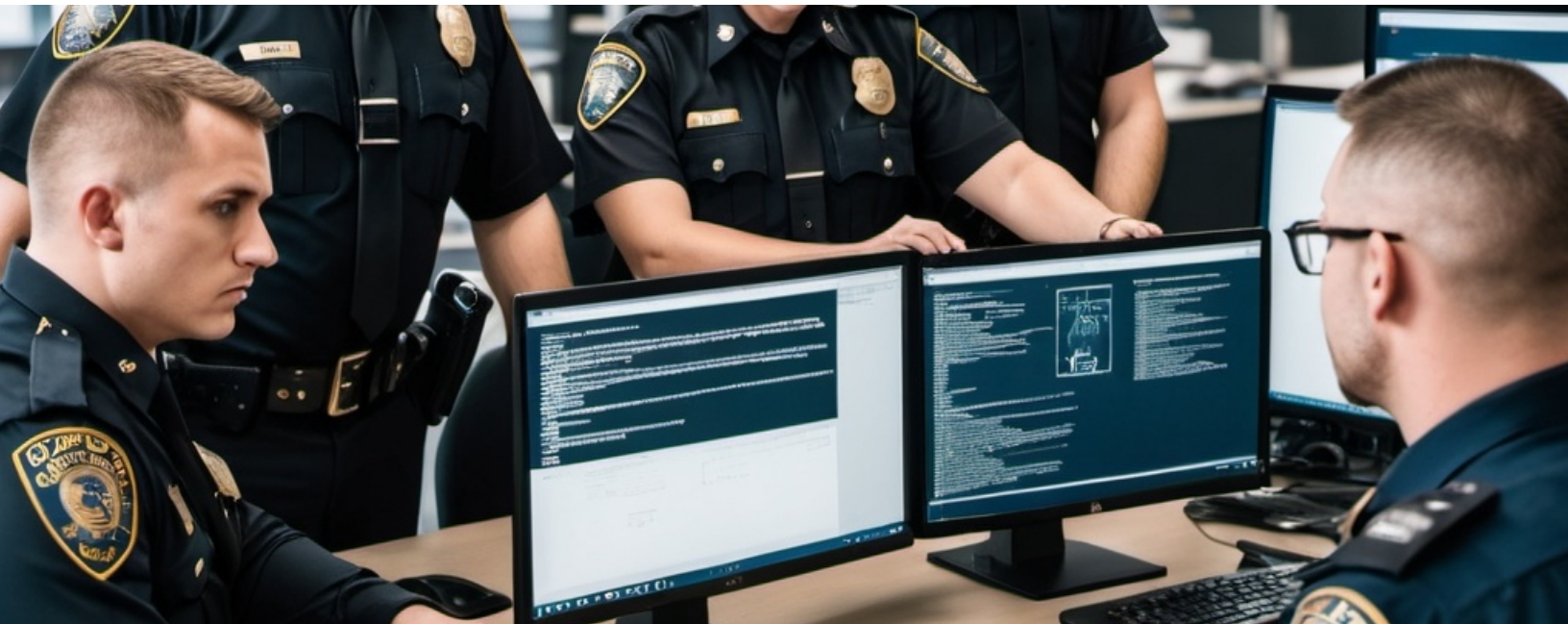
The ICT Division of a police force is a critical component, operating directly under the Chief of Police. This division plays a crucial role in modernizing the force by utilizing information and communication technology (ICT). It is also responsible for overseeing the use of ICT to ensure security and effectiveness.

Challenge

As an institution that holds sensitive state data, a police force has a significant responsibility in maintaining cybersecurity. However, there are substantial challenges in this area, particularly with penetration testing. Cybercriminals continuously develop new tactics and techniques, forcing the police force to adapt and update its defense systems. Organized cyberattacks by professional hacker groups pose a serious threat. The demand for competent cybersecurity experts is high, while the availability of adequate human resources remains limited.

Penetration testing is an effective way to identify weaknesses in security systems. By conducting pentesting regularly, the police force can:

- Identify security gaps that cyber-criminals could exploit before an attack occurs.
- Evaluate the extent to which existing security systems can protect data and infrastructure.
- Raise awareness of the importance of cybersecurity among police personnel.



Solution

RidgeBot is used for two types of perimeters. The first perimeter includes public-facing systems such as web applications and web servers. The second perimeter focuses on private systems, specifically endpoint security maturity within the LAN area. RidgeBot is a valuable tool for automated pentesting, identifying security vulnerabilities in these systems. It operates across two main perimeters:

1. Public Perimeter: Targets web applications and web servers connected to the internet.

2. Private Perimeter: Targets devices (endpoints) and assesses internal network security maturity levels.

RidgeBot automatically scans for various types of common vulnerabilities, such as injection, weak authentication, cross-site scripting (XSS), misconfiguration, and sensitive data leakage. Additionally, RidgeBot attempts to exploit discovered vulnerabilities to measure the level of risk.

In both perimeters, RidgeBot acts as a vigilant 'security guard,' proactively identifying potential threats.

Overall, RidgeBot helps organizations:

Identify security risks by finding vulnerabilities before they are exploited by hackers.

Save time and resources through the automation of the pentesting process.

Improve security levels by providing a better understanding of the organization's security posture.

Benefits

The implementation of automated pentesting within a police force is a strategic step to improve cybersecurity and protect valuable digital assets. By utilizing this technology, the police force can be more proactive in dealing with evolving cyber threats. Key benefits include:

- Early detection of vulnerabilities and automation of pentesting processes.
- Better visibility into network security and prioritization of risk management.
- Consistent procedures with automated pentesting.
- Time savings with automation.
- An updated vulnerability database with automated pentesting tools.

Automating repetitive and time-consuming pentesting tasks enables the police force to focus more on strategic security measures.

About Ridge Security

Ridge Security is a leader in exposure management, dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection, and cloud security monitoring.

Request a Demo

RIDGE SECURITY