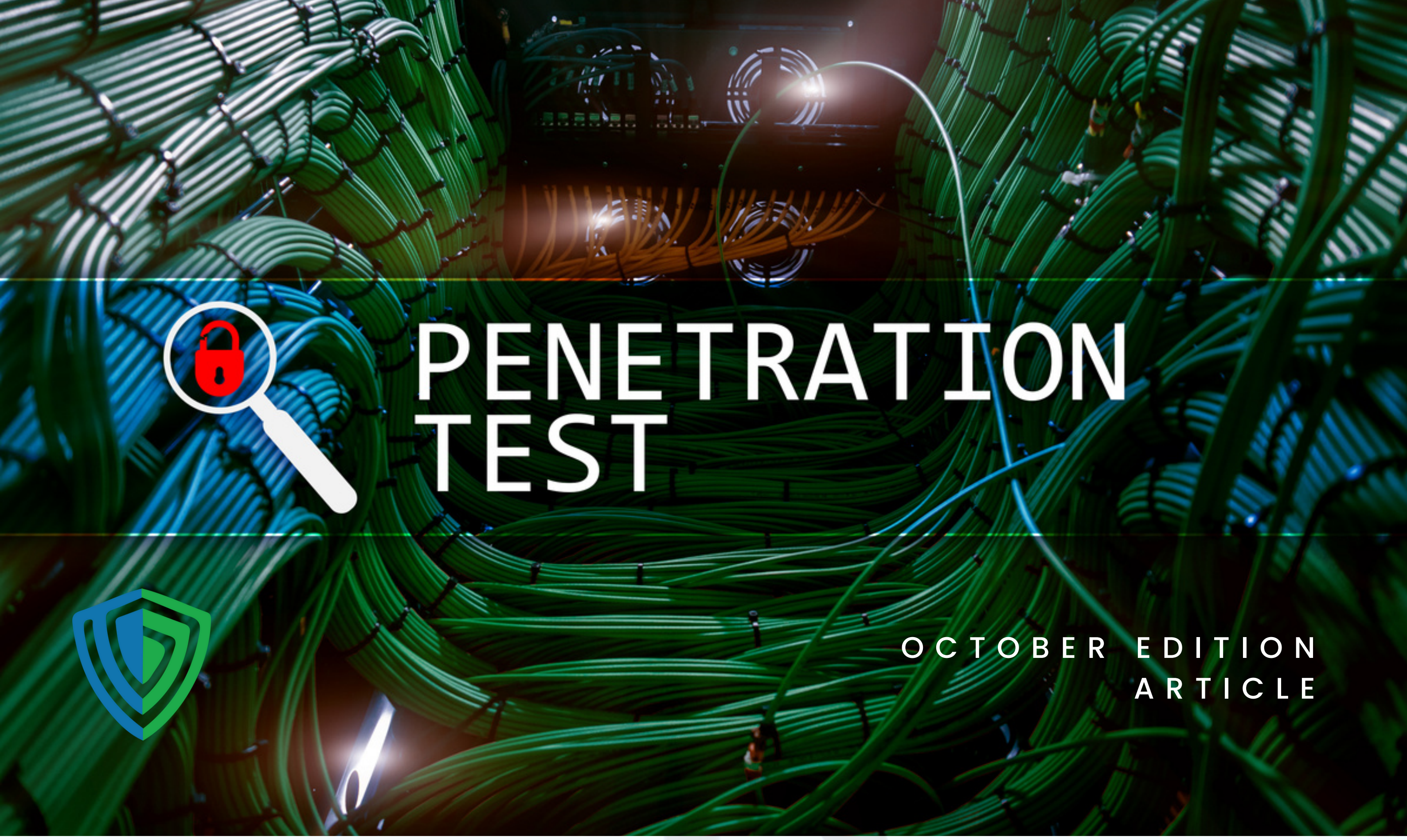

PENETRATION TEST

OCTOBER EDITION
ARTICLE

A GUIDE TO PENETRATION TESTING IN CYBERSECURITY

In the ever-evolving digital landscape, penetration testing stands as a crucial pillar of cybersecurity

In an era where digitization has transformed the very fabric of our society, the significance of robust cybersecurity cannot be overstated. With an ever-evolving landscape of threats and vulnerabilities, organizations must adopt proactive measures to safeguard their digital assets. One such indispensable practice is penetration testing, often referred to as "ethical hacking." This article serves as a comprehensive guide to penetration testing in cybersecurity, unravelling its methodologies, tools, and real-world applications.

The Need for Penetration Testing

Cyberattacks are becoming increasingly sophisticated, and attackers continuously probe for weaknesses in digital infrastructures. It is no longer a matter of 'if' but 'when' an organization will face a cyber threat. Penetration testing is a proactive approach that simulates real-world attacks to identify vulnerabilities before malicious actors exploit them. It is like stress-testing a fortress to uncover weak points that need reinforcement.

Methodologies in Penetration Testing

Penetration testing involves a structured approach to assess an organization's security posture. The methodologies typically followed include:

1. **Reconnaissance:** This phase involves gathering information about the target, which could be an application, network, or system. Testers use open-source intelligence, search engines, and other tools to understand the attack surface.
2. **Scanning:** In this phase, testers actively scan the target for vulnerabilities. This can include port scanning, vulnerability scanning, and service enumeration to pinpoint potential weaknesses.
3. **Gaining Access:** Testers attempt to exploit vulnerabilities they discover to gain unauthorized access. This is where they emulate the tactics of real hackers while staying within ethical boundaries.
4. **Maintaining Access:** Once inside, testers try to maintain access to the system, mimicking how an attacker might persistently exploit a vulnerability.
5. **Covering Tracks:** In the final phase, testers cover their tracks to ensure they leave no trace of their presence, like how attackers aim to remain undetected.

Tools of the Trade

Many tools are available to penetration testers to carry out their assessments. These tools range from open-source software to proprietary solutions and can be tailored to the specific needs of each engagement. Some common categories of tools include:

- **Scanning Tools:** Nmap, Nessus, and OpenVAS are popular for vulnerability and port scanning.
- **Exploitation Tools:** Metasploit is a renowned framework for developing and executing exploits.

- **Password Cracking Tools:** John the Ripper and Hydra help test password strength.
- **Wireless Assessment Tools:** Aircrack-ng and Wireshark are essential for evaluating wireless network security.
- **Web Application Testing Tools:** Burp Suite and OWASP ZAP are widely used for web app assessments.

Real-World Scenario

Penetration testing is not a theoretical exercise—it is about uncovering vulnerabilities that could have real-world consequences. Consider a scenario where a financial institution employs penetration testers to evaluate its online banking platform. If vulnerabilities are discovered and promptly remediated, it prevents potential financial losses and safeguards customer data.
An example where penetration testing could have identified a vulnerability before exploitation include:

- The Equifax data breach of 2017 where millions of customer records were exfiltrated due to some lapses in security management. In this breach, a widely known vulnerability was exploited, giving attackers the opportunity to access their systems and extract data which went unnoticed for some time. The crisis began in March 2017 when a vulnerability was announced that affected Equifax systems and administrators were informed to patch the affected systems. However, this did not happen. Secondly, some vulnerability scans were run by the IT department which did not identify the vulnerability either. For Equifax, it was not until July when the Equifax team noticed that a breach had occurred and only notified the public in September.

In summary some of the key takeaway's organizations can learn from the real-world scenario include;

- The need to conduct regular penetration testing and address identified vulnerabilities quickly - Penetration testing should not be considered as a one-time event or exercise for an organization. Businesses should look into having a planned activity schedule for penetration testing to be able to identify new vulnerabilities and address them early depending on the severity of the issue discovered. A consideration should also be made to have a test done before new systems or applications are deployed or a major change is implemented.

- The need to have either an inhouse penetration testing / red team or to work with an experienced vendor to conduct the exercise - Organizations may consider having the activity done by an inhouse independent team or engage the services of a provider with expertise in vulnerability assessment and penetration testing. An outsourced service provider may be considered when the organization may have budgetary constraints, the extent of the scope of the exercise or the lack of staff members to carry out the activity.
- The use of the penetration testing results to improve the cybersecurity posture of the organization - The report from a penetration testing exercise highlights issues that include critical and high rated vulnerabilities that may be exploitable. The collaboration between the penetration testing and the internal IT teams to remediate identified vulnerabilities improves the cybersecurity posture of the organization thus making it a little bit harder for a threat actor to make their way in.

Conclusion

Penetration testing is not a theoretical exercise—it is about uncovering vulnerabilities that could have real-world consequences. Consider a scenario where a financial institution employs penetration testers to evaluate its online banking platform. If vulnerabilities are discovered and promptly remediated, it prevents potential financial losses and safeguards customer data.
An example where penetration testing could have identified a vulnerability before exploitation include:

BY
SAMANTHA KUNG'U
PROJECT MANAGER (CYBERSHIELD)
SENTINEL AFRICA CONSULTING LTD

AND
GLORIA ISHIMWE
ASSOCIATE CONSULTANTS
SENTINEL AFRICA CONSULTING

Sentinel Africa
Your Advisor of Choice
FOLLOW US : **SENTINEL AFRICA CONSULTING**
www.sentinelafricaconsulting.com