SAMURAI SECURITY

Preparing Your Business for a Penetration Test Checklist

01
Define the Scope of Your Pen Test

Determine Testing Objectives:

- ☐ Identify the systems or applications you want to test (e.g., network security, web applications, physical access).
- ☐ Clearly state what success looks like (e.g., finding vulnerabilities in specific areas or assessing overall security resilience).

Set Boundaries:

- ☐ List all systems to be tested, such as specific IP addresses, applications, databases, or networks. Specify any systems or areas that are out of scope to avoid unintentional disruptions.

Agree on Testing Types:

- ☐ Choose a testing method: full-knowledge, partial-knowledge, or no-knowledge, depending on your security needs and the type of assessment required.

02
Select the Right Penetration Testing Partner

Research and Verify Credentials:

- ☐ Ensure the vendor holds industry-recognised certifications (CREST, NCSC, ISO 9001). Confirm they have experience with businesses similar to yours and specialise in the kind of testing you need.

Check Confidentiality Agreements:

- ☐ Sign a non-disclosure agreement (NDA) to protect your sensitive data during and after the test.

Evaluate Transparency:

- ☐ Ensure clear communication around the scope, cost, and timelines of the testing process.

03
Prepare Internal Teams

Notify Relevant Teams:

- ☐ Decide whether to inform your IT, security, or other relevant teams, based on the test type (for example, social engineering tests may require secrecy).

Business Continuity Planning:

- ☐ Ensure the test doesn't disrupt critical operations by scheduling it outside of peak business hours or having contingency plans in place.

04
Establish Clear Communication Channels

Assign a Point of Contact:

- ☐ Designate a primary person/team to liaise with the penetration testers and provide timely assistance.

Provide Neccessary Documentation:

- ☐ If conducting a white box test, gather and securely share network diagrams, application architecture, and other necessary data with the testing team.

05
Ensure Compliance and Legal Permissions

Review Compliance Requirements:

- ☐ Ensure the test aligns with industry standards like GDPR, HIPAA, or PCI-DSS.

Obtain Third-Party Permissions:

- ☐ Secure written consent from third-party service providers, cloud hosts, or vendors whose systems will be part of the test.

06
Backup Critical Systems and Data

Perform Full Backups:

- ☐ Complete and verify backups for all critical systems and data to avoid loss or corruption during the testing process.

Avoiding Testing in Production Environments:

- ☐ Whenever possible, conduct the test in a staging environment to reduce the risk of unintended system outages.

07
Plan for Debrief and Remediation

Schedule a Post-Test Debrief:

- ☐ Arrange a debriefing session with the testers to review the findings and understand the vulnerabilities discovered.

Allocate Resources for Remediation:

- ☐ Prioritise fixing the vulnerabilities based on severity and allocate the necessary resources and timelines for remediation.

08
Educate and Train Staff

Conduct Awareness Training:

- ☐ After the test, educate all relevant teams, including employees, developers, engineers, and anyone involved in the application or infrastructure, about security best practices.
- ☐ Highlight the vulnerabilities discovered during the test and provide guidance on how to avoid similar issues in the future to prevent potential security lapses.