(Rahul Balaji - 11449565)

Outline Test Plan

Introduction

The outline test plan aims to describe the main testing actions that must be taken to ensure system security, and to map out the responsibility of which team must undertake the particular action. In the following sections, the test plan will be outlined in a table with the following series of columns.

1) Information asset - This column specifies what exactly we are protecting, what this control mechanism is put in place for.
2) Control mechanisms - The control mechanism that we are testing.
3) Test plan - the test that will be conducted to ensure that the control mechanism is working.
4) Responsibility - The team that will undertake the task of testing it. Red team, blue team, purple team, or black team are the four different teams that can take up the tests.

Test Plan

Information Asset	Control Mechanisms	Test Plan	Responsibility
Physical server/machine locations.	Have physical security at locations that house major physical machines / servers that run the system or store information about citizens.	Run controlled infiltration attempts by asking a team to try and breach the physical security without alerting them at the location periodically. May use social engineering or other tactics. (covert operation).	Black team
Passport data / Licence data / Registered keeper data etc. (Citizen records)	Provide employee training on social engineering tactics. Filter all emails and block any known spam mails before	Conduct random tests on employees by sending them “bait” emails that are basically internal phishing mails to see if they fall for social	Purple team

	they are received by the employees. Block all emails from a list of suspicious email ids.	engineering. If they fail the test, train employee again. Try sending obvious spam mails with key words that will be recognized by the mail filter and see if the spam mail gets blocked before it is received by employee.	
System Network, Data stored in servers	Segregation of networks into zones and allowing access to services only when connected to internal private networks.	Trying to hack into the network by exploiting vulnerabilities and escalation of privileges. Conducting Pentests.	Red team
Passport database, DVLA database, and police national database	Encryption of data stored. Making sure all softwares installed are safe with no unknown vulnerabilities that can be exploited. Providing response to requests made by authenticated and authorised users only.	Making sure that no data stored in the database is in plain text that can allow threat actors to directly gain context from infiltrating the system. Conducting periodic vulnerability scans and software audits to ensure no unknown software is installed, and that all software is up to date with latest security patches. Monitor any suspicious requests, deliberately make requests with no session tokens in header that proves you are authenticated and check if you get any response.	Blue team

Backups	"3-2-1" rule must be followed which is established by the NCSC. At least 3 copies on 2 different devices and 1 must be offsite. Making sure hardware on which backups are stored is durable and damage resistant to an extent. Ensure data at rest is protected with encryption and also access restricted.	Test all backups by restoring them periodically and scan for any data loss. Try and gain access to backup data that is at rest and try to restore it to an offsite area. Make sure that only admins have right to access backup, and other users are restricted to access it, and unauthorised access is alerted, while authorised access is simply logged.	Blue team Red team Purple team
System availability	Adding Load balancers and firewalls to system to avoid D.o.S attacks and accommodate higher traffic.	Use booters and IP stressors to simulate traffic / D.D.o.S attacks on a scheduled time that has been allotted by the organisation.	Red team

Guest Lecture Reflections

Ian Thorton Trump of Cyjax

Ian's lecture emphasised the multifaceted role of a CISO beyond designing secure architecture and handling attacks. It involves ensuring compliance, upholding ethics, and fostering transparency to avoid being a scapegoat. Aligning the security program with the business strategy is key for maintaining positive company relations.

Paul Vlissidis of NCC

Paul's lecture highlighted the crucial role of red teaming in business. Despite unsettling the company by revealing vulnerabilities, it serves as a valuable tool for improvement. Compliance is the baseline; continuous enhancement is vital for sustaining business continuity.

Jon Noel of Zscaler

Jon's lecture has a main focus on the evolution of malware over time. Helped me understand about some new things like ransomware as a service (RaaS) that are now rapidly increasing in the market. While using AntiVirus is still a recommended practice, we need to consider the positives and negatives before making a choice.