X-Force Red

IBM **Security**

X-Force Red Cloud Testing for Microsoft Azure

Common Security Challenges

Microsoft Azure consists of many application, servers, services, firewalls and other components. While the Azure infrastructure comes with a suite of security tools, it is still the responsibility of the end users to configure and deploy them securely. If just one component is misconfigured or left exposed to the Internet, an attacker may find and use the vulnerability to compromise the entire environment. Credential management is also a challenge. Subscription accounts, for example, may be given to users who do not need that level of access. Azure enables users to create domain controllers in the Cloud that can speak to domain controllers on-premises. If the same controllers are used for both, an attacker could compromise one and take over the other.

X-Force Red Offensive Security Services for Azure environments can help find and fix those kinds of vulnerabilities. The services include testing from an external viewpoint, which means attempting an Azure compromise from the Internet or on-premises, or from an internal viewpoint, which means attempting a compromise from the Azure environment. An external Azure test can include X-Force Red hackers brute forcing their way into the Azure portal or leveraging open services, misconfigurations and cloud components without authentication.

X-Force Red Cloud Testing

An internal Azure test is more common, and can include the following:

Scoping

— X-Force Red works with the client to inventory important databases, applications and other internal systems, and X-Force Red determines if any are exposed to the Internet.

Vulnerability management for Azure environments

— X-Force Red Vulnerability Management Services (VMS) tracks new containers, assesses software versions in use, checks for secure provisioning, scans for known vulnerabilities, automatically ranks findings, and facilitates remediation.

Network Testing

— X-Force Red looks for misconfigurations, lack of network segregation and other exploitable vulnerabilities; and escalates privileges to see how deep into the environment an attacker could move.

Container Testing

— X-Force Red tests sample containers and images before they are released.

— Tests identify logic flaws, open ports, insecure application deployment and more.

Application Testing

— X-Force Red pulls apart applications, reviews source code, assesses security controls on browsers and mobile applications, assesses authorization token configurations, looks for access keys and unauthorized method calls, unencrypted data, and abuses functionality to test security controls' response.

— Simulates attacks against applications that run admin accounts like runbook automation.

X-Force Red offers flat rate project-based work or subscriptions and provides on demand access to all X-Force Red security testing services. To learn more, go to https://www.ibm.com/security/services/cloud-testing