Cloud Security Testing Playbook
Made By: Rami Ahmed (@Tr0cks)
TRAINING AND RESOURCES
Labs & Resources
Tools
misc
LEGAL
Key Points
Terms
CSA (Cloud Security Alliance)
The European Union Agency for Cybersecurity (ENISA)
Cloud Service Provider (CSP)
Microsoft SDL (Microsoft Secure Development Lifecycle)
CREST (Council of Registered Ethical Security Testers)
STRIDE
is a model of threats developed by Praerit Garg and Loren Kohnfelder at Microsoft for identifying computer security threats.
purpose
test cloud implementation of applications and systems (not the application itself)
Cloud Penetrating testing in Context
Other Terms referred to penetration testing
when it is performed ?
is penetration testing the best or most efficient form of security testing ?
NO, Its appropriateness can be determined based on context and purpose.
when penetration testing is advised to be performed ?
when security assurance of a live cloud-based product or feature is required
when threat modeling is advised over penetration testing ?
when the feature is just being designed
what phases of security testing this document is adapting
CREST (https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf)
CREST Preparation (part 3)
Testing (part 4)
suggests five main phases
preparation
Threat Modeling
Reconnaissance & Research
Testing
Report Writing
CLOUD PENETRATION TESTING SCOPE
Security controls that fall under the complete responsibility of the Cloud Service Provider (CSP) are usually not within the scope of a penetration test that is commissioned by the cloud consumer.
Software as a Service (SaaS) environment
what is allowed
exploit excessive permissions given to a particular user to conduct business level attacks (i.e. approve expenditure).
what is not allowed
the implementation of access control (session validation)
SaaS application input filtering (i.e. SQL injection) in the SaaS application.
underlying infrastructure is normally not part of the scope of a penetration test unless explicit permission from the CSP is given
Cloud penetration testing would not challenge the underlying technologies' design and code integrity but rather consider and leverage it
Leveraging flaws, common misconfigurations and known vulnerabilities in cloud services, technology and providers
Forensics, reverse engineering and research of the cloud service or fabric
The degree of testing and the scope of testing depends on the various services provided by the cloud service provider(s).
Infrastructure as a Service (IaaS)
User Access/Identity, Data, Application, and Operating System layers.
All other components below the red line are under the control and management of the CSP
the accidental discovery of any flaws and vulnerabilities of the cloud service should still be reported
The scope for testing and application of test cases also differs from service model to service model
a relatively small scope exists:
data and user access/identity controls.
Platform as a Service (PaaS) environment
the scope is extended here:
the application layer (and some platform configuration) is in scope; all layers lower are excluded.
the scope is further extended due to the flexibility of the model itself
the client responsibility is expanded and so does the scope of potential security testing.
Implementing or moving a workload to the cloud changes the scope for potential security tests (and breaches!).
Additional scope for testing is introduced (e.g. the cloud management plane), but some is still offloaded to the CSP (virtualization, hardware, and sometimes OS)
If the cloud customer gets authorization from the cloud service provider to test cloud components under the control and management of the cloud service provider:
additional complexity and scope will be introduced to the scoping of the cloud pentesting service.
Document Scope
this document does not detail testing of the application layer
SQLi
XSS Vulnerabilites
Virtual machines
already covered intensively by OWASP
this document is concerned only with the following domains
Account Security
User Identity & Access
IAM (Identity & Access Management)
Logging
Account level hardening practices
Cloud Federation & SSO (Single Sign-On interface)
Cloud Service Security
relates to data structures and cloud infrastructure that can be configured by the cloud customer
s3 bucket policies
vpc network access restrictions
Risky cloud formation templates
Application / Business logic
which is under control of the end user
Application & Design Flaws
Business Logic Flaws
Code Scripting flaws
DLP (Data Loss Prevention)
The scoping of a penetration test can and should consider all three domains, even if any are excluded from the scope of a penetration test as the three domains can substantially impact each other
Cloud Penetration Testing Objectives
key Points
identify vulnerabilities in code, configuration and otherwise insecure implementation and to advise on effective mitigations
Depending on what is being hosted and its implementation, the resulting vulnerability or security weakness will differ.
Naturally, such components will require their own testing guidelines
Spoofing
Tampering
Repudiation
Information Disclosure
DoS (Denial of Service)
Elevation of privileges
CLOUD PENETRATION TEST CASES AND CONCERNS
1. Preparation
2. Threat Modeling
3. Reconnaissance & Research
4. Testing
Report