Penetration Testing Frameworks

# General Frameworks

## NIST

NIST stands for the National Institute of Standards and Technology, this framework is based on existing standards, guidelines, and practices that allow cybersecurity risks to be manage and reduced.

There are three components to NIST: core, tiers, and profile. Core describes the reduction of cybersecurity risks in addition to an organization’s existing cybersecurity. Tiers guide cybersecurity management so that enough level is used for specific risks, used to discuss appetite, mission priority, and budget. Profiles are used to improve the cybersecurity at an organization [1].

This framework comprises of 5 steps for the guidance of reducing and managing cybersecurity risk [2].

### Identify

* Critical processes and assets
  + Activities that are mandatory, which must continue for the enterprise to be viable
  + Examples
    - Payments
    - Protect customer/patient information securely
    - Data that is collected is accessible and accurate
* Document information flows
  + Where data is located and travels
  + Important with contracts and external partners
* Maintain hardware and software inventory
  + Good understanding of computers and software as it’s the main entry point for malicious attackers
  + Spreadsheet is useful
* Establish policies for cybersecurity that includes roles and responsibilities
  + Expectations for how cybersecurity activities protect the data and systems
  + How they support critical processes
  + Policies within mind of other risks e.g. financial and reputational
* Threats, vulnerabilities, and risk to assets
  + Risk management processes are established and managed
  + Ensure internal and external threats are identified, assessed, and documented
  + Risk responses identified and prioritised
  + Execute risk responses as appropriate and monitor the results

### Protect

* Manage access to assets and information
  + Unique accounts (roles) for each employee
  + Making sure they have access to enough data, computers and applications required for their jobs; nothing more
  + Authentication
    - Passwords
    - Multi-factor
  + Manage and track physical access to devices
* Protect sensitive data
  + Encryption locally and while being transmitted
  + Integrity checking to ensure only approved changes to data have been made
  + Securely delete and/or destroy data when it’s no longer needed or required if asked
* Conduct regular backups
  + OS’s have built in back up capabilities
  + Software and cloud solutions
  + Keep one frequently backed up locally (offline) – protection against ransomware
* Securely protect your devices
  + Host-based firewalls
  + Uniform configurations to devices and control changes to device configurations
  + Only use what’s necessary – disable device services or features that are not needed
  + A policy and those devices are disposed of
* Manage device vulnerabilities
  + Regularly update OS and applications installed on computers
  + Automatic updates
  + Software tools to scan for additional vulnerabilities with high likelihood and/or impact
* Train users
  + Awareness of policies and procedures
  + Roles and responsibilities identified

### Detect

Identifying an attack.

* Test and update detection processes
  + Procedures for
    - Detecting unauthorized entities
    - Actions in the network and physical environment incl. personnel activity
  + Staff aware of their roles and responsibilities for detection
    - Reporting
* Maintain and monitor logs
  + Identify anomalies in computers and applications
  + Example
    - Changes to systems or accounts
    - Initiation of communication channels
  + Look for patterns
* Know the expected data flows for your enterprise
  + Unexpected data flow examples
    - Customer data being exported from an internal database and leaving the network
  + With clouds and managed services providers
    - Discuss how they track data flows and report (including unexpected events)
* Understand impact of cybersecurity events
  + Understand breadth and depth of the impact
  + Seeking help from stakeholders
  + Improve policies and processes

### Respond

Action against a detected attack.

* Response plans are tested
  + Making sure each person knows their responsibilities in executing the plan
  + Better prepared the organization is, more effective the response will be
  + Including
    - Legal reporting requirements
    - Required information sharing
* Response plans are updated
  + Testing this plan will reveal needed improvements
* Coordinate with internal and external stakeholders
  + Response plans and updates includes all key stakeholders and external services providers
  + Possibly contribute to improvements in planning and execution

### Recover

Restoring capabilities or services that were impaired or damaged due to an attack.

* Communicate with internal and external stakeholders
  + What, how, and when information will be shared with various stakeholders
  + All interested parties receive the information they need but no inappropriate information is shared
* Ensure recovery plans are updated
  + Improve employee and partner awareness by testing execution
  + Highlights areas for improvement
* Manage public relations and company reputation
  + Manage the enterprise’s reputation
  + Manage public relations so that data sharing is accurate, complete, and timely – not reactionary

### In relation to Penetration Testing [8, 9]

* In NIST 800-53, Control CA-8, mentions a standard method for penetration testing
  + Pre-test analysis based on the full knowledge of the target system
  + Pre-test identification of potential vulnerabilities based on the pre-test analysis
  + Testing designed to determine exploitability of identified vulnerabilities
  + All parties agree to rules of engagement before performing penetration testing scenarios
* Extent and rigor of the testing should be proportional to the risk the system presents
* Additional controls
  + CA-8(1): Independent Penetration Agent or Team
    - An individual can be an ‘external’ party that will be free from any perceived or actual conflicts of interest
    - Internal security teams may hide vulnerabilities to present the efficient of their defensive measures
    - External agent/tea, is free of any such biases
  + CA-8(2) Red Team Exercises
    - Select red team exercises and rules of engagement
    - Reflect a simulated attacking attempt to compromise information systems
    - Provide detailed assessment of an organization’s security
    - Closer to real-world conditions
    - Includes technology-focused and social engineering attacks

## MITRE ATT&CK

This is a knowledge containing tactics and techniques for the development of threat models and methodologies. Describing how attackers escalate privileges and evade security defences, looking at the perspective of the attacker.

* Understand the way attackers plans, launches, and executes their attacks.
* Allows you to detect attackers’ actions
* Includes resources to design analytics to detect their attacking techniques
* Maintains library of information about selected attacking groups and campaigns they have conducted
* Divided into a series of technology domains including enterprise networks with Windows or Linux OS and mobile devices
* Likely techniques that attackers may use

It is divided into multiple categories:

* Reconnaissance
* Resource development
* Initial access
* Execution
* Persistence
* Privilege escalation
* Defence Evasion
* Credential access
* Discovery
* Lateral movement
* Collection
* Command and control
* Exfiltration

Each technique has:

* Description
* Systems and platforms they apply to
* Which attacking groups that use this technique
* Ways to mitigate the behaviour
* Published references to the technique being employed

## Open Web Application Security Project (OWASP) [11]

* Web application security throughout the whole SDLC
* A penetration test can only identify a small representative of all security risks in a system
* Advantages
  + Fast and cheap
  + Lower skill set than source code review
  + Tests code that is being exposed
* Disadvantages
  + Too late in the software development life cycle
  + Front-impact testing only
* Web application scanners
  + Automated – not completely effective in black-box testing
  + Static source code scanners
    - May not be effective when used alone, it cannot understand the context which the code is constructed
* Test objectives specified by the security requirements
  + Validate that security controls are operating as expected (proving confidentiality, integrity and availability of the data including service)
  + Validate that security controls are implemented with few or no vulnerabilities – common ones such as OWASP Top Ten and ones that have been previously identified

## OSSTMM [12]

* Manual for security testing
* Focuses on operation security for penetration testing
* Test for security of 5 channels
  + Human security
  + Physical security
  + Wireless communications
  + Telecommunications – analog and digital
  + Data networks

## Triaxiom Security [15]

* Based on OWASP, NIST and Penetration Testing Execution Standard (PTES)
* Mentions some primary tools
  + Burp Suite Pro
  + Dirbuster/Dirb/Gobuster
  + Nikto
  + Sqlmap
  + B33F
  + Nessus
  + Recon-ng
  + Metasploit Framework
  + Searchsploit

### Planning

* Gather scoping information
  + Target info collected from client
  + Including
    - IP addressees and URLs
    - Authentication credentials – 2 sets of credentials for each role being tested
    - List of any sensitive or restricted portions of the application that shouldn’t be tested
* Reviewing rules of engagement
  + Meeting with client
  + Discuss rules of engagement and confirm project scope
  + Testing timeline, objectives, limitations/restrictions discussed

### Execution

* Intelligence gathering
  + Publicly available information and resources
  + Gather sensitive information
    - Email addresses
    - Usernames
    - Software information
    - User manuals
    - Forum posts
  + Tools include
    - Recon-ng
    - Maltego
    - Google Hacking
    - Wayback Machine
* Threat Modelling
  + Types of threats that may affect targets in scope
  + Risk rankings/priorities assigned to vulnerabilities
  + Validity of vulnerabilities discovered (external, internal, authenticated, unauthenticated, etc.)
  + Manual discovery and crawling of the application
    - Functionality from authenticated and unauthenticated perspective
  + Application proxy to evaluate packet-level traffic and response headers used
  + Tools
    - Burp Suite Pro
    - Cookie Manager+
    - NoRedirect
* Vulnerability Analysis
  + Target in network and application layer
  + In network
    - Evaluate attack surface of all in-scope assets via
      * Port scans
      * Banner analysis
      * Vulnerability scans
  + In application
    - Automated vulnerability scans – in unauthenticated then authenticated roles (for each in-scope)
  + Manual identification of vulnerabilities including form submission and application input points
  + E.g. injection attacks, error analysis, file uploads
  + Directory brute-forcing and vulnerability identification based on software versions
  + Tools
    - Burp Suite Pro
    - Nessus
    - Dirbuster/Dirb
    - Nikto
    - Searchsploit
* Exploitation
  + Exploit vulnerabilities – simulate an attacker
  + Realistic risk level
  + Possibility of exploit/attack chains
  + Any mitigating controls that may be in place
  + False positives identified
  + Evaluate issues requiring manual identification and exploitation
    - Business logic flaws
    - Authentication/authorization bypasses
    - Direct object references
    - Parameter tampering
    - Session management
  + Tools
    - Burp Suite Pro
    - Metasploit Framework
    - Sqlmap
    - B33F
* Post Exploitation
  + Infrastructure analysis
  + Pivoting
  + Sensitive data identification
  + Exfiltration
  + Identification of high-value targets/data
  + Use info from prioritization and ranking of vulnerabilities identified

### Post Execution

* Reporting
  + Formally document findings
  + Executive-level
    - Assessment activities
    - Scope
    - Critical/thematic issues discovered
    - Overall risk scoring
    - Organizational security strengths
    - Screenshots
  + Technical findings
    - All vulnerabilities listed
    - How to create the issues
    - Understand the risk
    - Recommendations for remediation
    - Reference links
* Quality assurance
  + May include follow-ups with client to confirm or deny environment details
* Presentation
  + Walk the client through information provided
  + Updates when needed
  + Address questions
  + New revisions of documentation
  + Schedule formal retesting

# Cloud Security Frameworks

## Background [4]

* List of cloud frameworks
  + CCM by Cloud Security Alliance
  + FedRAMP
    - Government use
  + ISO/IEC 27017:2015
    - For multinational organizations with security programs already built because controls are more familiar and align directly with the existing security programs
* CSP having an agreed-upon list of generally accepted controls for security
* Set of frameworks employed

## Cloud Controls Matrix (CCM)

### From [5]:

* A control framework
* Spreadsheet with 16 domains covering all key aspects of cloud technology
* Each domain broken into 133 Control objectives
* Mapped against industry-accepted security standards:
  + ISO/IEC 27001/27002/27017/27018
  + CCM V3.0.1
  + CIS Controls V8.
* Lists common frameworks and regulations
* Reduce need for multiple frameworks
* Common cloud standards in one place
* For each Control you can see all the different requirements it fulfils
* Questionnaire

### From [6]:

* Aimed to establish a better understanding and trust level between the cloud customer and the CSP
* Security issues broadly classified
  + In cloud infrastructure, platform, and hosted code
  + Data security
    - Data integrity
    - Data lock-in
    - Data remanence (residual data after it’s been removed)
  + Issues related to
    - Access control
    - Authentication
    - Authorization
    - Encryption
    - User-id management
  + Compliance issues
    - Security audit
    - Data location
    - Operation traceability etc.
* Transparency
  + Data subjects informed on who processes their data and for what purposes
* Risk analysis between business house and a cloud aministration
* First domain
  + Compliance concerns for
    - Regular audits
    - Inspections
    - Reviews of
      * Data
      * Application
      * Infrastructure
      * Hardware
  + Audits planned by CSP and agreed with stakeholders

## FedRAMP [7]

* Government-wide program, designed for federal agencies
* Standardizes approach for
  + Security assessment
  + Authorization
  + Continuous monitoring for cloud-based services
* Created in collaboration with NIST, GSA, DOD, and DHS
* Purpose
  + Ensure cloud systems used by Government entities have adequate safeguards
  + Eliminate duplication of effort and reduce risk management costs
  + Enable rapid and cost-effective government procurement of information systems/services

## Coalfire [10]

* Identifies the attack vectors
  + Attacking the cloud environment from the internet – emulating an anonymous attacker
  + Attack from within context of a customer’s access
    - Impact a compromised customer system or partner network have by:
      * Escalating privileges within the customer environment
      * Gaining access to CSP backbone infrastructure
      * Compromising other cloud service tenants
  + Attack corporation
    - Gaining foothold in environment via social engineering
    - Collect credentials that have access to the cloud environment
    - Gain access to source code or other sensitive programming material

## Pacu [13]

* Exploitation of configuration flaws within an AWS account
* Uses its modules to expand its functionality
* Range of attacks included such as
  + Privilege escalation
  + Backdooring of IAM users
  + Attacking vulnerable lambda functions
  + Etc.
* Uses Python 3
* 36 modules for AWS attacks

## BishopFox Methodology

* Simulate attacker attempting to access a client’s cloud environment unauthorized – user, application etc.
* Three phases: Pre-assessment, Discovery & Penetration Testing, Analysis & Reporting
* For example
  + Role-based access control misconfigurations providing users with unintended administrative access to cloud resources

### Pre-assessment

Describes what the assessment team should have access to and assess the objectives that are to be met

* Account for configuration review
  + Cloud account with access to
    - API access to cloud environment
    - GUI or console access to cloud environment
    - Security audit permissions
* Accounts for penetration testing
  + A typical user account / compromised application
  + Based on penetration test’s goals or objectives (e.g. software developer’s account)
* Environment access
  + Network access to cloud API and all in-scope services
  + Provisioned through
    - Client laptop with VPN access
    - Jumpbox
    - Direct internet access
* Objectives
  + Primary goals that can include
    - Compromising trophy targets
      * Privileged credentials
      * Customer data
    - Accessing restricted portions of the cloud environment
    - Stealing/exfiltrating data to determine client’s detection capabilities
    - Accessed levels of access and privileges as an attacker
* Scope
  + List in cloud environments (e.g. AWS, Azure, GCP)
* Taking in account of minimizing network availability
* Before testing, discuss risks to environmental stability with client
* Resources hosted on a third-party system will need consent to test

### Information Gathering and Automated Testing

* Configuration enumeration
  + Using open source and proprietary tools to gather config information
    - Service config details
    - Identity and access management (IAM) config data
    - Resource-level access controls, such as data buckets
    - Credentials and other confidential data exposures
  + Using this info to conduct
    - Finding security misconfigs
    - Find cloud privilege escalation paths
    - Map environment’s attack surface
      * Points at which an attacker can enter or extract data
* Network discovery
  + Identify live hosts
    - Cloud Resource Enumeration
      * Query cloud API to find exposed service endpoints
    - Common TCP Port Scanning
      * Used to identify specific TCP ports
      * Target subnets associated with hostnames and domains
* Service and application enumeration
  + After live hosts on target network are identified, list running network services
    - Detailed Port Scans
      * TCP/UDP port scan against known ports and live hosts
    - Service and Application Enumeration
      * Fingerprint and examine running networks and applications

### Penetration Testing

* Attempt to compromise
  + In-scope systems & credentials
  + Perform lateral movement
  + Escalate privileges within target environment
* Conducted by
  + Traversing cloud privilege escalation paths
  + Hunting for exposed secrets and credentials
  + Testing access of identified credentials
  + Find overly permissive network access controls
  + Exploit misconfigured cloud services
  + Exploit vulnerable network services and applications
  + Identify abandoned subdomains

### Analysis and Reporting

* Likelihood determination
  + Based on
    - Threat-source motivation and capability
    - Nature of the vulnerability
    - Existence and effectiveness of controls
* Impact analysis
  + Impact of successful exploitation (affects customers and organization)
* Severity determination
  + Rating methodologies such as OWASP or Common Vulnerability Scoring System (CVSS)
  + Evaluates the likelihood and impact
  + Critical, high, medium, or low
  + Independent for each finding

## CSA Methodology [14]

* Performing tests on the security of the cloud
* PaaS (Platform as a Service) Scope
  + User Access/Identity
  + Data
  + Application
* States that client-side application testing is sufficiently covered by OWASP and other resources
* Concerned with domains
  + Account security
  + Cloud service
    - Misconfigs such as vpc network access restrictions
  + Application / business logic
* Lists the activities used in standard penetration testing as well as ones relevant to the cloud
* 5 phases:
  + Preparation – legal agreements
  + Threat modelling
    - Treacherous 12
  + Reconnaissance and Research
  + Testing
  + Report

## TechBeacon [16]

* Suggests understanding the policies of the cloud provider
  + E.g. DDoS attacks not allowed
  + Penetration testing taking too many resources, risk closing of your account
* Create pen-testing plan with items covered:
  + Application(s)
    - Identify and include user interffaces and APIs
  + Data access
    - How data will be pen tested through application or directly in database
  + Network access
    - How well network protects the application and data
  + Virtualization
    - How well virtual machines isolate the workload
  + Compliance
    - Laws and regulations that are needed to be complied with within the application or database
  + Automation
    - Identify automated pen-testing tools (cloud/not cloud) employed for the penetration test
  + Approach
    - Identify application admins to be included or excluded in pen testing
    - Could use a real-life scenario where attacking excluded admins give a realistic view of their reaction
* Select tools
  + Cloud-based pen testing tools
  + Tool can simulate an actual attack
  + Many use automated processes to find vulnerabilities
  + E.g. guessing paswords repeatedly, APIs with access directly to data
* Observe response
  + Human
    - Admin team and application users response to pen test
    - Tests that aren’t disclosed – more realistic
    - Examples
      * Shutting system down
      * Diagnose issue before identifying and elevating the threat
    - Also, humans at your client provider
  + Automated
    - How the security system can spot and respond to the tests
    - Tiered e.g. blocking IP address generating the pen test to shutting down application down entirely
    - Descriptions about corrective actions sent to admins
  + Finding and eliminating vulnerabilities
    - Examples
      * Access data via API
      * API access granted after 10 attempts
      * VM not isolating workload properly
      * Password guessed using auto-password generator
      * VPN allows outside access if DNS disabled
      * Encryption not compliant with new regulations
    - Different network layers considered – tested and reported separately
  + Being too familiar with the application may lead to oversight

# References

1. Keller, N., 2018. NIST - Getting Started [WWW Document]. NIST. URL <https://www.nist.gov/cyberframework/getting-started> (accessed 2.14.22).
2. CSRC, 2016. NIST Cybersecurity Framework: A Quick Start Guide [WWW Document]. CSRC | NIST. URL <https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide> (accessed 2.14.22).
3. MITRE ATT&CK® [WWW Document], n.d. URL <https://attack.mitre.org/> (accessed 2.14.22).
4. Moyle, E., 2021. What are cloud security frameworks and how are they useful? [WWW Document]. SearchCloudSecurity. URL <https://searchcloudsecurity.techtarget.com/tip/What-are-cloud-security-frameworks-and-how-are-they-useful> (accessed 2.15.22).
5. CSA [WWW Document], 2021. . CSA. URL <https://cloudsecurityalliance.org/research/cloud-controls-matrix/> (accessed 2.15.22).
6. Saxena, S., 2013. Ensuring Cloud Security Using Cloud Control Matrix 6.
7. FedRAMP [WWW Document], n.d. URL <https://www.fedramp.gov/> (accessed 2.15.22).
8. Verry, J., 2018. What is a NIST Penetration Test? [WWW Document]. Pivot Point Security. URL <https://www.pivotpointsecurity.com/blog/what-is-a-nist-penetration-test/> (accessed 2.15.22).
9. Penetration testing requirements for NIST SP 800-53, 2021. . BreachLock. URL <https://www.breachlock.com/penetration-testing-requirements-for-nist-sp-800-53/> (accessed 2.15.22).
10. Cloud security penetration testing [WWW Document], n.d. . Coalfire.com. URL <https://www.coalfire.com/solutions/cloud-security/cloud-security-penetration-testing> (accessed 2.15.22).
11. WSTG - Stable | OWASP Foundation [WWW Document], n.d. URL <https://owasp.org/www-project-web-security-testing-guide/stable/2-Introduction/README> (accessed 2.15.22).
12. Harvey, S., 2019. What is the Open Source Security Testing Methodology Manual (OSSTMM)? [WWW Document]. KirkpatrickPrice Home. URL <https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/> (accessed 2.15.22).
13. Pacu GitHub, 2022. . Rhino Security Labs. URL <https://github.com/RhinoSecurityLabs/pacu> (accessed 2.15.22)
14. Cloud Penetration Testing Playbook [WWW Document], n.d. . CSA. URL <https://cloudsecurityalliance.org/artifacts/cloud-penetration-testing-playbook/> (accessed 2.15.22).
15. Johnson, J., 2018. Our Web Application Penetration Testing Methodology » Triaxiom Security. Triaxiom Security. URL <https://www.triaxiomsecurity.com/our-web-application-penetration-testing-methodology/> (accessed 2.18.22).
16. Linthicum, D., n.d. Penetration testing cloud-based apps: A step-by-step guide [WWW Document]. TechBeacon. URL <https://techbeacon.com/enterprise-it/pen-testing-cloud-based-apps-step-step-guide> (accessed 2.19.22).