TATA COMMUNICATIONS

TATA

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

TATA COMMUNICATIONS – VAPT SERVICES OVERVIEW

MAR 2020

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

We deliver Tata Communications' 'VAPT' services via an SaaS (Software as a Service) cloud model in Manged Services and in a Consulting Model (One time testing). They're primarily for customers who need both their network and web applications monitoring for new vulnerabilities and malware that could infect site visitors. Our Security Operations Centre (SOC) - part of the Global Services Management Centre (GSMC) - monitors and manages service availability, and assists customers to schedule remote scans on a 24/7/365 basis.

SERVICE OVERVIEW

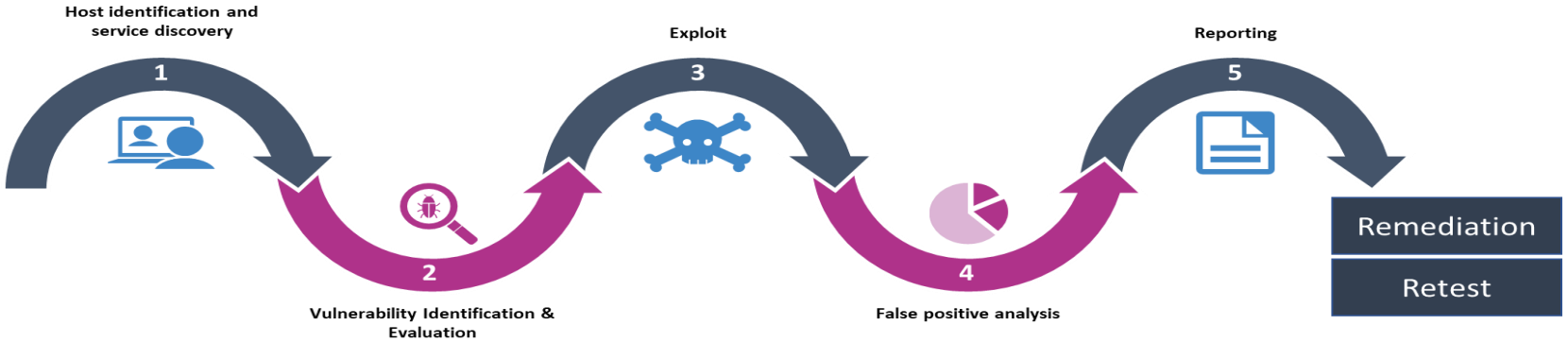
- Network
  - ✓ Vulnerability management - to identify network vulnerabilities before they're breached
  - ✓ Penetration testing - to verify potential network impact of vulnerability exploits
- Web application
  - ✓ Vulnerability scanning for dynamic web applications
  - ✓ Malware detection
  - ✓ Penetration testing - to verify potential web app impact of vulnerability exploits

VAPT – DELIVERY MODEL

- **Managed Services**
  - Vulnerability Assessment Service
    - Network/Servers (Internal & External)
  - Penetration Testing Services (Internal & External)
  - Web Application Security Assessment Service
  - Mobile Application Security Testing (Android/IOS)
  - Phishing Simulation Campaign

- **Consulting Services (One time Testing Services)**
  - Vulnerability Assessment Service
  - Penetration Testing Services (Internal & External)
  - Web Application Security Assessment Service
  - Mobile Application Security Testing (Android/IOS)
  - Phishing Simulation Campaign

TCL METHODOLOGY



At Tata Communications we follow a rigorously defined methodology to identify security findings within our clients' infrastructure. All our security assessments feature the following phases:

- **Host identification:** through detailed reconnaissance
- **Vulnerability Identification and Evaluation:** We perform detailed vulnerability scans against identified scope and evaluate the vulnerabilities according to risk score and business criticality after discussion with Customer SPOC.
- **Exploit:** Final list of Vulnerabilities exploited with advance tools and manual technique to determine the impact on the scoped targets.
- **False positive analysis:** We analyse all findings for impact, severity and criticality.
- **Reporting:** We develop recommendations for mitigating risk or implementing compensating controls to reduce risk to an acceptable level.
- **Retest :** Retest will be performed after the remediation.

ASSESSMENT APPROACH

Planning & Preparation	➢ **Assets Identification** ➢ **Stake holders identification** ➢ **Detailed Schedule / test plan for each activity with date and time** ➢ **Identify the business impacts if any for assessment** ➢ **Discuss and Meet Stakeholders, Communicate and get Approvals from stakeholder**
Information Gathering and Analysis	➢ Information about network segments ➢ Perform Network discovery to determine the reachable systems in the IT infrastructure. ➢ Identify the targets for Vulnerability Assessment and Penetration Testing.
Assessment Phase (VA & PT)	➢ Internal VAPT, External VAP, Application Security Testing, Server VAPT & Wireless PT ➢ Identify Vulnerabilities & Security Risk ➢ Exploit the Vulnerabilities & Clean-up
Review and Reports	➢ Review the scan results manually to eliminate false-positives. ➢ Consolidate the scan results once the false-positives are removed and final vulnerabilities including CVE numbers along with recommendation for remediation. ➢ Present executive summary report for senior management in word and ppt format. ➢ Detailed VA and PT assessment report.
Remediation Phase	➢ Customer asset owners will perform the remediation activity, TCL will be provide guidance wherever required.
Verification of the Remediation	➢ TCL will Re-perform the vulnerability or penetration test to verify the results.

Project Management

- **Project Management personnel to oversee the Project and interface between both companies.**
- **Complete tracking of Project schedule, Execution and Reporting.**

VULNERABILITY ASSESSMENT

Internal | **External**

Vulnerability Management Process

- Leverage VM Process
- Discuss with Stake holders
- Identify Assets in scope
- Schedule the date and time

Planning

- Performing Vulnerability scanning of the assets at agreed time

Vulnerability Analysis

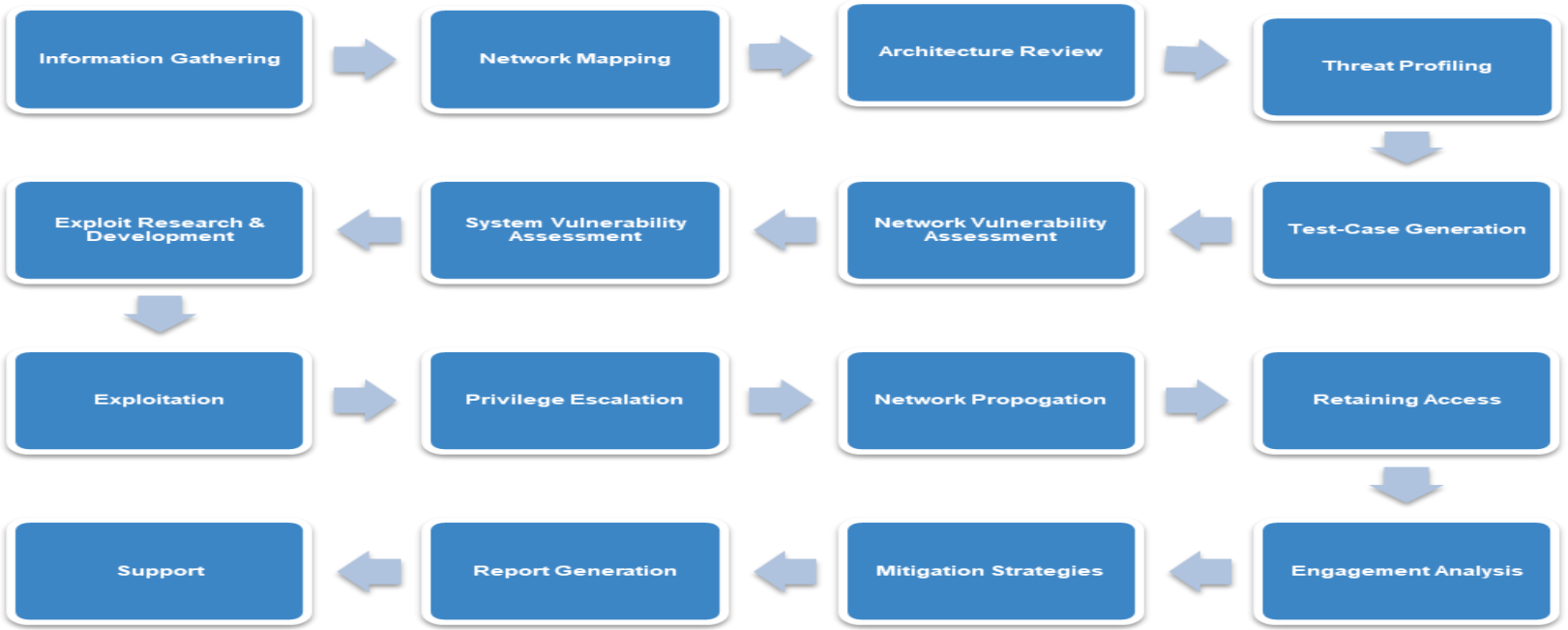
- Results verification & validation
- False Positive Scrubbing
- Results categorization based on vulnerability types

Reporting

- Publishing comprehensive assessment report.
  - Executive Summary
  - Technical Details

PENETRATION TESTING

Tata Communications' Penetration Testing simulates techniques used by hackers to help you understand potential threats while providing detailed recommendations.

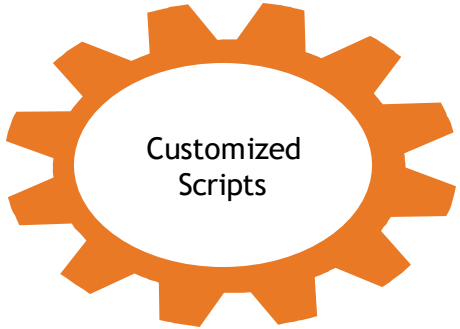


APPLICATION SECURITY TESTING

Application security testing aims to emulate external and internal directed attacks on the web application to identify any weaknesses which may provide unauthorized access or disruption to systems or data

VAPT – TOOLS IN FOCUS

TCL - OEM Partners :
- ✓ Qualys
- ✓ Tenable
- ✓ Rapid7
- ✓ Microfocus



TATA COMM VAPT TEAM - SKILLS & CERTIFICATION

VAPT Team Strength: Certified Resources spread across (India, Singapore and Dubai)

- CREST Certified and Trained professionals
- OSCP (Offensive Certified Security Professional)
- OSCE (Offensive Certified Security Expert)
- CEH (Certified Ethical Hacker)
- ECSA (EC-Council Certified Security Analyst)
- ITIL (Information Technology Infrastructure Library)
- Qualys Certifications for VA and Application
- Other Network Certifications

ADDING VALUE THROUGH ENGAGEMENT

Our four-step engagement model is designed to increase the success of our work and the value to our clients. We first ask scoping questions and use the information gathered to perform a penetration test. We then report on our findings and review them with our client to inform remediation planning.

- ✓ **Tailored approach** – around the specifics of every client
- ✓ **Structured methods and expert delivery** - using a defined methodology delivered by trained professionals
- ✓ **Quantitative results** - meaningful for clients and their remedial planning

PILLARS OF STRENGTH

Experienced security consultants

- Senior security consultants with cross-industry experience
- Experienced in providing consultation on security architecture, frameworks and compliance

Coverage across the globe

- Global coverage for GRC security consulting and assessment projects through onsite / offshore model delivered from Singapore, India, Dubai

Security consulting advisories

- Expertise in providing security advisories and benchmarking across the industry. Provide daily threat advisories to esteemed customers across globe.

Security certifications

- Security consultants certified with various globally accepted standards including CREST, OCSP, OSCE, CEH, ECSA, CISSP, CISA and More.,

https://www.tatacommunications.com/threat-advisory/

REPORTING

TEST REPORTS OVERVIEW

MANAGEMENT EXECUTIVE REPORT

- High level summary
- Key metrics
- Root cause analysis
- Risk analysis

EXCEL DASHBOARD

- Vulnerability details
- Risk scoring
- Detailed metrics
- Track patch status and action items

TECHNICAL REPORT

- Detailed description
- Proof of concepts
- How to fix with source-code examples
- Reference documents

Executive Summary Report

Excel Dashboard - VA Report

Technical Report - App Sec Test

DETAILED REPORTS

Our Penetration test report provides:

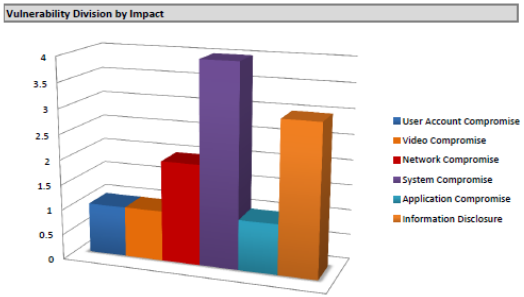
- Executive summary
- Risk statement
- Finding description
- Infrastructure impact
- Risk severity
- Recommendations

External PT

4.0 Recommendation Summary

We have addressed the identified vulnerabilities and provided recommendations to mitigate the risk involved immediately.

- Implement input validation mechanism.
- Eliminate user control and use secure sessions to hold and manage such information.
- Implement strong validation to check the file extensions and type of file being uploaded
- Implement strong permissions and restrictions on SQL users and databases.
- Implement strong production and development processes to prevent unapproved files from reaching a production environment.
- Write code with managed errors and disable error messages in server configuration.
- Install URLScan and disable In-secure HTTP methods through this tool.



Impact:	Video Conferencing Compromise	**Cause:**	Insecure Configuration
Who will fix:	Network Administrator	**Difficulty of fix:**	Easy

Instances

IP Address	Protocol and Port	Details
10.165.52.78	TCP 443	LifeSize Video Conferencing System

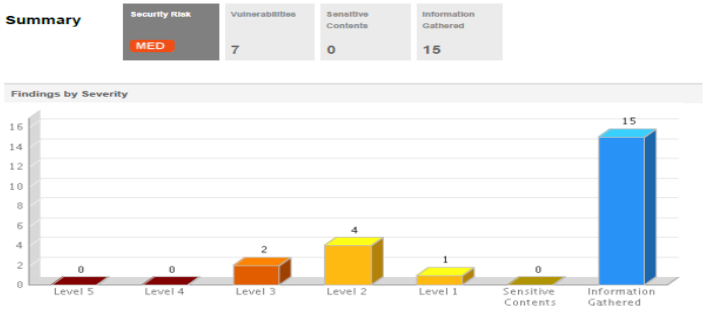
Proof-Of-Concept

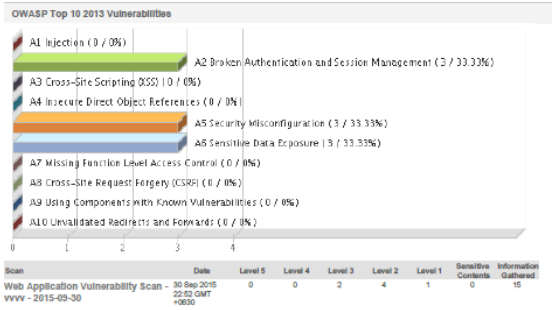
Recommendations

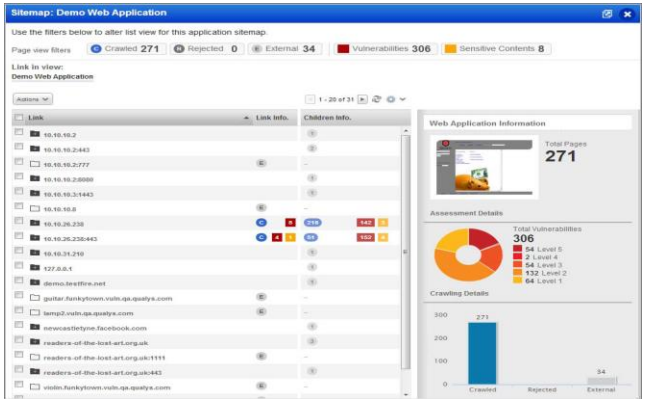
Video Conferencing System should be disallowed over the internet. Additionally it's advisable to disable the default username or set a strong password for the same.

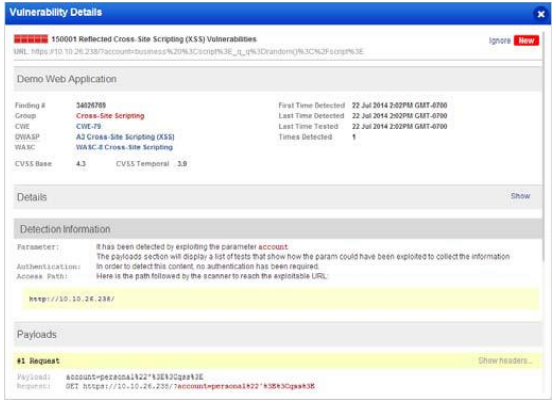
Sample VA & Standard PT Repor

WEB APPLICATION ASSESSMENT - SAMPLE REPORTS









KEY CUSTOMERS

Due to NDA in place, we will not be listing some of our key Banking and Finance Customers.

TATA COMMUNICATIONS

CASE STUDY

Hindustan Coca-Cola Beverages Pvt. Ltd.

HCCBPL (Hindustan Coca-Cola Beverages Pvt Ltd) is an Indian Subsidy of Coca-Cola which acts as umbrella organization for all local and global compliance requirements. HCCBPL requirement is to comply the Security assessment and compliance requirements with its parent organization.

Customer's Need

- HCCBPL required Internal and External Posture to be assessed on on-going basis in regular Interval for 3 years.
- Identify the Internal/External posture and exposure.
- Examine the external infrastructure from internet
- Vulnerabilities that can be exploited by external resources
- External Business Applications vulnerabilities
- Critical Mobile Applications Security Risks

TCL Solution

TCL proposed the Gray/Black box perspective of VA and Penetration testing for the customer requirement. In this method, TCL VAPT team will act as an external resource who doesn't know anything about the target network and try to identify the information of the target network and its associated vulnerabilities.
TCL proposed the scanning activity over internet without whitelisting to identify the vulnerabilities in the black box perspective.

Approach

- Scope confirmation
- Identify the target network IPs and range
- Ports/service identification
- Vulnerability identification
- Correlate and analyze the vulnerability
- Identify the exploitable vulnerabilities
- Manual and automated method of exploiting
- Identify the risk level and impact
- Recommend Mitigation

Deliverables

- Executive report with high level overview of activity
  - Identified Vulnerabilities
  - Business Risk Level
  - Roadmap for remediation
- Detailed report
  - IP/Vulnerability
  - Impact
  - Risk Level/CVE
  - Solution/Recommendation

WHY TATA COMMUNICATIONS?

- We provide our clients with customized, industry approved approaches for assessment.
- TCL customized framework and approach for network/application PT.
- Highly Experienced, CREST Trained and OSCP, OSCE, CEH certified professionals.
- Dedicated Lab setup with leading commercial and open source tools for assessing public facing infrastructures.
- Retest
- OWASP Top 10 and CVE scoring based reports.
- Leading commercial tools for VA and Automated PT.
- Customized reports based on the requirement. Detailed finding Reports with recommendations in Excel format and High-level executive reports.
- TCL have different customers across all the verticals. TCL provided the security consulting services to leading national banks, logistics, retails and beverages industries in India and other regions.

THANK YOU

THE SCIENCE BEHIND SECURITY

M ULTI-LAYERED I NTEGRATED S ECURE T RUSTED

TATA COMMUNICATIONS | CLOUD NETWORK MOBILITY SECURITY