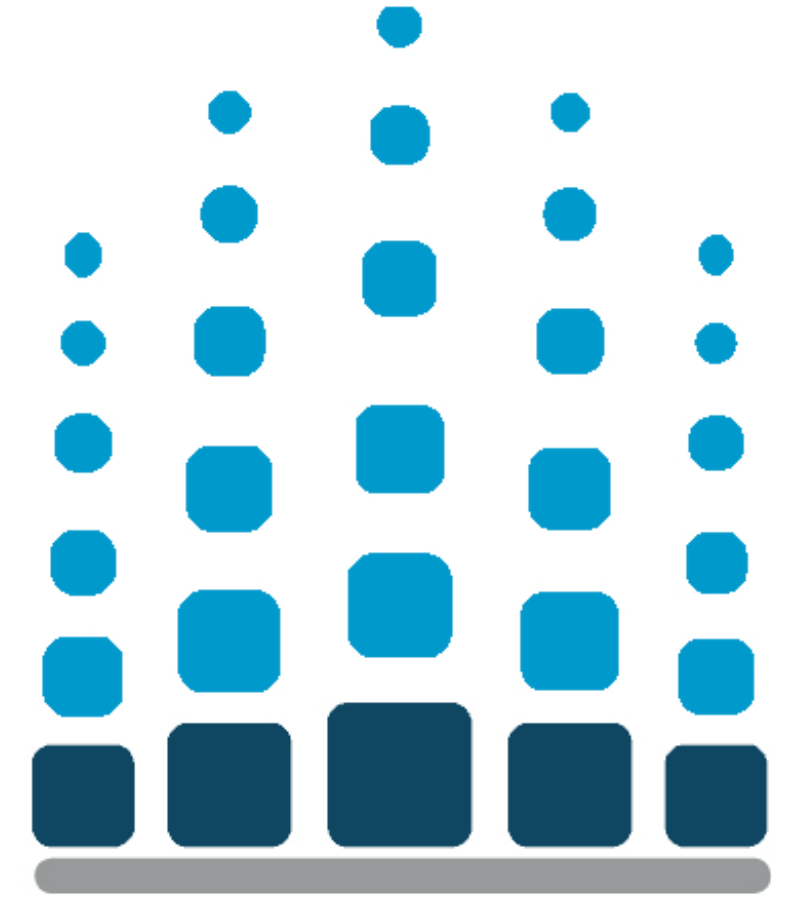
Building Telco Businesses

Invoice Portal Penetration Test Plan



2 January 2018 Version: 1.0

Prepared by: George Stewart

Table of Contents

Commercial-in-Confidence

Executive Summary

This document, prepared by Colman Communciations, defines the scope of the penetration test against BTB's Invoice Portal, rules of engagement, and checklists that need to be completed before the penetration test can commence.

The assessment is planned to start on 3 January 2018, conclude on 12 January 2018, with delivery of a draft report on 15 January 2018.

BTB Responsibilities

- Provide a single point of contact with the authority and responsibility to make binding decisions in relation to matters within the scope of this engagement.
- Provide timely responses to all queries throughout the engagement.
- Ensure that appropriate IT service and business function owners have been adequately informed of the project and agree to provide support and information as requested.
- Co-ordinate all activities with IT operations, business owners and other third parties and is responsible for any direct project management activities including change control and associated requirements.
- Maintain backups and other means of recovering services and data that may be adversely affected.
- Inform Colman Communciations immediately of any detected adverse effects caused by testing, and early termination of testing if required.
- Inform Colman Communciations immediately of any changes to ownership of in-scope systems, or the inclusion of any third party servers, devices and services in the assessment scope.
- Complete all activities in the checklist at the end of this document and notify Colman Communciations at least two business days prior to planned test commencement.
- Inform Colman Communciations immediately if a variation to the schedule is required.
- If retesting report findings is in scope, a single exercise will be scheduled within two (2) weeks of the report delivery, unless another time is agreed in the kick-off meeting.

Scope

Background

Building Telco Businesses (BTB) is a company specialising in whitelabling broadband telecommunications services to businesses with existing customer bases. BTB provide the complete range of services required to operate an internet service provider, allowing their customers to focus on the sales and marketing.

BTB has entered into an agreement with a large energy provider to whitelabel their services, who has specified that their systems be subject to network and web application penetration testing prior to launch. One round of testing has been completed, with a second required.

Part of BTB's offering is an Invoice Portal, which requires security testing. In addition, further retesting is required from the previous round of penetration testing.

Threat Model

Several threats have been identified as being of interest:

- Attacks from application users
- Attacks from the broader Internet

Of particular concern to BTB are attacks that could result in:

- Remote compromise of BTB systems
- Unauthorised disclosure of commercial and/or personally identifiable information
- Fraud or other loss of money

BTB have stated that all users should have access to all functions.

Activities

The following activities are in-scope for this assessment:

- A penetration test of the Invoice Portal
- Delivery of a single report covering all activities above
- Retesting of fixes implemented for vulnerabilities identified during the assessment and confirmation they are effective
- A review of remediation performed as a result of previous testing:
    - Missing/Default passwords
    - Domain privileges

Exclusions

The following activities are out of scope:

- Colman Communciations will not implement fixes for vulnerabilities identified the assessment
- Denial of service is out of scope
- Social engineering is out of scope
- Any activities not explicitly defined as in-scope is out of scope

Rules of Engagement

Proposed Dates

Milestone	Date
Test Start	3 January 2018
Test End	12 January 2018
Draft Report Delivery	15 January 2018
Acceptance of Final Report	19 January 2018

System Details

The following system details have been provided:

System	IP/URL	Entry Point
Invoice Portal	http://10.3.65.74:9999/	http://10.3.65.74:9999/
Retest systems	10.3.11.11, 10.3.11.12, 10.3.11.13, 10.3.11.14, 10.3.11.16, 10.3.11.17, 10.3.11.18	N/A

Accounts

The following accounts will be supplied:

Account Type	Number	System
Portal User	3	Invoice Portal
Domain Administrator	1	b2b.local

Contacts

Name	Role	Number	Email
George Stewart	Penetration Tester	0432 918 830	george.stewart@colmancomm.com
Sachin Patel	GM - Product & Technology	0411 655 405	sachin@btbaustralia.com.au
Graham Corrigan	GM - Software and Architecture	0409 368 903	graham@btbaustralia.com.au
Clem Colman	Security Consultant	0417 744 511	clem@colmancomm.com

Permitted Activities

The following table shows activities that are permitted and those that are expressly forbidden. Any activity not included in this list is forbidden by default.

Colman Communciations will seek specific agreement should any actions potentially affect the integrity or availability of

targeted systems.

External testing

Activity	Execution Permission
Network scanning and service identification	PERMITTED
Vulnerability scanning and identification	PERMITTED
Vulnerability exploitation	PERMITTED
Modification of system configurations	PERMITTED (CINDY ONLY)
Modification of application/business data	PERMITTED (CINDY ONLY)
Brute force attempts	PERMITTED
Denial of Service (DoS) testing	NOT PERMITTED
Social engineering	NOT PERMITTED

Third Parties

The following third parties have been identified as managing systems under test, or as being likely to recieve security events while testing is underway. They should be notified that the penetration test is taking place, and given a chance to warn users, security teams, system managers and upstream providers that there may be a potential interuption to services and/or a large number of security events generated.

- N/A

Source IPs

The penetration test will be performed from the following IP addresses:

- N/A

Intrusion Detection Systems and other automatic countermeasures operated by BTB or other third parties should be configured to ignore traffic from these addresses for the test.

Checklist

The following pre-requisites must be met before Colman Communciations can begin the penetration test:

- Ownership of target systems confirmed
- Disaster recovery in place and tested
- System owner(s) notified of activity
- Acknowledgement of client responsibilities
- Acceptance of rules of engagement
- Third parties identified
- Third parties notified of activity

In addition to the accounts, IP addresses and entry points defined above, BTB will provide the following:

- Application frameworks, libraries and versions
- Application source code

The following activities must be completed to confirm environment readiness:

- Provide VPN access
- Environment access tested by BTB
- Environment access confirmed by Colman Communciations
- Test accounts created by BTB
- Test account details supplied to Colman Communciations
- Test accounts confirmed by Colman Communciations
- Intrusion Detection Systems disabled
- Provide domain administrator credentials

Document Management

Filename

btb_invoice_portal_2018_test_plan_v1.0.pdf

Change History

Version	Date	Author	Change Description
0.1	2 January 2018	George Stewart	Draft complete
0.2	2 January 2018	Clem Colman	Internal QA
1.0	2 January 2018	George Stewart	Initial release to client

Referenced Documents

Title	Filename	Version
N/A	N/A	N/A

Disclaimer

Colman Communciations notes that penetration tests are limited in a number of aspects:

- They are conducted with limited resources over a limited period of time. An attacker may not face the same constraints.
- They are a point in time assessment. Changes to the security landscape including the discovery of new vulnerabilities, attack techniques, and changes in the CINDY and corporate network infrastructure 's configuration may lead to new vulnerabilities over time.
- They are performed in a specific environemnt. There may be differences in configuration between the environment assessed and others.

As a result, Colman Communciations gives no guarantee, warranty, or assurance that the services it has performed and provided pursuant to the assessment will have the effect of:

- Identifying an exhaustive list of all threats and risks to the Client's systems;
- Documenting all possible controls that might be applied to remediate identified threats and risks; and or
- Being continually accurate and relevant as threats and risks as identified by the Vendor (and any recommended controls) may be time specific.

Threats and risks to assessed systems and controls that have been implemented to remediate such risks and threats should be reviewed regularly to ensure their currency and efficacy.