Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240



**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |

**[Insert PROJECT or Service Name]**

**Penetration Test**

**Scoping Document**

**Origin/Author(s): [Insert Author of document]**

**Date Approved: [Insert approved date]**

**Version: [insert version number, this should reflect the change on page 3]**

**Contents**

Document control 8

1. Introduction 9

1.1 Overview 9

1.2 Location 9

1.3 Dates of Testing 9

1.4 General 9

2. Background & technical Information 10

3. Scope 11

3.1 Target Area List 17

3.2 Security targets out-of-scope 18

3.3 Principle security concerns 18

4. Test specifics 20

4.1 Daily reporting 20

4.2 Final report 20

4.3 Assumptions 21

Appendices 23

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 23

Appendix 2 – Application flows/user journey 23

Appendix 3 – Application screenshots 23

Appendix 4 – NTA Monitor scoping questionnaire 23

Appendix 5 – NTA Monitor test plan 23

Glossary: 24

Document control 32

1. Introduction 33

1.1 Overview 33

1.2 Location 33

1.3 Dates of Testing 33

1.4 General 33

2. Background & technical Information 34

3. Scope 35

3.1 Target Area List 41

3.2 Security targets out-of-scope 42

3.3 Principle security concerns 42

4. Test specifics 44

4.1 Daily reporting 44

4.2 Final report 44

4.3 Assumptions 45

Appendices 47

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 47

Appendix 2 – Application flows/user journey 47

Appendix 3 – Application screenshots 47

Appendix 4 – NTA Monitor scoping questionnaire 47

Appendix 5 – NTA Monitor test plan 47

Glossary: 48

Document control 56

1. Introduction 57

1.1 Overview 57

1.2 Location 57

1.3 Dates of Testing 57

1.4 General 57

2. Background & technical Information 58

3. Scope 59

3.1 Target Area List 65

3.2 Security targets out-of-scope 66

3.3 Principle security concerns 66

4. Test specifics 68

4.1 Daily reporting 68

4.2 Final report 68

4.3 Assumptions 69

Appendices 71

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 71

Appendix 2 – Application flows/user journey 71

Appendix 3 – Application screenshots 71

Appendix 4 – NTA Monitor scoping questionnaire 71

Appendix 5 – NTA Monitor test plan 71

Glossary: 72

Document control 80

1. Introduction 81

1.1 Overview 81

1.2 Location 81

1.3 Dates of Testing 81

1.4 General 81

2. Background & technical Information 82

3. Scope 83

3.1 Target Area List 89

3.2 Security targets out-of-scope 90

3.3 Principle security concerns 90

4. Test specifics 92

4.1 Daily reporting 92

4.2 Final report 92

4.3 Assumptions 93

Appendices 95

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 95

Appendix 2 – Application flows/user journey 95

Appendix 3 – Application screenshots 95

Appendix 4 – NTA Monitor scoping questionnaire 95

Appendix 5 – NTA Monitor test plan 95

Glossary: 96

Document control 104

1. Introduction 105

1.1 Overview 105

1.2 Location 105

1.3 Dates of Testing 105

1.4 General 105

2. Background & technical Information 106

3. Scope 107

3.1 Target Area List 113

3.2 Security targets out-of-scope 114

3.3 Principle security concerns 114

4. Test specifics 116

4.1 Daily reporting 116

4.2 Final report 116

4.3 Assumptions 117

Appendices 119

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 119

Appendix 2 – Application flows/user journey 119

Appendix 3 – Application screenshots 119

Appendix 4 – NTA Monitor scoping questionnaire 119

Appendix 5 – NTA Monitor test plan 119

Glossary: 120

Document control 128

1. Introduction 129

1.1 Overview 129

1.2 Location 129

1.3 Dates of Testing 129

1.4 General 129

2. Background & technical Information 130

3. Scope 131

3.1 Target Area List 137

3.2 Security targets out-of-scope 138

3.3 Principle security concerns 138

4. Test specifics 140

4.1 Daily reporting 140

4.2 Final report 140

4.3 Assumptions 141

Appendices 143

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 143

Appendix 2 – Application flows/user journey 143

Appendix 3 – Application screenshots 143

Appendix 4 – NTA Monitor scoping questionnaire 143

Appendix 5 – NTA Monitor test plan 143

Glossary: 144

Document control 152

1. Introduction 153

1.1 Overview 153

1.2 Location 153

1.3 Dates of Testing 153

1.4 General 153

2. Background & technical Information 154

3. Scope 155

3.1 Target Area List 161

3.2 Security targets out-of-scope 162

3.3 Principle security concerns 162

4. Test specifics 164

4.1 Daily reporting 164

4.2 Final report 164

4.3 Assumptions 165

Appendices 167

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 167

Appendix 2 – Application flows/user journey 167

Appendix 3 – Application screenshots 167

Appendix 4 – NTA Monitor scoping questionnaire 167

Appendix 5 – NTA Monitor test plan 167

Glossary: 168

Document control 176

1. Introduction 177

1.1 Overview 177

1.2 Location 177

1.3 Dates of Testing 177

1.4 General 177

2. Background & technical Information 178

3. Scope 179

3.1 Target Area List 185

3.2 Security targets out-of-scope 186

3.3 Principle security concerns 186

4. Test specifics 188

4.1 Daily reporting 188

4.2 Final report 188

4.3 Assumptions 189

Appendices 191

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 191

Appendix 2 – Application flows/user journey 191

Appendix 3 – Application screenshots 191

Appendix 4 – NTA Monitor scoping questionnaire 191

Appendix 5 – NTA Monitor test plan 191

Glossary: 192

Document control 200

1. Introduction 201

1.1 Overview 201

1.2 Location 201

1.3 Dates of Testing 201

1.4 General 201

2. Background & technical Information 202

3. Scope 203

3.1 Target Area List 209

3.2 Security targets out-of-scope 210

3.3 Principle security concerns 210

4. Test specifics 212

4.1 Daily reporting 212

4.2 Final report 212

4.3 Assumptions 213

Appendices 215

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 215

Appendix 2 – Application flows/user journey 215

Appendix 3 – Application screenshots 215

Appendix 4 – NTA Monitor scoping questionnaire 215

Appendix 5 – NTA Monitor test plan 215

Glossary: 216

Document control 224

1. Introduction 225

1.1 Overview 225

1.2 Location 225

1.3 Dates of Testing 225

1.4 General 225

2. Background & technical Information 226

3. Scope 227

3.1 Target Area List 233

3.2 Security targets out-of-scope 234

3.3 Principle security concerns 234

4. Test specifics 236

4.1 Daily reporting 236

4.2 Final report 236

4.3 Assumptions 237

Appendices 239

Appendix 1 – NHSBSA [insert project or service name] Firewall/Security Groups 239

Appendix 2 – Application flows/user journey 239

Appendix 3 – Application screenshots 239

Appendix 4 – NTA Monitor scoping questionnaire 239

Appendix 5 – NTA Monitor test plan 239

Glossary: 240

# **Document control**

**Status:**

|  |  |
| --- | --- |
| **Author** | Name and role of author] |
| **Status** | [Draft or Approved] |

**Change log:**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.1 | [dd/mm/yyyy] | First draft prepared by [insert name] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Template completion instructions

[Follow the instructions given in the guidance. These appear in-line throughout the template in the same format as this statement.

All guidance statements should be removed from the completed scope together with this Template Completion instructions subsection. There should be no blue font left in the completed template]

# **1. Introduction**

## **1.1 Overview**

This document defines the scope of the Penetration Test on [insert Project or Service name]

## **1.2 Location**

The testing will take place from the offices of the test company.

13-15 Railway Street

Chatham

Kent

ME4 4HU

## **1.3 Dates of Testing**

The Penetration Test will take place from [Insert required start and end dates of testing]

Testing will be conducted [during business hours 9-5pm / out of hours 5pm -8am, weekend]

## **1.4 General**

The NHSBSA Dev Ops Engineer contact is:

[supply name and contact number of the DevOps person dealing with the migration of your service to the Production environment]

The Technical Contact during the test is:

[supply name and contact number, maybe project senior developer and /or technical architect?]

The Escalation point for any unresolved queries or issues are:

The Project Manager is:

[supply name and contact number, maybe Project Manager?]

The NHSBSA Vulnerability Management Team contact is:

[supply name and contact number of whoever s leading your pen test from an Information Security (IS) point of view, speak to IS if unsure]

# **2. Background & technical Information**

The NHSBSA is a Special Health Authority which provides a range of essential central services to NHS organisations’, NHS contractors, patients and the public.

[Insert the background, why carry out the test. An overview of the system including any constraints. Please include infrastructure diagrams in this section rather than embedding the HLTAD. You can however add the HLTAD for reference as an Appendix at the end of this document if it is not excessive in size.

If testing is to be carried out across multiple VLANS or segregated networks, then you will need to advise the number of VLANs]

# **3. Scope**

The scope of this Penetration Test is targeted at the hosts being deployed for the [insert Project or Service name]services.

The test would consist of the following distinct components: [Please delete component sections that are not required]

**3.A. Exposure testing**

Is one of the most common types of test and involves finding details about the target systems on the network, identifying any available network services and open ports, and looking to try and identify ways into and out of the devices or environment. Often this testing takes place remotely, targeting the perimeter networks. It can also be launched locally, from the targets Local Area Network (LAN), to assess the security of the internal network or the De-Militarised Zone (DMZ) from within, seeing the kinds of vulnerabilities an internal threat actor could exploit.

**3.B. Server build review**

Involves searching for weaknesses and misconfigurations in the basic build of the operating systems of any identified system or device. This will require Admin or root level access to the hosts.

**3.C. Firewall review**

Maps the deployed rule base or Access Control List (ACL) looking for weaknesses or configurations that are deemed to be overly permissive or which would increase the risk level to the solution or the wider network/environment.

[If Firewall rule review is required then you must include the following detail in the target kit list:

* How many firewalls are to be reviewed and what make/version of firewalls are they
* Is this a ruleset review (where a number of selected rulesets are to be reviewed disregarding the general firewall configuration) or full configuration review?
* How many rulesets are there to be reviewed on each firewall?
* Could an electronic, plaintext copy of the ruleset /configuration be provided?
* Could testing be conducted remotely - i.e. a copy of the firewall configuration is provided via a secure and accredited/approved channel?

The firewall rule set/security rules should be attached at Appendix 1.

**3.D. Database configuration review**

Depending on the type and version of the database generally this review is conducted in line with the industry accepted security benchmark. The database configuration will be audited to establish the following security concerns:

* Presence of default user names and passwords
* Database is listening on its default port
* Database service is restricted to a set of whitelisted IP addresses
* Connection and authorisation restrictions
* Owner of the process is sufficiently restricted
* Excessive user privileges
* Encrypted channel of communication
* Excessive number of super users
* Limit on the number of connections
* Overly permissive data files, log files of configurations (permissions or owners)
* Logging and audit policies

**3.E. Application testing**

Looks for security vulnerabilities or misconfiguration in the applications and programs deployed and installed on the target systems. This should include business logic testing. Scope of the testing may include but is not limited to the following:

* Session management
* Role separation
* Privilege escalation
* Input validation – e.g. Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Uniform Resource Locater (URL) redirection etc.
* Data caching
* Injection
* Insecure direct object references
* Security misconfiguration
* Insecure cryptographic storage
* Opportunities for sensitive data exposure
* Failure to restrict URL access
* Missing function level access control
* Exposure testing [especially if the application is internet facing]

[If Application testing is required you must include the following detail in section 2 ‘Background & technical Information’:

* How many dynamic pages
* How many static pages
* How many roles and what type
  + Is test data required, i.e. National Insurance numbers (NINOs), case reference numbers etc.
  + Is the application internet facing? If so, should it be subject to an external Network Assessment?
  + Does the application use an API? If so, should it be subjected to Web Services Testing?
  + If the web application is not internet facing - could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?

The URLs/access points and roles for testing the application should be documented. You may use a sample of roles covering a wide range of access if there are many roles within the application. Screen shots of the application may be beneficial and can be included in the appendix where available. If a roles matrix is available please supply this as an appendix]

**3.F. Web service testing**

Web services or API provide an attack vector which is not dissimilar to Application testing. Frequently the severity of a security breach on an API is much greater than the application testing due to the level of access often granted to the API user.

The specific tests are entirely dependent on the type of web service in use, however the following areas are regarded as potential threats to web services:

**Communication**

* Man-in-the-Middle attacks
* Use of suitable cipher suites
* Adequate server certification
* Web Services routing security
* Replay attacks

**Web service engine**

* Buffer overflows
* XML parsing errors
* Spoiling schema
* Complex or recursive structure as payload
* Session information leakage

**Web services deployment**

* Fault code leaks
* Privilege escalations
* Customized error messages (information leakage)
* Parameter tampering
* SQL/XPATH/LDAP/OS command injection
* Password brute force attacks
* Directory traversal
* Content spoofing
* Sessions tampering

**[**If Web services testing is needed then you must include the following detail:

* What type of web services are to be tested -SOAP or RESTful API?
* If SOAP:
  + How many API or WSDL are there?
  + How many SOAP operations for each API?
* If RESTful API:
  + How many URLs are there?
* Could testing be conducted remotely?
* If API is only exposed to internal infrastructure, could testing be conducted remotely using a secure VPN connection such as an IPSec VPN?]

**3.G. Static source code review of Infrastructure As Code (IAC)**

The review provides an in-depth analysis of the source code, highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent upon the application functionality however the following areas are common to most source code analysis reviews:

* Best practice adherence
* Deployment review processes
* Assessments of:
  + Input validation
  + Error handling
  + Session management
  + Authentication
  + Cryptography
  + Logging
  + Denial of service

[If Static source code analysis is required then you must include the following detail in section 2 ‘Background & technical Information’:

* How many applications are to be reviewed?
* What programming language is used by each of the applications?
* How many lines of code are there in each application?
* Note the number of lines of code should include all of the bespoke libraries, classes, configuration files and ‘launcher’ scripts]

**Application flows/user journey can be seen in Appendix 2**

**Application screenshots are provided in Appendix 3**

## **3.1 Target Area List**

The details of the target devices in the scope of this Penetration Testare provided in the table below:

[Where the target list comprises of multiple instances of target types a sampling approach may be adopted (this should not be less than 10% of the assets). This will consist of all targets being scanned and the sample targets being tested in full and only the differences being additionally tested. Please indicate if this is required]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Description** | **Hostname** | **IP Address** | **Test type** | **Testing location** | **In or out of hours** |
| [To include device types, Operating system details etc. If multiple hosts of the same nature are to be tested please use a separate row for each, this includes firewalls. If firewalls are in scope you must include the approximate number of rules on each firewall, along with the type and model] | [If available] | [If available, if not known please indicate how many IP’s per device] | [This should be taken from Section 3, i.e. Build review, exposure test] | [Include site name where testing will be conducted from. Please indicate whether remote testing can be conducted, i.e. from test suppliers offices] | [Some elements of the testing may be required out of normal office hours (9am-5pm, Mon-Fri), please advise] |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **3.2 Security targets out-of-scope**

No hosts other than those detailed above should be subjected to any form of manual or automated vulnerability assessment.

## **3.3 Principle security concerns**

To support the provisioning of the Penetration Test against [insert Project or Service name] the following Principle Security Concerns (PSCs) have been identified:

|  |  |
| --- | --- |
| **Number** | **Description** |
| PSC 1 | The device/system allows the use of invalid, expired, revoked or signed certificates, or SSL/TLS is not configured in accordance with NHS BSA security standards or best practice, or certificates signed with deprecated hash algorithms (i.e. MD5 and SHA-1). Certificate usage is not known for the device/application (unknown number of certificates in use and unknown certificate attributes, i.e. expiry date, hash algorithms etc. |
| PSC 2 | There are weaknesses resulting from the use of outdated operating systems or through missing patches on devices/systems potentially allowing an attacker to gain a foothold and break out of the *[insert service name]* |
| PSC 3 | There are differences in the builds of the devices/systems within or between the data centre/Cloud environments |
| PSC 4 | Access is allowed to prohibited areas, data, or a combination thereof (i.e. directories, file systems, data stores or records) |
| PSC 5 | The devices/systems, or supporting Cloud infrastructure (VLANs/VRFs) are incorrectly patched or configured, or have vulnerabilities, or a combination thereof, or are running unnecessary services that can be exploited potentially allowing an attacker to gain a foothold and break out of the [insert service name] compartment |
| PSC 6 | The devices/systems are accessible to unauthorised users. This should include but is not limited to, as required, the following profiles:   * NHSBSA user with an application icon * Client * Privileged user |
| PSC 7 | The resident Anti-virus solution is not up to date with regards to engine and/or signatures, is not configured to receive automatic updates, or does not identify or treat malware in accordance with NHS BSA policy (namely clean and delete) |
| PSC 8 | The devices/system allows unauthorised access to management interfaces (or that management interfaces are exposed to non-administrative processes or users) |
| PSC9 | Boundary firewall rules allowing ingress and egress of traffic on an overly permissive basis |
| PSC10 | Deprecated protocols are in use with vulnerabilities that have exploit code available |
| PSC11 | Plain text protocols are in use that can be trivially exploited and secure alternative protocols exist |
| PSC12 | The application is susceptible to compromise or has inherent vulnerabilities introduced through virtualisation. It is suggested that the testing is focussed on but not limited to the following types of common attack (SQL, XML, PHP, Java, XSS and XRSF) |
| PSC13 | That the deployed critical system protection (Host Intrusion Prevention System) local firewall is ineffective and is overly permissive |
| PSC14 | That usernames and passwords are hard coded into scripts or files or are trivial to determine, with emphasis on Service Accounts |
| PSC15 | That a [insert service name] user can bypass application security controls to permit unauthorised viewing of Special Customer Records |
| PSC16 | That the [insert service name] permits unauthorised privilege escalation, enabling access to data or functions not permitted for that user |
| PSC17 | That the [insert service name] interfaces introduce unnecessary weaknesses or routes into the application that can be exploited |

# **4. Test specifics**

A start up meeting should be conducted with the test supplier to identify all requirements are met prior to testing.

NHSBSA request that a Test Plan be produced by the test supplier, the primary objective of this is to define the assurance activities required to establish the current security posture of *[insert project or service name]*.The Test Plan will include an understanding of the target system and what is required to complete the Penetration Test. This should also include how the test supplier intends to test against each of the PSCs identified.

The test supplier must provide details of the hardware, software and any known scripts to be used prior to the commencement of the Penetration Test. The test supplier should include what type of access and how many of each type is required so that access can be granted to the devices for the time period required.

Staff working on this assignment will require the appropriate security clearance prior to deployment on the work package Security Check (SC).

Prior to commencement of testing the tester shall ensure that their systems are clear of any uncontrolled malware. The testers will be required to assert that their systems are patched and up to date.

A review meeting may be required with the test supplier and NHSBSA at the end of the testing to assure that the issues that have been raised are correct.

## **4.1 Daily reporting**

The test supplier shall inform the Technical Advisor at the soonest possible time should a critical vulnerability be discovered.

The test supplier shall take part in a daily wash-up meeting where the day’s findings will be disclosed to NHSBSA. The planned testing for the remainder of the test will also be discussed in these wash-up meetings.

## **4.2 Final report**

The test supplier shall include only those details in the technical report which are necessary to understand the work undertaken, the background issues and any suggested remedial work. Remedial advice and contact information must be provided for the identified weaknesses. The minimum amount of raw data is desirable.

Results must be provided in context where possible, i.e. the relevance of a given vulnerability in the context of the system under test.

The report should indicate how each of the PSCs was tested and if vulnerabilities were identified, the report should reference the PSC number alongside any findings.

For each specific test scenario the test supplier shall:

* Provide a log report written in Plain English, using a conversational narrative style describing each threat simulation, the outcome and the recommendation. The report shall be:
  + An executive summary
  + A ‘Top Ten’ list of any security weaknesses encountered
  + A description of the actions that were performed, including a time stamp of when these were performed and which device they were targeted at
  + For each vulnerability identified the report will advise, a description of the vulnerability, the source systems, the CVSS score, vulnerability score and suggested remediation
  + Formal Service Provider company assessment (score) which will be used to aid NHSBSAs understanding of the vulnerability
  + A prioritised list of findings in tabular form
* Provide the completed report of all works carried out, no later than five working days after the last day of performing the testing. The report will be securely delivered to the NHSBSA.

## **4.3 Assumptions**

This security document is provided with the following assumptions/caveats:

* The test provider will be required to participate in post testing reviews via telekit with other NHSBSA Service Providers in order to contextualise any findings
* The Penetration Testshould test the robustness of security awareness both in the Service Provider and NHSBSA communities
* The Penetration Testwill be undertaken in both the Production and Development environments and is required to be a NCSC ‘Green light’ CHECK level test and should include all standard CHECK testing procedures
* The Penetration Testwill be an exploitation test – however the testers do not actively exploit but should instead indicate where they would have been able to do so. Destructive testing is NOT a requirement nor is it to be undertaken. [this assumption is based upon testing taking place in the production environment, should testing be taking place in a test environment you may want to consider a full exploitation test?]
* NHSBSA will provide full details of the actual testing targets (IP addresses, hostnames, ports etc.) in advance and in good time to the test supplier
* Denial of Service (DoS) attacks will not be attempted during the testing unless explicitly authorised. Should the testing determine that a DoS attack may be successful the report will detail any systems that may be vulnerable to this type of attack, together with relevant countermeasures, where available
* If there is an Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) monitoring the environments the monitoring teams will be made aware of the Penetration Testand the normal IDS/IPS and Incident Response mechanisms will be set to monitor the test rather than taking countermeasures (i.e. blocking) or following the normal escalation procedures
* If it is necessary to cancel or postpone the dates for testing the test supplier may invoke cancellation charges. Charges may vary dependent upon the timescales

# **Appendices**

## **Appendix 1 – NHSBSA** *[insert project or service name]* **Firewall/Security Groups**

List of security groups with associated ports and IP restrictions for the *[insert project or service name]* service

## **Appendix 2 – Application flows/user journey**

## **Appendix 3 – Application screenshots**

## **Appendix 4 – NTA Monitor scoping questionnaire**



## **Appendix 5 – NTA Monitor test plan**

**Appendix 6 – Penetration tester user guide for NHSBSA AWS platform**

****

**Appendix 7 – Log in credentials**

## **Glossary:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ACL | Access Control List |
| AZ | Availability Zone |
| CSRF | Cross-Site Request Forgery |
| DMZ | Demilitarised Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DNS | Domain Name System |
| HTTP | Hypertext Transfer Protocol |
| IAC | Infrastructure As Code |
| IAM | Identity and Access Management |
| ITHC | Information Technology Health Check |
| LDAP | Lightweight Directory Access Protocol |
| NHSBSA | National Health Service Business Services Authority |
| NTP | Network Time Protocol |
| OS | Operating System |
| PHP | Hypertext Preprocessor |
| PSC | Principle Security Concerns |
| RDS | Relational Database Service |
| SC | Security Check |
| SG | Security Group |
| SQL | Structured Query Language |
| URL | Uniform Resource Locater |
| VPC | Virtual Private Cloud |
| XSS | Cross Site Scripting |
|  | [Add any abbreviations used throughout the document to this glossary. Remove any of the above examples in the pre-populated list if not used in the creation of this document] |