

# Threatsys Security Audit & Penetration Testing Scoping Questionnaire

**Type of Assessment Required:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Website/Application Penetration Testing |  | External Infrastructure Penetration Testing |  | Internal Penetration Testing |  |
| Wireless Penetration Testing |  | Configuration/Build Review |  | Firewall Ruleset Review |  |
| Red team |  | Social Engineering scenarios |  | Source Code review |  |
| Voice Over IP Penetration Testing |  | Enterprise Access Penetration Testing |  | Vulnerability Assessment scans |  |

**Project goal(s)** :

* Identify main risks affecting the tested environments
* In order to comply to a standard
* Test if the systems can be exploited
* Other goal(s):

**Timelines**:

* As soon as possible
* In the next month
* In the next 3 months
* In the next 6 months
* Out of hours testing required   
  (i.e. outside 09:00 – 17:00)

**Compliance Reason**:

* PCI DSS
* ISO 27001
* SOC 2 Type 2
* GDPR
* CERT-IN
* STQC

**Impact Level**: Is CERT-in / STQC / Or any other Security Audit required? (Indian only) Yes / No

Please specify your Audit standard:

**Website / Application Penetration Testing:**

|  |  |
| --- | --- |
| What is/are the URL(s) and function (brief explanation) of each application? |  |
| What is/are the Sub Domain(s)? |  |
| Number of Static Pages |  |
| Number of Dynamic Pages |  |
| Is there a login function? |  |
| Would you like to test authenticated parts of your application (for instance, an account management feature)? |  |
| If required for the quotation process would you be willing to provide some low level credentials? |  |
| Are there any areas of functionality that are specifically out of scope? |  |
| Is testing to be performed on site or remotely? |  |
| What is the nature of the environment that we will be testing? | Production/staging/development/live  (delete as appropriate) |
| Are card payments taken and stored on-site or is this controlled by a third party? | Please specify |
| IP Address if testing the associated infrastructure  *Please specify if these addresses are belonging to you own infrastructure of if it is hosted externally* |  |
| Type of application | Web application / Mobile application (please specify on which Operating System) / Web service |

Please note

If the site is hosted by a 3rd Party Supplier, it would be your responsibility to obtain permission before testing begins. At some point Threatsys will need to use some low level login credentials for application and website testing. For confidentiality reasons we will ask for these to be text/emailed to us when required.

If an Intrusion Prevention System (IPS), Web Application Firewall (WAF) or Active Intrusion Detection System is present, exclusion for the IP Addresses associated with testing may be required.

**External Infrastructure Penetration Testing**

|  |  |
| --- | --- |
| Please add all external facing IP address ranges here  Please specify if these ranges are belonging to you own infrastructure of if it is hosted externally |  |
| Please state how many of these external facing IP addresses are LIVE |  |
| Please describe the main functionalities of every server hosted on this perimeter (VPN, web-service, etc.) |  |

**Internal Infrastructure Penetration Testing**

|  |  |
| --- | --- |
| Number of servers (including virtual machines) |  |
| Number of Physical sites |  |
| Are all Physical sites accessible from a single network location? |  |
| Number of desktops (a minimum of 10% is tested unless requested otherwise) |  |
| Are the desktops built from a standard image? |  |

**Wireless Penetration Testing**

|  |  |
| --- | --- |
| Names of Wireless SSID(s) |  |
| Number of locations sites to test |  |
| Type of Wireless Access | Captive portal / private access / enterprise access (802.1x) |
| Will enumeration of rogue access points be necessary? |  |
| Will the team be assessing wireless attacks against clients?  If yes, how many clients will be using wireless access at the time of the assessment? |  |

**Voice over IP Penetration Testing**

|  |  |
| --- | --- |
| What constructor do you use for your Infrastructure? | Avaya/Cisco/Huawei/Alcatel/Others |
| Number of locations sites to test |  |
| Would you like to test your IP phone? |  |
| Would you like to test the security of your server infrastructure (Call manager, SIP proxy, etc.)? |  |

**Enterprise Access Penetration Testing (Tests from a Citrix-like environment)**

|  |  |
| --- | --- |
| Type of access | For instance, Citrix / RDP / VDI |
| Can credentials be provided? If yes, which type of authentication is in use? | Password, OTP, Security tokens, Certificates |
| Is the Enterprise access farm hosted in your infrastructure or externally? |  |

**Firewall Ruleset Review**

The goal of firewall rules review is to verify the efficacy of your filtering policy by ensuring that the firewall configuration and rule set meet business and compliance requirements by verifying that actual configurations and traffic actually flowing through the firewalls matches approved configurations and traffic that is approved to flow through the firewalls.

|  |  |
| --- | --- |
| Firewall Vendor:    E.g.  Check Point:  Cisco:  SonicWALL:  WatchGuard:  Barracuda:  Juniper: |  |
| Number of firewall rule sets to be reviewed  *(For PSN compliance, only the firewall between your corporate network and PSN is required)* |  |
| How many rules are in place for each firewall? |  |
| Will they be reviewed on site or offsite? (If offsite, by what preferred method.) |  |
| Can documents (network diagrams, information about your filtering policy) be provided? If yes, which kind? |  |

**Code Review**

Source code auditing is the most comprehensive service that can be applied to a given application: it can exhaustively detect the vulnerabilities affecting an application by reviewing the source code.

|  |  |
| --- | --- |
| Number of lines of Code |  |
| Code Language |  |
| Third Party / Open Source components |  |
| Would there be a test environment available? |  |
| Would the design documents be available? |  |

**Configuration Review – Build Review**

Performed following a white box approach, the configuration audits make it possible to compare the security level of a given environment with the state of the art, with all the necessary points of view (access to equipment configurations, interviews with teams in charge of the platforms, provision of documentation, etc.).

|  |  |
| --- | --- |
| Type and amount of equipment/build to audit: system (OS, Database, application, others) network (Firewall,  Router/Switch, others)  *Please specify if builds are different or if they share common aspects* |  |
| Are you able to export and send the configuration or do you need a consultant to do the audit on  a live system ? |  |
| Would there be a test environment available? |  |
| Are there specific guidelines you want the consultant to use? |  |
| Would design documents / specifications be available? |  |

**Social Engineering**

|  |  |
| --- | --- |
| Would you want to test social engineering scenarios through phishing simulation?  If yes, please specify if users can be phished using fake website or through sending malicious files? |  |
| Would you want to test your employee awareness through physical intrusion simulation?  If yes, how many physical sites? |  |
| Would you want to test your employee awareness through phone calls simulation? |  |
| Number of people to target  *It is advised not to target more than 100 persons for each campaign* |  |

**Red Team**

Red team engagements use real attacking tactics applied to your infrastructure.

It is a life-size exercise that aims to find a way to infiltrate your internal network in order to extract real data, all this avoiding detection.

The purpose of this service is to reveal how effective your organisation's defences are against a real attack but also to test security at several levels of your organisation. The tests will be carried out remotely, but can also need to be done from your premises.

|  |  |
| --- | --- |
| Size (number of people) and type of the organisation you wish to be assessed |  |
| Method you wish to be used (multiple can be selected) | Email campaign containing malicious  attachment(phishing), External attack surface, Physical intrusion, Wi-Fi |

**VA Scans (Vulnerability Assessment)**

|  |  |
| --- | --- |
| How many IP addresses do you need to scan?  *Please state if all machines are hosted externally* |  |
| How many web applications do you need to scan?  *Please state if all applications are hosted externally* |  |

|  |
| --- |
| **Other Requirements:** |
| **Additional Notes:** |