Penetration Testing Scoping Checklist

The intent of this form is to gather initial information about your technology infrastructure and testing intent so that we may properly plan a penetration test / security exercise. Our services will safely evaluate the security of your resources against attacks from a malicious source.

All information provided in this form is strictly confidential. Send completed forms to Chris Wireman at chris@geteventlog.com.

Network Penetration Testing

1. Why is the customer having the penetration test performed against their environment?

2. Is the penetration test required for a specific compliance requirement?

3. When does the customer want the active portions (scanning, enumeration, exploitation, etc...) of the penetration test conducted?

- During business hours?

- After business hours?

- On the weekends?

4. How many total IP addresses are being tested?

- How many internal IP addresses, if applicable?

- How many external IP addresses, if applicable?

5. Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

6. In the case that a system is penetrated, how should the testing team proceed?

- Perform a local vulnerability assessment on the compromised machine?

- Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?

- Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc/shadow on Unix machines)?

Web Application Penetration Testing

1. How many web applications are being assessed?
2. How many login systems are being assessed?
3. How many static pages are being assessed? (approximate)
4. How many dynamic pages are being assessed? (approximate)
5. Will the source code be made readily available?
6. Will there be any kind of documentation?

- If yes, what kind of documentation?

7. Will static analysis be performed on this application?
8. Does the client want fuzzing performed against this application?
9. Does the client want role-based testing performed against this application?
10. Does the client want credentialed scans of web applications performed?

Wireless Network Penetration Testing

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so:

- Does the guest network require authentication?
- What type of encryption is used on wireless networks?
- What is the square footage of coverage?
- Will enumeration of rogue devices be necessary?
- Will the team be assessing wireless attacks against clients?
- Approximately how many clients will be using the wireless network?

Physical Penetration Testing

1. How many locations are being assessed?

2. Is this physical location a shared facility? If so:

- How many floors are in scope?
- Which floors are in scope?

3. Are there any security guards that will need to be bypassed? If so:

- Are the security guards employed through a 3rd party?
- Are they armed?
- Are they allowed to use force?

4. How many entrances are there into the building?
5. Is the use of lock picks or bump keys allowed?
6. Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?
7. What is the square footage of the area in scope?
8. Are all physical security measures documented?
9. Are video cameras being used?

- Are the cameras client-owned? If so:
- Should the team attempt to gain access to where the video camera data is stored?

10. Is there an armed alarm system being used? If so:

- Is the alarm a silent alarm?
- Is the alarm triggered by motion?
- Is the alarm triggered by the opening of doors and windows?

Social Engineering

1. Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?
2. Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?

3. Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so:

- How many people will be targeted?

Questions for Business Unit Managers (may or may not be needed)

1. Is the manager aware that a test is about to be performed?
2. What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?
3. Are testing and validation procedures to verify that business applications are functioning properly in place?
4. Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?
5. Are Disaster Recovery Procedures in place for the application data?

Questions for System Administrators and or Help Desk Personnel (may or may not be needed)

1. Are there any systems which could be characterized as fragile? (Systems with tendencies to crash, older operating systems, or which are unpatched)
2. Are there systems on the network which the client does not own, that may require additional approval to test?
3. Are Change Management procedures in place?
4. What is the mean time to repair systems outages?
5. Is any system monitoring software in place?
6. What are the most critical servers and applications?
7. Are backups tested on a regular basis?
8. When was the last time the backups were restored?