

NOT PROTECTIVELY MARKED



CHECK SERVICE ASSAULT COURSE

Notes for Candidates

Issue 2.1

October 2006

© Crown Copyright 2006 – All Rights Reserved

Page 1 of 18

NOT PROTECTIVELY MARKED



INVESTOR IN PEOPLE

NOT PROTECTIVELY MARKED

This page is intentionally blank

NOT PROTECTIVELY MARKED



Table of Contents

Table of Contents 3
Revision History..... 4
Introduction 5
Access to information..... 5
Confidentiality..... 5
Scope, Schedule, Methodology and Equipment..... 6
 Scope 6
 Schedule 6
 Phase 1..... 6
 Phase 2..... 6
 Phase 3..... 7
 Assault Course Wash-up 7
 Methodology 7
 Equipment 7
Assault Course Components 8
 Introduction 8
 Worked Example..... 8
 Proposal Definition and Scoping..... 11
 Legal and Contractual Issues..... 11
 Preparation and Vulnerability Knowledge..... 11
 Recommendations 11
 Network Configuration and Security 12
 Windows Security 14
 UNIX Security..... 16
Assault Course Decisions..... 17
 Pass..... 17
 Fail..... 17
 Reschedule 17



NOT PROTECTIVELY MARKED

Revision History

November	1999	CESG/DERA Notes For Candidates written by Simon Halsall
September	2001	CESG V1.0 Notes for Candidates written by Greg Masters
October	2002	CESG V1.1 updated by Dominic Beecher
January	2004	CESG V1.2 updated by Dominic Beecher
July	2005	CESG V2.0 updated by Greg Masters and Steven Bates
October	2006	CESG V2.1 updated by Greg Masters and Mark Lodge

This document may not be reproduced or copied in any form without the express permission of the specified CESG officers. The specified CESG officers are Greg Masters (gregory.masters@cesg.gsi.gov.uk) and Mark Lodge (mark.lodge@cesg.gsi.gov.uk)



NOT PROTECTIVELY MARKED

Introduction

1. The CHECK Service Assault Course is designed to assess IT security consultants against a baseline of practical penetration testing skills. The aim of the Assault Course is to ensure the candidate can perform a complete and thorough technical IT Health Check within the criteria described in this document. The majority of this document is dedicated to describing the breadth and depth of knowledge required to complete the CHECK Service Assault Course successfully and attain Team Leader status. To indicate the depth of knowledge required, this document will use two terms:

- **Understand:** candidates must know about the existence, technical details and security implications of a subject, but are not required to demonstrate the knowledge practically.
- **Demonstrate:** candidates must know about the existence, technical details and security implications of a subject, and will be required to demonstrate this knowledge practically.

2. All candidates should be experienced penetration testing consultants.

Access to information

3. The Assault Course is an open book assessment; candidates may use any reference materials they feel are appropriate.

Confidentiality

4. Candidates must not disclose the content or structure of the CHECK Service Assault Course network (see section 11 of the “Terms and Conditions of Membership of the IT Health Check Service”). Furthermore, candidates are reminded that these notes may not be reproduced without the permission of CESG, as is detailed in the above document.

5. It should be noted that prior knowledge of the Assault Course network will be of little use to the candidate, as it is constantly updated and revised. Candidates will be required to demonstrate a thorough understanding of the theory behind the tools and techniques they use, and explain in detail to the assessors their analysis of the results obtained and any conclusions drawn. Without this knowledge, a candidate will not pass the Assault Course.

NOT PROTECTIVELY MARKED

Scope, Schedule, Methodology and Equipment

Scope

6. The current scope of the CHECK Service Assault Course is restricted to popular UNIX-like and Windows operating systems, web applications and common network components, including routers, switches and firewalls. The network protocols assessed are restricted to the IP, supported by switched or shared Ethernet. Networks are divided into routed subnets.

Schedule

7. The Assault Course is divided into three phases, which mirror the stages of a 'typical' IT Health Check, including a remote and an on-site test. The candidate will be required to work through each phase. The format of the Assault Course will include two written examinations, each followed by a viva that will allow candidates to follow their own methodology.

8. Phases 1 and 2 should take no more than 1.5 hours. When these phases have been completed, the assessors will examine the candidate's results and understanding of the tools and techniques used. Only after the successful completion of phases 1 and 2, will candidates move onto phase 3. This final phase should take no more than 2 hours to complete and will include a viva in each phase. The viva will examine the methods used to retrieve the results, and will call for practical demonstrations of the techniques used.

9. The timings of the Assault Course will vary from candidate to candidate and will depend on the methodology and techniques used. While the assessors are flexible with regard to the timing of each individual phase, 4 hours is the maximum time allocated to the Assault Course.

Phase 1

10. Candidates will provide information on the preparatory work that would constitute a normal penetration test. This is to include:

- Scoping, proposal production and customer liaison;
- Legal and contractual issues;
- Information gathering.

11. Candidates will be required to understand the necessary protection mechanisms, both physical and electronic, for processing and storing protectively marked material.

Phase 2

12. Candidates will be provided with a network connection point and an IP address. The candidate will also be given the domain name of the network to be tested. Using a sound working knowledge of IP protocols, DNS and network routing (detailed requirements are stated below), the candidate will be expected to map the network and identify key target systems within the network address range. The deliverable produced by the candidate must take the form of an annotated and logical connectivity diagram of the target network. At the

NOT PROTECTIVELY MARKED

end of this phase, the candidate should be prepared to explain in detail how the network was discovered and the mechanics of any tools used.

Phase 3

13. Candidates will be provided with a network connection point and an IP address on the internal target network. The candidate will be expected to assess the security of UNIX and Windows hosts and any other network components, and advise on possible countermeasures. The candidate will require a sound working knowledge of IP protocols, and UNIX and Windows vulnerabilities, to perform this task (detailed requirements are described below).

Assault Course Wash-up

14. The assessors will inform the candidate of the result, and conduct a short feedback session to discuss any issues identified during the Assault Course. CESG will issue a letter confirming the result, and a certificate to successful candidates. All candidates will be provided with a feedback form, which should be completed and returned to CESG.

Methodology

15. The candidate will be required to demonstrate that the assessed penetration test has been conducted in a methodical and structured manner. However, the candidate is free to follow any test methodology. The assessors may, if necessary, direct the candidate towards certain portions of the network in the interests of time, and the candidate should make it known if this deviates from their standard procedure.

Equipment

16. The candidate is required to bring any computer equipment and software necessary to conduct a penetration test against a 10/100Base-T Ethernet network.

17. During the assessment, the candidate's computer equipment will be connected to an external monitor supplied by CESG. This will allow the assessors to view the work performed by the candidate. The candidate must therefore ensure that all their computer equipment functions correctly when connected to an external monitor. When using a laptop computer, the display must be output to the laptop screen and the external monitor. Failure to do so may result in failure.

18. The operating systems and tools used must be capable of conducting network and host discovery and demonstrating or identifying vulnerabilities against criteria detailed later in this document. Candidates may use any software tools they deem appropriate. However, they must ensure any tools used are appropriately licensed and function correctly. Ideally, a complete tool-set will contain complementary and alternative vulnerability discovery and/or system administration tools. Failure to demonstrate penetration test capabilities due to hardware or software misconfiguration may result in failure.

NOT PROTECTIVELY MARKED

Assault Course Components

Introduction

19. The following components make-up the core knowledge-base a candidate requires in order to successfully complete the CHECK Service Assault Course. These components only detail the core requirements for a CHECK Service Team Leader and have been designed to address common vulnerabilities and network configurations. Not all components will necessarily be covered fully during the Assault Course. However, candidates should satisfy themselves that they can meet the requirements for all components.

20. Candidates will be required to identify vulnerabilities in the Assault Course network. Exploitation of vulnerabilities is not a requirement *per se*, but candidates should use all techniques at their disposal to obtain the highest level of assurance regarding the presence or absence of vulnerabilities in the target systems. Candidates are expected to provide a value-added service above that of an automated vulnerability scanner and should be able to eliminate false positives and negatives where possible. Techniques to accomplish this may include, but are not limited to, vulnerability exploitation.

Worked Example

21. The Assault Course focuses on vulnerabilities that the CESG Health Check team regularly identify when performing penetration tests. For any subject area that this document uses the word “demonstrate”, the candidate will be required to:

- Explain any vulnerabilities associated with the technology;
- Explain the limitations and default behaviour of the vulnerabilities;
- Demonstrate the remote detection of the vulnerabilities (the candidate will be required to eliminate possible false positives from scanning tools by, for example, manually demonstrating the exploitation of a vulnerability) and describe how the detection mechanism works.
- Explain protection measures that could be implemented to secure the computer system against the identified vulnerabilities.

22. The CESG Health Check team infrequently assess NIS domains and therefore vulnerabilities in NIS are not examined. However, to provide an indication of the knowledge level required in the CHECK Assault Course, a worked example for NIS has been included below.

23. This document would include the following statement:

- Candidates are required to demonstrate vulnerabilities associated with the use of NIS in a UNIX environment.

NOT PROTECTIVELY MARKED

During the Assault Course the following questions might be asked:

Can you identify a NIS server on the network?

An acceptable response would be:

The following machine has been identified as an NIS server because it is running the following RPC services:

- ypserv;
- ypbind;
- yppasswdd;
- ypxfrd.

Explain the vulnerabilities commonly associated with NIS.

An acceptable response would be:

It is possible to fake an RPC NIS server reply sent from the server to the client, following a request for user account information. This fake reply will be accepted by the client and accepted as a valid passwd file map.

And/or:

If rpc.bootparamd is available on the server, it may be possible to query the NIS server for a domain name. This name could then be used to request maps, including the passwd map.

Please demonstrate whether the system is a vulnerable NIS server and explain how the test works.

An acceptable answer would be:

I am sending a request to the rpc.bootparamd RPC service to obtain the NIS domain name. The service has told me that the domain name is "foo".

I am now requesting a maplist from the server. The server has not provided the maplist, so I will try to request the passwd.byname map. The server has now provided me with the password map, which contains a number of hashed passwords.

Now you are logged into the server, please demonstrate how can you view the password map on the host.

An acceptable answer would be:

I used ypcat to view the passwd.byname map.

NOT PROTECTIVELY MARKED

Now you have a password file, how can the passwords for the user be determined and what level of access might the users have to the system?

An acceptable answer would be:

I would crack the password file using the “bar” cracking tool.

And/or:

I would only expect to find non-root users in the passwd map. If a root user was present, I would investigate the matter further.

How would you advise your client to secure this server?

An acceptable answer would be:

I would advise my customer to investigate the use of NIS+. NIS+ uses Secure RPC authentication, which is based on the Diffie-Hellman key exchange protocol and DES. The use of NIS+ and Secure RPC will have an operational impact, as it will require cryptographic processing and the management of keys.

NOT PROTECTIVELY MARKED

Proposal Definition and Scoping

24. The candidate will be required to understand how a particular penetration test would be scoped. This may include:

- Requesting network diagrams;
- Identification of target systems;
- Customer care, e.g. requesting that backups are made before testing begins;
- Advice on IDS and logging processes.

Legal and Contractual Issues

25. The candidate will be required to understand the legal and contractual requirements pertaining to a penetration test, particularly those relating to the unlawful use of computer systems, the protection of customer and personal data, and privacy. The assessors do not expect a detailed knowledge of the pertinent articles of law, but a layman's grasp of their impact on penetration testing will be required.

Preparation and Vulnerability Knowledge

26. The candidate will be required to understand how vulnerability information for a target is acquired.

27. The candidate will be required to understand current significant open-source vulnerabilities. An indication of a significant vulnerability would be a vulnerability in a firewall or a default service on a mainstream operating system.

Recommendations

28. At the end of each practical stage (phases 2 and 3), the candidate will be required to make suitable recommendations for mitigating any security vulnerabilities discovered.

NOT PROTECTIVELY MARKED

Network Configuration and Security

29. The candidate will be required to understand protective network architectures; this will include:

- Firewalls;
- DMZ Configurations;
- Proxy servers.

30. The candidate will be required to demonstrate network data capture and analysis from a shared network media.

31. The candidate will be required to understand network ARP spoofing, data capture and analysis from a switched network media.

32. The candidate will be required to demonstrate information retrieval from DNS servers, for both single and multiple DNS record sets.

33. The candidate will be required to demonstrate an understanding of DNS record structure pertaining to the identification of target systems.

34. The candidate will be required to understand the principles of, and differences between, TCP, UDP and ICMP. They will also be required to understand the security implications associated with their use.

35. The candidate will be required to understand the vulnerabilities in using clear-text protocols, such as TELNET.

36. The candidate will be required to understand how routing protocols, such as RIP and OSPF, can affect network security.

37. The candidate will be required to demonstrate the use of ICMP to aid mapping a network. An example of a network mapping tool is *traceroute*.

38. The candidate will be required to demonstrate information retrieval from SNMP servers.

39. The candidate will be required to understand the SNMP MIB structure pertaining to the identification of target systems and network routes.

40. The candidate will be required to demonstrate the detection of TCP and UDP services available from servers and network components.

NOT PROTECTIVELY MARKED

41. The candidate will be required to demonstrate common weaknesses in routers and switches. These may involve:

- TELNET access;
- HTTP access;
- SNMP access;
- TFTP access.

42. The candidate will be required to demonstrate the construction of a network map from the gathered information sources.

NOT PROTECTIVELY MARKED

Windows Security

43. The candidate will be required to demonstrate enumeration techniques using the default NetBIOS service. Candidates should be able to enumerate:

- Users;
- Groups;
- Shares;
- Password policies;
- Domains;
- Domain Controllers.

44. The candidate will be required to demonstrate enumeration of user names through RID cycling.

45. The candidate will be required to demonstrate a technique to test user names and passwords remotely.

46. The candidate will be provided with any authentication required and will then be required to demonstrate:

- Vulnerabilities associated with using terminal services. This may include local privilege escalation and bypassing local security policies;
- Remotely mapping network drives;
- Remotely opening the registry.

47. The candidate will be required to demonstrate the detection of known security weakness within common Windows web servers.

48. The candidate will be required to demonstrate the detection of default installations of the Microsoft SQL server.

49. Candidates will be required to detect vulnerabilities associated with databases and bespoke web front-ends. This will include SQL injection and cross-site scripting.

50. The candidate will be required to demonstrate information retrieval from Windows SNMP servers.

51. The candidate will be required to understand the Windows SNMP MIB structure pertaining to the identification of security weakness.

52. The candidate will be required to understand the security impact of Windows trust relationships.

NOT PROTECTIVELY MARKED

53. The candidate will be required to demonstrate security vulnerabilities in incorrectly configured FTP servers.

54. Individual vulnerabilities in databases and applications are not addressed. However the candidate should understand the approach they should adopt if present and discovered during testing.

NOT PROTECTIVELY MARKED

UNIX Security

55. The candidate will be required to demonstrate common user enumeration techniques. These techniques should include:

- User enumeration through SMTP;
- User enumeration through the finger service;
- User enumeration through rusers or rwho.

56. The candidate will be required to demonstrate the enumeration of Remote Procedure Call services.

57. The candidate will be required to demonstrate vulnerabilities associated with the RPC services.

58. The candidate will be required to demonstrate the enumeration of NFS exported directories.

59. The candidate will be required to demonstrate the mounting of insecure NFS exported directories.

60. The candidate will be required to demonstrate the remote manipulation of UIDs and GIDs, to gain access to files on NFS exported directories.

61. The candidate will be required to demonstrate the detection of insecure X servers.

62. The candidate will be required to demonstrate security vulnerabilities due to incorrectly configured anonymous FTP servers.

63. The candidate will be required to demonstrate security vulnerabilities in incorrectly configured anonymous TFTP servers.

64. The candidate will be required to demonstrate the detection of known security weaknesses within common UNIX web servers.

65. The candidate will be required to demonstrate banner-grabbing techniques.

66. The candidate will be required to demonstrate exploitation of Berkeley R-services (rexec, rlogin, rsh) trust relationships.

67. The candidate will be required to demonstrate the exploitation of SAMBA shares.

68. The candidate will be required to demonstrate information retrieval from UNIX SNMP servers.

69. The candidate will be required to understand the UNIX SNMP MIB structure pertaining to the identification of security weakness.

70. Individual vulnerabilities in databases, applications, SSH and DNS are not addressed. However, the candidate should understand the approach they should adopt if present.

NOT PROTECTIVELY MARKED

Assault Course Decisions

71. There are three Assault Course decisions: pass, fail and reschedule.

Pass

72. The candidate has successfully completed the core components assessed and is competent to fulfil the role of a CHECK Team Leader. The Pass is valid for 3 years and it is the CHECK Service Provider's responsibility to ensure that it is renewed if required within the said period.

Fail

73. The candidate has not successfully completed the core components and is required to improve the areas of weakness identified in the feedback information before rescheduling another Assault Course at commercial rates.

Reschedule

74. The candidate has been unable to complete all of the core components due to circumstances beyond the control of the candidate or assessors. Under these conditions, the Assault Course will be rescheduled at the discretion of the assessor.

75. If a candidate fails to complete the Assault Course because of computer equipment misconfiguration or malfunction, a fail decision will be issued and NOT a reschedule.

NOT PROTECTIVELY MARKED

This page is intentionally blank

NOT PROTECTIVELY MARKED

