GIAC NT

PRACTICAL ASSIGNMENT FOR SANS SECURITY MONTEREY 2000

Prepared By

Jeff Payne

TABLE OF CONTENTS

Introduction ---------- 1

Disclaimer---------- 1

Securing Windows NT---------- 1

Section 1 – Convert Fat Partitions to NTFS Partitions---------- 1
Section 1a – Set ACLS on Operating System Files---------- 2
Section 1b – File System Configuration---------- 2

Section 2 – Registry---------- 2
Section 2a – User Logon Information Display---------- 3
Section 2b – Logon Banner---------- 4
Section 2c – Auto Admin Logon---------- 4
Section 2d – Disable Anonymous Users---------- 5
Section 2e – Encrypt SAM Database---------- 6
Section 2f – Remote Registry Access---------- 6
Section 2g – Secure Event Log Viewing---------- 7
Section 2h – Backups---------- 8
Section 2i – Cached Logons---------- 8

Section 3 – Best Practices for NT Passwords ---------- 9
Section 3a – Use of Passfilt.dll---------- 10
Section 3b – Disable Guest Account---------- 11
Section 3c – Rename Administrator Account ---------- 12
Section 3d – Install latest Service Pack---------- 12
Section 3e – Recovery Disk---------- 13

Section 4 – Disabling Non-Essential Services---------- 13
Section 4a – Messenger Service---------- 13

Section 5 – User Manager Audit Policy---------- 14

Section 6 – File Auditing/Vulnerability Software (SPI)---------- 17
Section 6a – Installing SPI for Windows NT ---------- 17
Section 6b – Tools & Configuration Parameters---------- 22

Conclusion---------- 26

References---------- 27

Introduction

This document was written to fulfill requirements for the practical assignment portion of the GIAC-NT certification. It represents only a portion of items to be addressed in terms of threats and vulnerabilities of a computing environment that utilizes Microsoft's Windows NT. This document should be used as a security baseline and is meant to serve only as a sample guide not a complete list of all best practices that should be followed in attempting to secure a Windows NT environment

Securing Windows NT

There are multiple steps in the sections to follow that cover some best practices for securing computers running Windows NT 4.0 Workstation or Server. These are a subset of the best practices identified in Securing Windows NT: Step By Step, published by the System Administration, Networking and Security (SANS) Institute. Implementing these best practices alone will not guarantee the security of a computing environment but will be useful as a basis of security practices.

Section 1 - Convert FAT Partitions to NTFS Partitions

[1] NSWC NT Risk Assessment helpfile