



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

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

© SANS Institute 2000 - 2005 for retention rights.

© SANS Institute 2000 - 2005, Author retains full rights.

¹ NSWC NT Risk Assessment helpfile

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	vLive
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
Univ. of California - SEC505: Securing Windows and PowerShell Automation	Los Angeles, CA	Jan 29, 2018 - Feb 03, 2018	vLive
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	vLive
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced