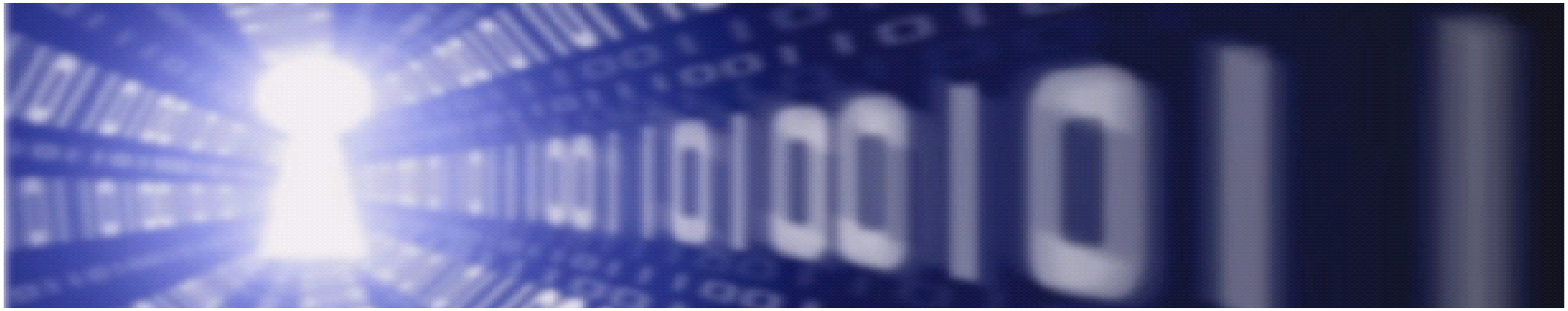
I'm Going to Shoot the Next Person who says VLANS

Presenter: Himanshu Dwivedi

August 3rd, 2006

BlackHat Briefings 2006

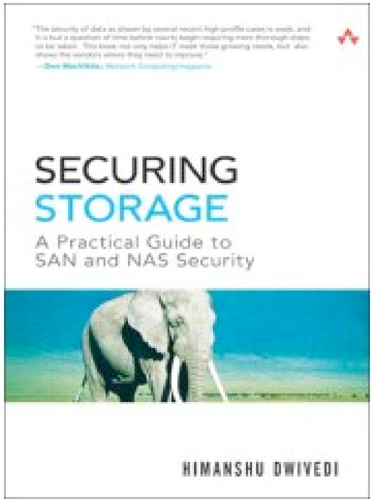


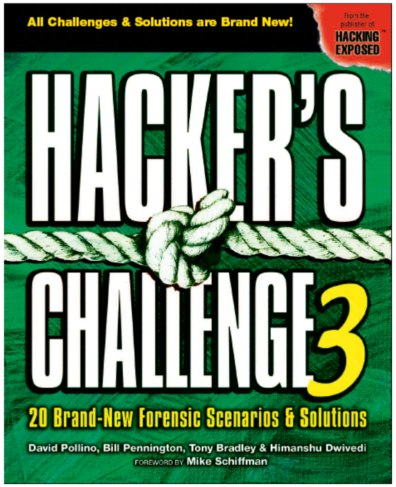
iSEC Partners

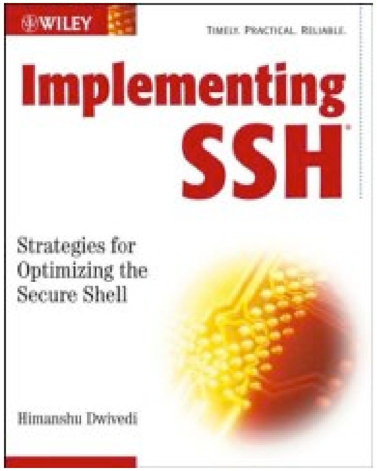
https://www.isecpartners.com

Presenter BIO

- **Books**
  - Securing Storage
  - Hacker's Challenge 3
  - Implementing SSH
- **Tools**
  - SecureNetApp (New!)
  - SNAP (New!)
  - NetApp.iSCSI.checker
  - CHAP Password Tester
  - StorScan
  - SecureCookies
  - CiscoIPv6check
  - SecureCisco
  - SecureBigIP
  - SecureWin2003
  - SecureWinXP




All Challenges & Solutions are Brand New!
From the publisher of HACKING EXPOSED
HACKER'S CHALLENGE 3
20 Brand-New Forensic Scenarios & Solutions
David Pollino, Bill Pennington, Tony Bradley & Himanshu Dwivedi
FOREWORD BY Mike Schiffman


WILEY
TIMELY. PRACTICAL. RELIABLE.
Implementing SSH
Strategies for Optimizing the Secure Shell
Himanshu Dwivedi

Agenda

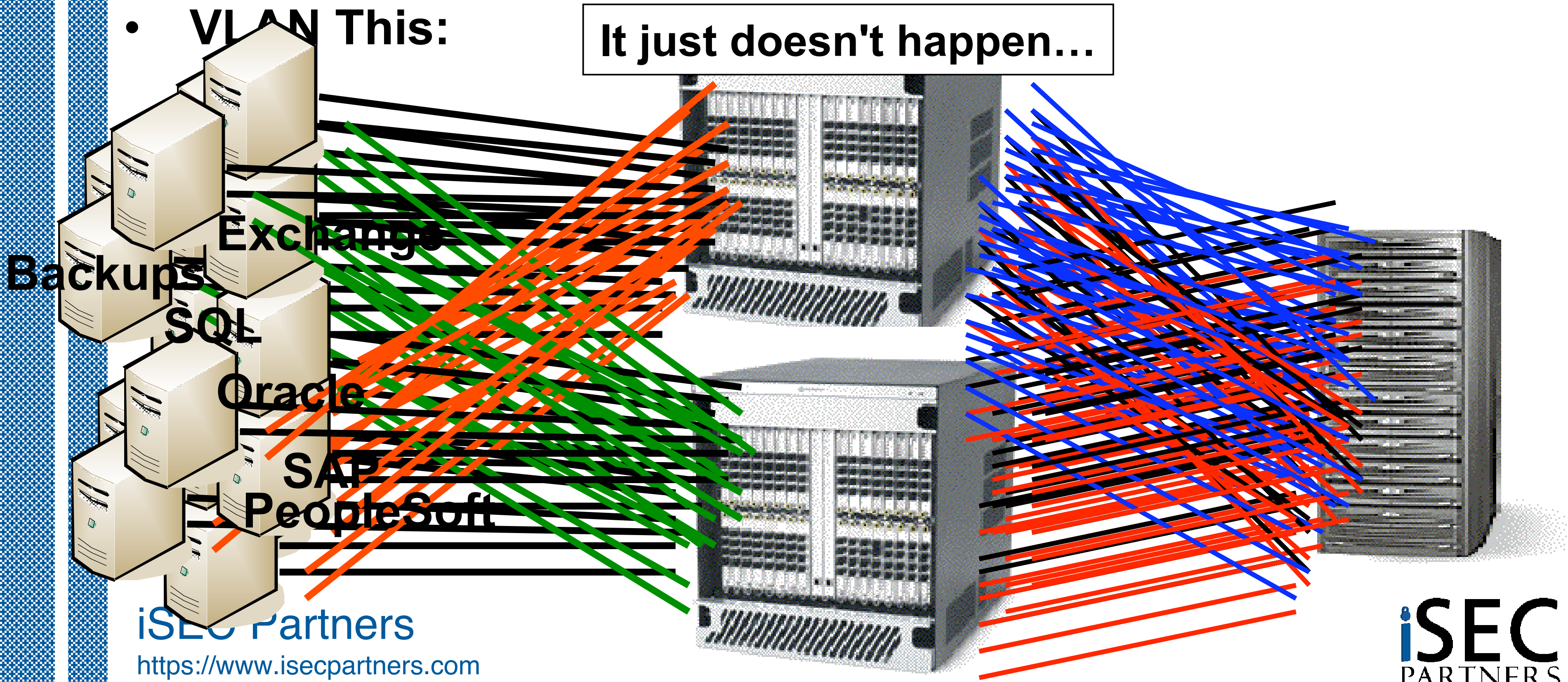
- The VLAN Myth
- Storage Network Audit Program
  - SNAP
- SecureNetApp
  - NetApp Security Configuration Analyzer
- I learned it from watching you!!
  - Home Storage Devices

VLAN Myth

- **Definition of the “VLAN” Answer**
  - “VLANs”
  - “Firewalls”
  - “You need to authenticate to the network”
  - *“[Existing items used for security]* were not intended as intrinsic security measures”
  - “File systems provide security for files - no network security mechanism SHOULD”
  - “*[No current encryption method]* is a problem?”

VLAN Myth

- **Fact: VLANs are great**
  - I love them, I like like, I want to marry them
  - 4 and of 5 dentists recommend VLANs
- **VLAN This:**



VLAN Myth

- **VLANs are to storage…**

  ..as application firewalls are to e-Commerce
- **What If?**
  - Microsoft took the “VLAN” approach and said the Vista security model is simply asking the customer to use a network firewall and hope for the best
- **Does it make sense?**
  - Should an entity with terabytes of storage, including sensitive information, be unable to protect itself?
  - Do banks keep their vaults unlocked at night since they have security guards and cameras?

SNAP

(Storage Network Audit Program)

SNAP

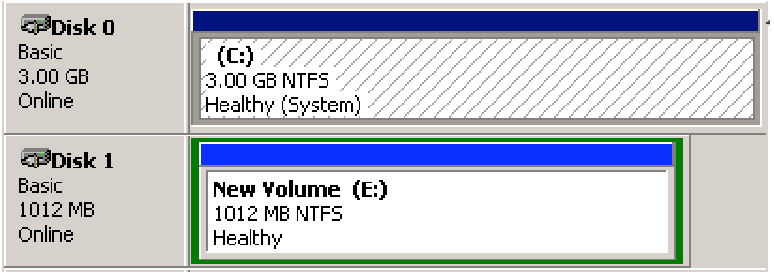
- **Storage Network Audit Program**
  - Goal: Provide a resource to audit the security of storage networks
  - Scope:
    - Fibre Channel SANs
    - Network Attached Storage (NAS)
    - iSCSI SANs
  - Presented in Chapter 13 of Securing Storage book
    - Updated June 2006

SNAP - tastic

SNAP: Storage Network		
Audit Topic	**Audit Questions**	**Audit Compliance**
SAN: HBA-WWNs WWNs should be difficult to spoof or enumerate	Which type of WWN are used, port WWN, node WWNs, or WWNs that use both port and node WWNs?	**Meets Expectations:** Port WWNs are used Port and Node WWNs are used.. **Does not meet Expectations:** Node WWNs are used for authorization.
iSCSI: Authentication iSCSI Initiator should be required to authenticate for all iSCSI communication	Is CHAP Authentication and/or Mutual Auth enabled?	**Meets Expectations:** CHAP is enabled (Mutual Authentication is also enabled) **Does not meet Expectations** CHAP is disabled.

SAN - Spoofing

- WWN Spoofing Attack



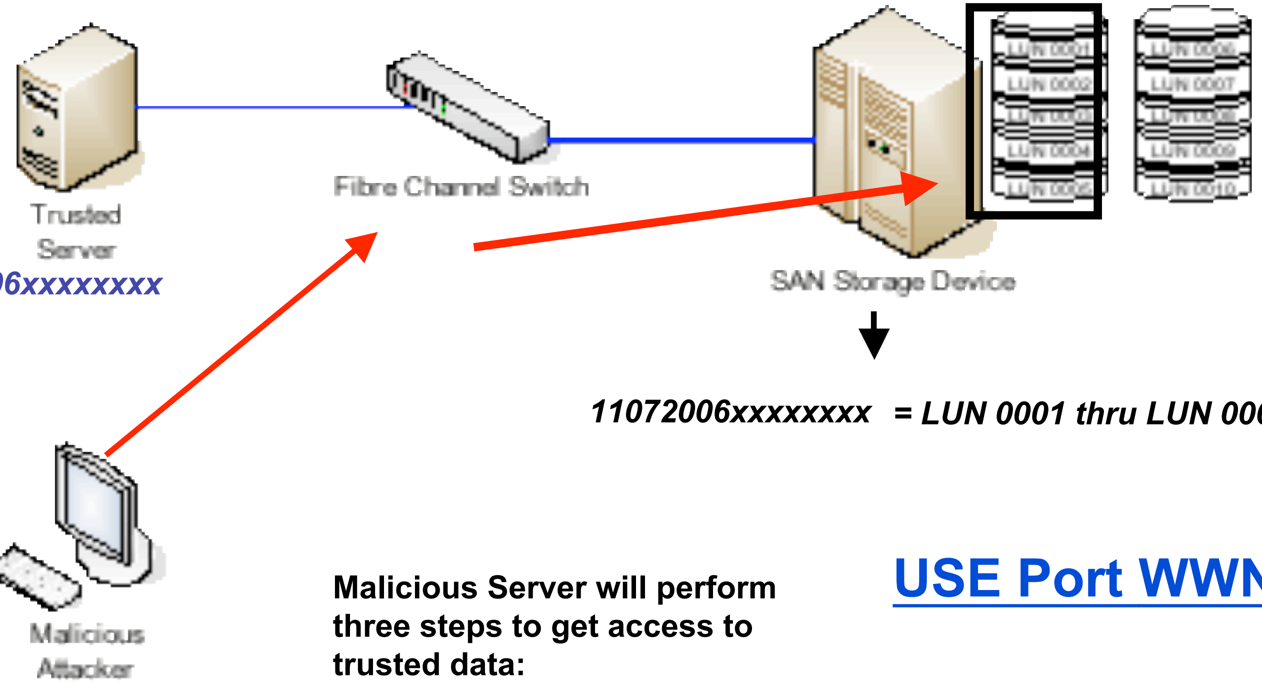
Disk 0
Basic
3.00 GB
Online

(C:)
3.00 GB NTFS
Healthy (System)

Disk 1
Basic
1012 MB
Online

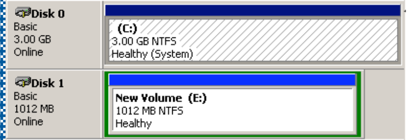
New Volume (E:)
1012 MB NTFS
Healthy

Trusted Server has access to LUN 0001, 0002, 0003, 0004, and 0005



nWWN: 11072006xxxxxxxx

11072006xxxxxxxx = LUN 0001 thru LUN 0005



Disk 0
Basic
3.00 GB
Online

(C:)
3.00 GB NTFS
Healthy (System)

Disk 1
Basic
1012 MB
Online

New Volume (E:)
1012 MB NTFS
Healthy

nWWN: 11072006xxxxxxxx

Malicious Server will perform three steps to get access to trusted data:

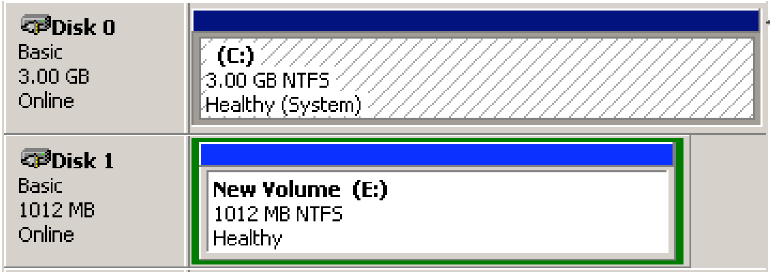
1. Query the switch for WWNs

2. Change their WWN

3. See Data

USE Port WWNs!

iSCSI w/o Auth



Disk 0
Basic
3.00 GB
Online

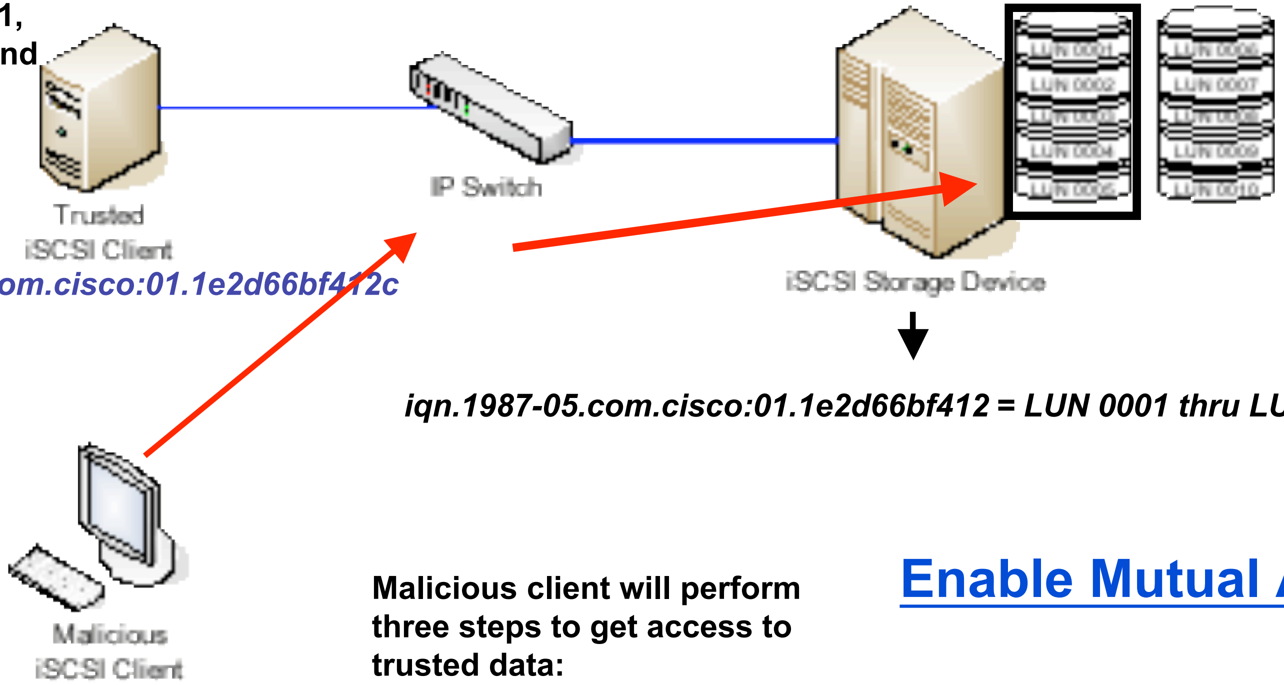
(C:)
3.00 GB NTFS
Healthy (System)

Disk 1
Basic
1012 MB
Online

New Volume (E:)
1012 MB NTFS
Healthy

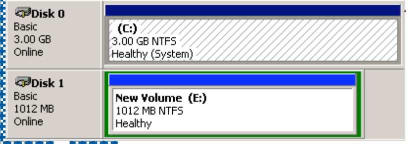
- <u>iSCSI Attack Demo</u>

Trusted Client has access to LUN 0001, 0002, 0003, 0004, and 0005



iqn.1987-05.com.cisco:01.1e2d66bf412c

iqn.1987-05.com.cisco:01.1e2d66bf412 = LUN 0001 thru LUN 0005



Disk 0
Basic
3.00 GB
Online

(C:)
3.00 GB NTFS
Healthy (System)

Disk 1
Basic
1012 MB
Online

New Volume (E:)
1012 MB NTFS
Healthy

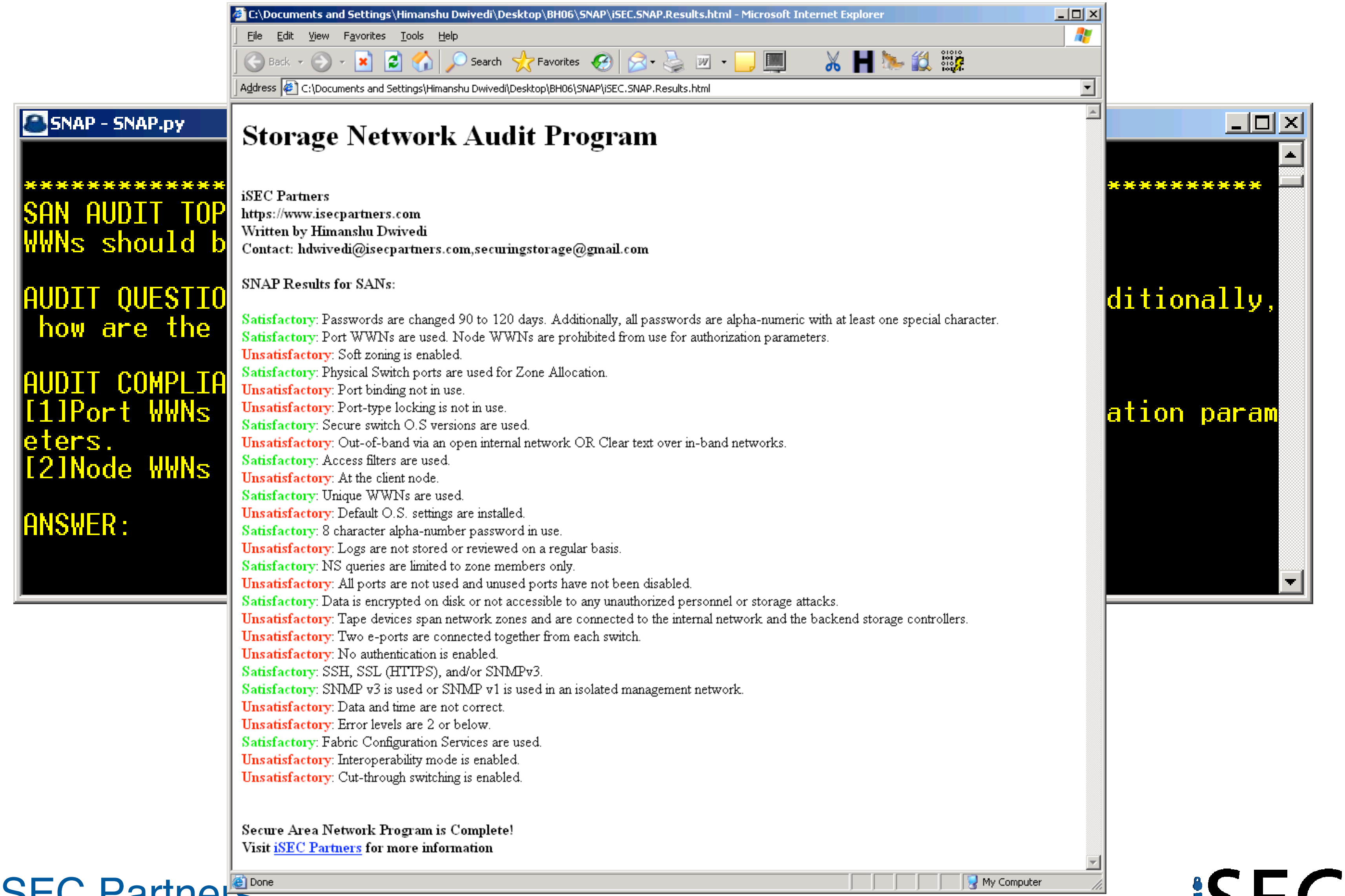
iqn.1987-05.com.cisco:01.1e2d66bf412c

Malicious client will perform three steps to get access to trusted data:

1. Sniff
2. Spoof
3. See Data

<u>Enable Mutual Auth!</u>

SNAP – a - lious


SNAP - SNAP.py
C:\Documents and Settings\Himanshu Dwivedi\Desktop\BH06\SNAP\iSEC.SNAP.Results.html - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
C:\Documents and Settings\Himanshu Dwivedi\Desktop\BH06\SNAP\iSEC.SNAP.Results.html
Done
My Computer

```
**************                                   ***********
SAN AUDIT TOP
WWNs should b

AUDIT QUESTIO                                    ditionally,
 how are the

AUDIT COMPLIA
[1]Port WWNs                                     ation param
eters.
[2]Node WWNs

ANSWER:
```

Storage Network Audit Program

iSEC Partners
https://www.isecpartners.com
Written by Himanshu Dwivedi
Contact: hdwivedi@isecpartners.com,securingstorage@gmail.com

SNAP Results for SANs:

Satisfactory: Passwords are changed 90 to 120 days. Additionally, all passwords are alpha-numeric with at least one special character.
Satisfactory: Port WWNs are used. Node WWNs are prohibited from use for authorization parameters.
Unsatisfactory: Soft zoning is enabled.
Satisfactory: Physical Switch ports are used for Zone Allocation.
Unsatisfactory: Port binding not in use.
Unsatisfactory: Port-type locking is not in use.
Satisfactory: Secure switch O.S versions are used.
Unsatisfactory: Out-of-band via an open internal network OR Clear text over in-band networks.
Satisfactory: Access filters are used.
Unsatisfactory: At the client node.
Satisfactory: Unique WWNs are used.
Unsatisfactory: Default O.S. settings are installed.
Satisfactory: 8 character alpha-number password in use.
Unsatisfactory: Logs are not stored or reviewed on a regular basis.
Satisfactory: NS queries are limited to zone members only.
Unsatisfactory: All ports are not used and unused ports have not been disabled.
Satisfactory: Data is encrypted on disk or not accessible to any unauthorized personnel or storage attacks.
Unsatisfactory: Tape devices span network zones and are connected to the internal network and the backend storage controllers.
Unsatisfactory: Two e-ports are connected together from each switch.
Unsatisfactory: No authentication is enabled.
Satisfactory: SSH, SSL (HTTPS), and/or SNMPv3.
Satisfactory: SNMP v3 is used or SNMP v1 is used in an isolated management network.
Unsatisfactory: Data and time are not correct.
Unsatisfactory: Error levels are 2 or below.
Satisfactory: Fabric Configuration Services are used.
Unsatisfactory: Interoperability mode is enabled.
Unsatisfactory: Cut-through switching is enabled.

Secure Area Network Program is Complete!
Visit iSEC Partners for more information

SecureNetApp

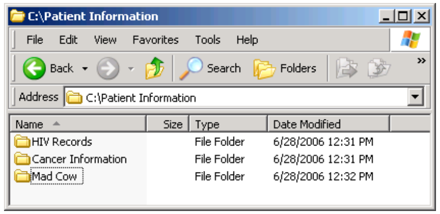
(NetApp Security Configuration Analyzer)

SecureNetApp

- **Secure Configuration Analyzer for NetApp Filers**
  - Why? Because by default, an attacker can:
    - Enumerate:
      - Usernames (e.g. administrator, root, etc)
      - SMB Shares (C$, ETC$)
      - NFS Exports (e.g. /dev/dsk/server2fs3)
      - The administrator ID
      - Authorized Hostnames (e.g. All Machines)
    - Connect and access:
      - NFS Exports with anonymous access
        - » Including the administrative share (ETC$)
    - Bypass Access Controls:
      - UID/GID attacks and gain full rights to all files on the filer
        - » Despite ownerships values!
    - Gain access to passwords
      - Downgrade attacks (NTLM authentication)

NAS Attacks

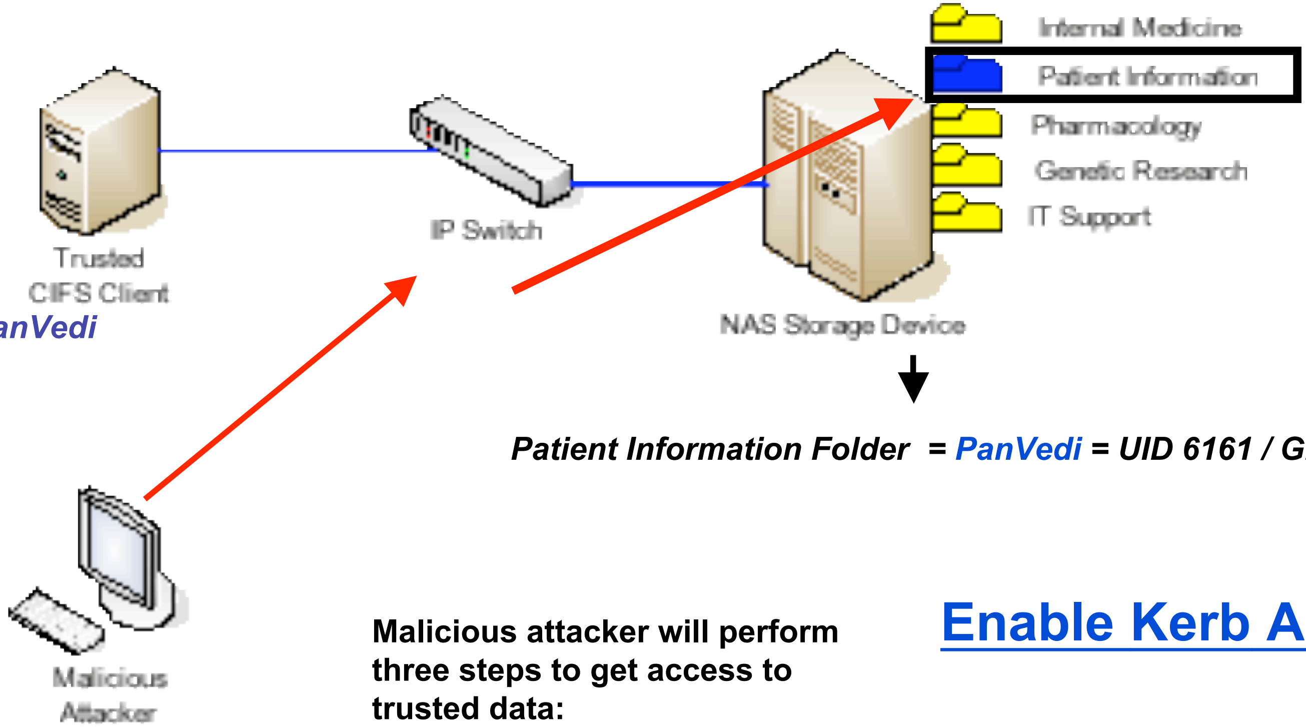
- <u>NAS Attack Demo</u>



Address: C:\Patient Information

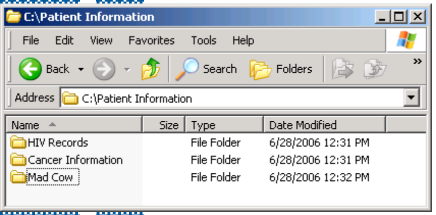
Name	Size	Type	Date Modified
HIV Records		File Folder	6/28/2006 12:31 PM
Cancer Information		File Folder	6/28/2006 12:31 PM
Mad Cow		File Folder	6/28/2006 12:32 PM

Trusted Client has access to Patient Information Folder



Username: PanVedi

Patient Information Folder = PanVedi = UID 6161 / GID 30



Address: C:\Patient Information

Name	Size	Type	Date Modified
HIV Records		File Folder	6/28/2006 12:31 PM
Cancer Information		File Folder	6/28/2006 12:31 PM
Mad Cow		File Folder	6/28/2006 12:32 PM

UID: 6161 , GID: 30

UID: 0 , GID: 0

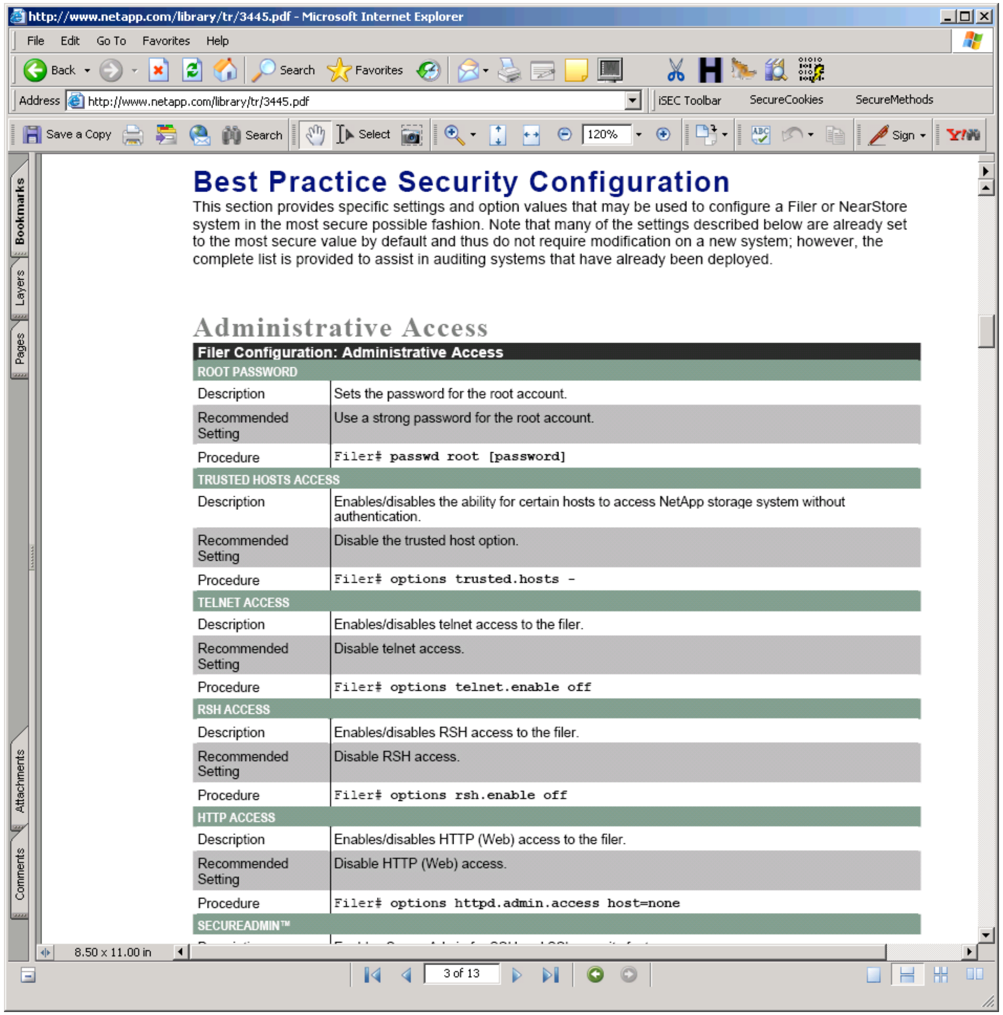
Malicious attacker will perform three steps to get access to trusted data:

1. **Enumerate usernames/shares**
2. **Spoof UID/GID**
3. **See Data**

<u>Enable Kerb Auth!</u>

SecureNetApp

- NetApp Secure Configuration



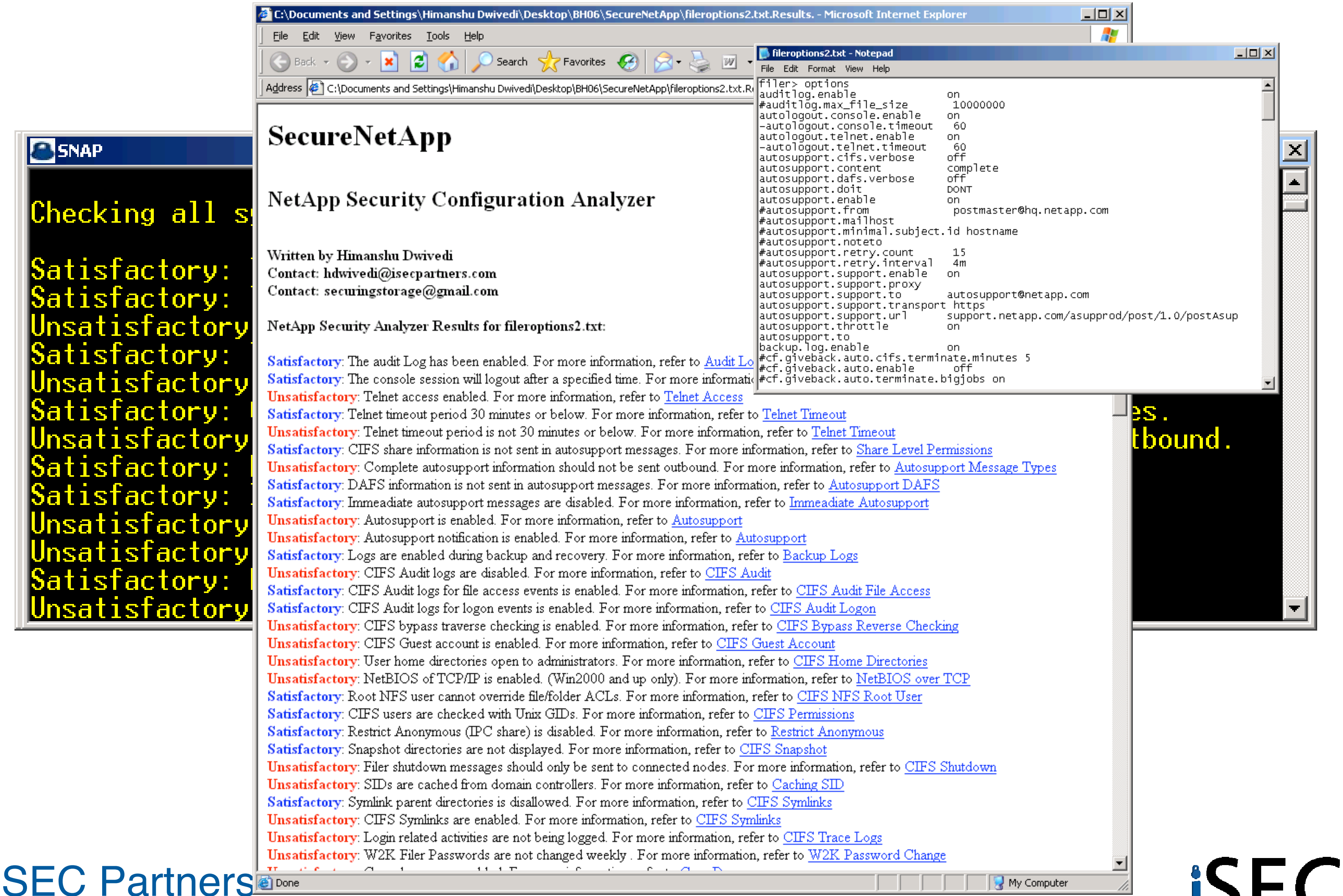
Best Practice Security Configuration

This section provides specific settings and option values that may be used to configure a Filer or NearStore system in the most secure possible fashion. Note that many of the settings described below are already set to the most secure value by default and thus do not require modification on a new system; however, the complete list is provided to assist in auditing systems that have already been deployed.

Administrative Access

Filer Configuration: Administrative Access	
ROOT PASSWORD	
Description	Sets the password for the root account.
Recommended Setting	Use a strong password for the root account.
Procedure	`Filer# passwd root [password]`
TRUSTED HOSTS ACCESS	
Description	Enables/disables the ability for certain hosts to access NetApp storage system without authentication.
Recommended Setting	Disable the trusted host option.
Procedure	`Filer# options trusted.hosts -`
TELNET ACCESS	
Description	Enables/disables telnet access to the filer.
Recommended Setting	Disable telnet access.
Procedure	`Filer# options telnet.enable off`
RSH ACCESS	
Description	Enables/disables RSH access to the filer.
Recommended Setting	Disable RSH access.
Procedure	`Filer# options rsh.enable off`
HTTP ACCESS	
Description	Enables/disables HTTP (Web) access to the filer.
Recommended Setting	Disable HTTP (Web) access.
Procedure	`Filer# options httpd.admin.access host=none`
SECUREADMIN™	

SecureNetApp



```
Checking all s
Satisfactory:
Satisfactory:
Unsatisfactory
Satisfactory:
Unsatisfactory
Satisfactory:
Unsatisfactory
Satisfactory:
Satisfactory:
Unsatisfactory
Unsatisfactory
Satisfactory:
Unsatisfactory
```

```
es.
tbound.
```

C:\Documents and Settings\Himanshu Dwivedi\Desktop\BH06\SecureNetApp\fileroptions2.txt.Results. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\Himanshu Dwivedi\Desktop\BH06\SecureNetApp\fileroptions2.txt.R

SecureNetApp

NetApp Security Configuration Analyzer

Written by Himanshu Dwivedi
Contact: hdwivedi@isecpartners.com
Contact: securingstorage@gmail.com

NetApp Security Analyzer Results for fileroptions2.txt:

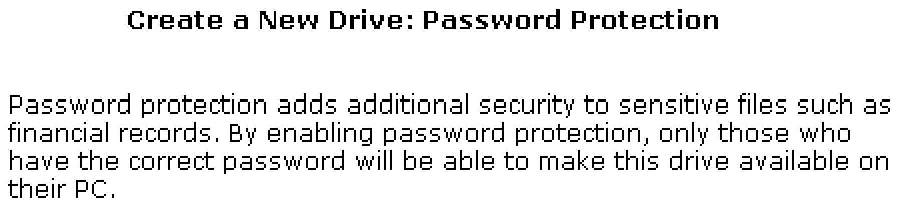
Satisfactory: The audit Log has been enabled. For more information, refer to Audit Lo
Satisfactory: The console session will logout after a specified time. For more informati
Unsatisfactory: Telnet access enabled. For more information, refer to Telnet Access
Satisfactory: Telnet timeout period 30 minutes or below. For more information, refer to Telnet Timeout
Unsatisfactory: Telnet timeout period is not 30 minutes or below. For more information, refer to Telnet Timeout
Satisfactory: CIFS share information is not sent in autosupport messages. For more information, refer to Share Level Permissions
Unsatisfactory: Complete autosupport information should not be sent outbound. For more information, refer to Autosupport Message Types
Satisfactory: DAFS information is not sent in autosupport messages. For more information, refer to Autosupport DAFS
Satisfactory: Immeadiate autosupport messages are disabled. For more information, refer to Immeadiate Autosupport
Unsatisfactory: Autosupport is enabled. For more information, refer to Autosupport
Unsatisfactory: Autosupport notification is enabled. For more information, refer to Autosupport
Satisfactory: Logs are enabled during backup and recovery. For more information, refer to Backup Logs
Unsatisfactory: CIFS Audit logs are disabled. For more information, refer to CIFS Audit
Satisfactory: CIFS Audit logs for file access events is enabled. For more information, refer to CIFS Audit File Access
Satisfactory: CIFS Audit logs for logon events is enabled. For more information, refer to CIFS Audit Logon
Unsatisfactory: CIFS bypass traverse checking is enabled. For more information, refer to CIFS Bypass Reverse Checking
Unsatisfactory: CIFS Guest account is enabled. For more information, refer to CIFS Guest Account
Unsatisfactory: User home directories open to administrators. For more information, refer to CIFS Home Directories
Unsatisfactory: NetBIOS of TCP/IP is enabled. (Win2000 and up only). For more information, refer to NetBIOS over TCP
Satisfactory: Root NFS user cannot override file/folder ACLs. For more information, refer to CIFS NFS Root User
Satisfactory: CIFS users are checked with Unix GIDs. For more information, refer to CIFS Permissions
Satisfactory: Restrict Anonymous (IPC share) is disabled. For more information, refer to Restrict Anonymous
Satisfactory: Snapshot directories are not displayed. For more information, refer to CIFS Snapshot
Unsatisfactory: Filer shutdown messages should only be sent to connected nodes. For more information, refer to CIFS Shutdown
Unsatisfactory: SIDs are cached from domain controllers. For more information, refer to Caching SID
Satisfactory: Symlink parent directories is disallowed. For more information, refer to CIFS Symlinks
Unsatisfactory: CIFS Symlinks are enabled. For more information, refer to CIFS Symlinks
Unsatisfactory: Login related activities are not being logged. For more information, refer to CIFS Trace Logs
Unsatisfactory: W2K Filer Passwords are not changed weekly . For more information, refer to W2K Password Change

```
filer> options
auditlog.enable              on
#auditlog.max_file_size       10000000
autologout.console.enable    on
-autologout.console.timeout   60
autologout.telnet.enable     on
-autologout.telnet.timeout    60
autosupport.cifs.verbose     off
autosupport.content          complete
autosupport.dafs.verbose     off
autosupport.doit             DONT
autosupport.enable           on
#autosupport.from             postmaster@hq.netapp.com
#autosupport.mailhost
#autosupport.minimal.subject.id hostname
#autosupport.noteto
#autosupport.retry.count      15
#autosupport.retry.interval   4m
autosupport.support.enable   on
autosupport.support.proxy
autosupport.support.to       autosupport@netapp.com
autosupport.support.transport https
autosupport.support.url      support.netapp.com/asupprod/post/1.0/postAsup
autosupport.throttle         on
autosupport.to
backup.log.enable            on
#cf.giveback.auto.cifs.terminate.minutes 5
#cf.giveback.auto.enable      off
#cf.giveback.auto.terminate.bigjobs on
```

Home Storage
(NetGear Z-SAN)

Z-SAN

- **NetGear Z-SAN**
  - “Home SAN”
- Do home office products need to be secure?
  - SoHo Firewalls
  - Linksys/Netgear Wireless AP
- What if they encourage the storage of financial information?

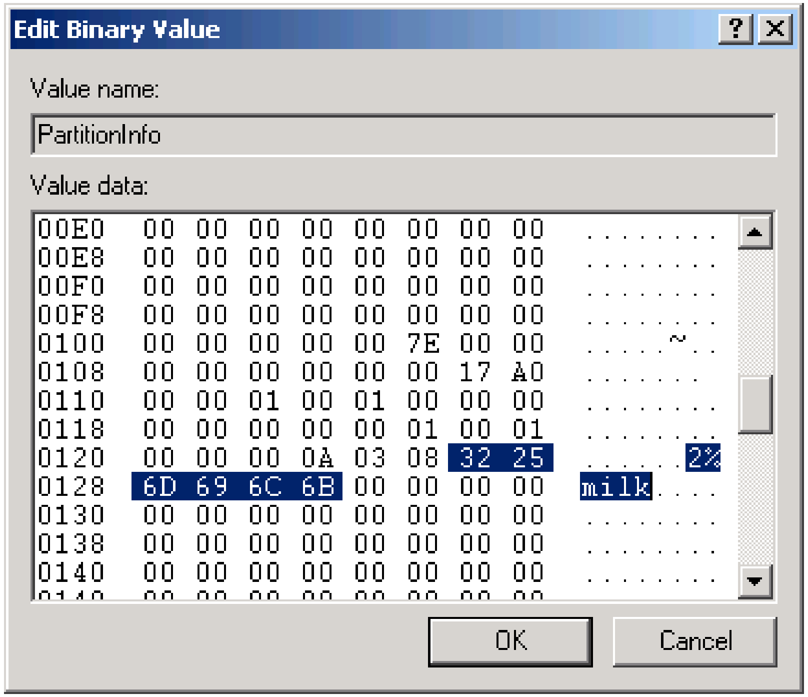


Create a New Drive: Password Protection

Password protection adds additional security to sensitive files such as financial records. By enabling password protection, only those who have the correct password will be able to make this drive available on their PC.

Z-SAN

- Admin Passwords to reset drive passwords are stored in the registry…in the clear
  - HKLM\Software\ZNS\client\[Identifier]



Value name:

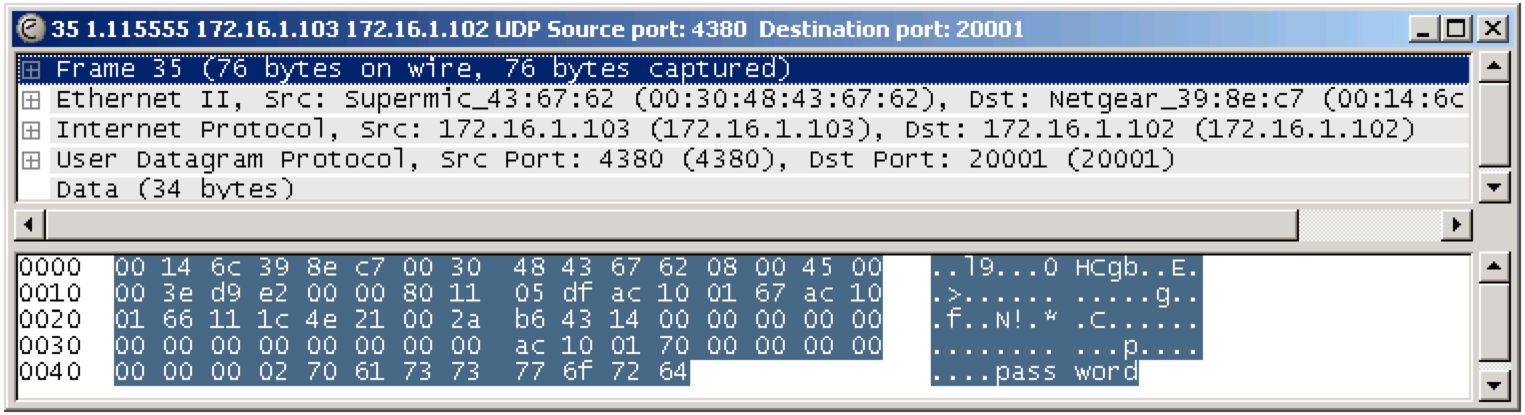
PartitionInfo

Value data:

```
00E0   00  00  00  00  00  00  00  00    ........
00E8   00  00  00  00  00  00  00  00    ........
00F0   00  00  00  00  00  00  00  00    ........
00F8   00  00  00  00  00  00  00  00    ........
0100   00  00  00  00  00  7E  00  00    .....~..
0108   00  00  00  00  00  00  17  A0    .......
0110   00  00  01  00  01  00  00  00    ........
0118   00  00  00  00  00  01  00  01    ........
0120   00  00  00  0A  03  08  32  25    ......2%
0128   6D  69  6C  6B  00  00  00  00    milk....
0130   00  00  00  00  00  00  00  00    ........
0138   00  00  00  00  00  00  00  00    ........
0140   00  00  00  00  00  00  00  00    ........
```

Z-SAN

- Drive passwords are sent over the network in clear text
  - UDP port 20001
  - Sent several times a minute (repeated)



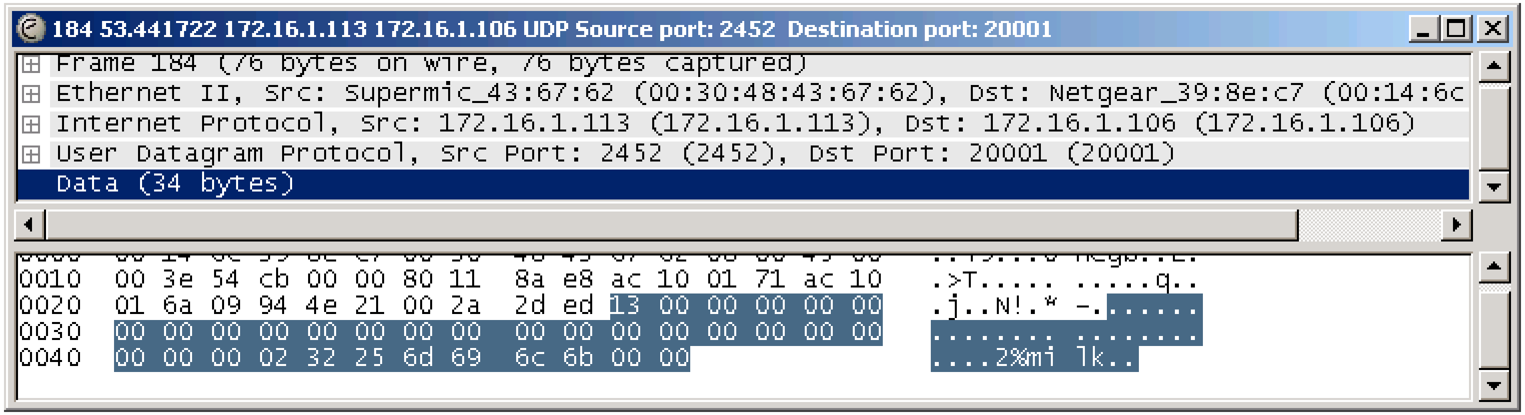
35 1.115555 172.16.1.103 172.16.1.102 UDP Source port: 4380 Destination port: 20001

```
⊞ Frame 35 (76 bytes on wire, 76 bytes captured)
⊞ Ethernet II, Src: Supermic_43:67:62 (00:30:48:43:67:62), Dst: Netgear_39:8e:c7 (00:14:6c
⊞ Internet Protocol, Src: 172.16.1.103 (172.16.1.103), Dst: 172.16.1.102 (172.16.1.102)
⊞ User Datagram Protocol, Src Port: 4380 (4380), Dst Port: 20001 (20001)
  Data (34 bytes)
```

```
0000  00 14 6c 39 8e c7 00 30  48 43 67 62 08 00 45 00   ..l9...0 HCgb..E.
0010  00 3e d9 e2 00 00 80 11  05 df ac 10 01 67 ac 10   .>...... .....g..
0020  01 66 11 1c 4e 21 00 2a  b6 43 14 00 00 00 00 00   .f..N!.* .C......
0030  00 00 00 00 00 00 00 00  ac 10 01 70 00 00 00 00   ........ ...p....
0040  00 00 00 02 70 61 73 73  77 6f 72 64               ....pass word
```

Z-SAN

- Admin Passwords to reset drive passwords are also sent over the network in clear text
  - UDP port 20001



184 53.441722 172.16.1.113 172.16.1.106 UDP Source port: 2452 Destination port: 20001

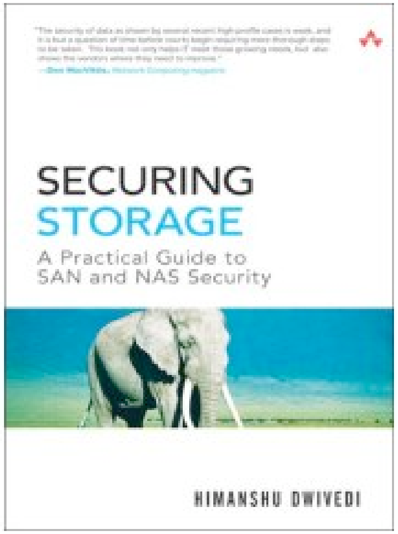
```
⊞ Frame 184 (76 bytes on wire, 76 bytes captured)
⊞ Ethernet II, Src: Supermic_43:67:62 (00:30:48:43:67:62), Dst: Netgear_39:8e:c7 (00:14:6c
⊞ Internet Protocol, Src: 172.16.1.113 (172.16.1.113), Dst: 172.16.1.106 (172.16.1.106)
⊞ User Datagram Protocol, Src Port: 2452 (2452), Dst Port: 20001 (20001)
  Data (34 bytes)
```

```
0010  00 3e 54 cb 00 00 80 11  8a e8 ac 10 01 71 ac 10   .>T..... .....q..
0020  01 6a 09 94 4e 21 00 2a  2d ed 13 00 00 00 00 00   .j..N!.* -.......
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 02 32 25 6d 69  6c 6b 00 00              ....2%mi lk..
```

Conclusion

- Storage isn't secure by default
  - Fibre Channel
  - iSCSI
  - NAS
  - Home SANs
- Use tools to enumerate and mitigate storage security problems
  - **SNAP (Storage Network Audit Program)**
- Use tools to lock down your storage devices
  - **SecureNetApp**

Questions



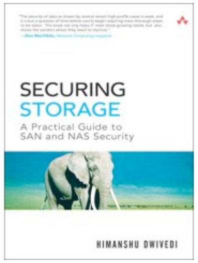
- **Himanshu Dwivedi**
  - hdwivedi@isecpartners.com
  - securingstorage@gmail.com
- **Tools**
  - https://www.isecpartners.com/tools.html
- **Book's Website**
  - http://www.isecpartners.com/securingstorage.html

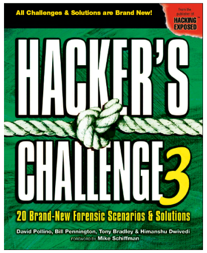
iSEC Partners

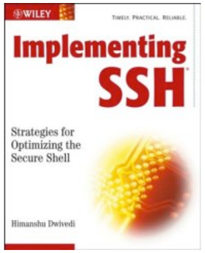
- **Information Security**
  - **Consulting**
  - **Tools**
  - **Products**
- **Specialization**
  - Application Security
    - Java, Win32 Analysis, .Net, C, C++, Python/Perl
  - Web Services
    - SOAP, XML, AJAX
  - Product Penetration Tests:
    - Applications (Siebel OnDemand, Macromedia Flash, WebEx Meeting)
    - Appliances (Juniper SSL-VPN/JEDI, Sarvega XML Gateway)
  - Storage Security
    - FibreChannel, iSCSI, CIFS/NFS

iSEC Research

- **BlackHat 2006: 4 Presentations (5 speakers)**
  - **Fuzzing Selected Win32 Interprocess Communication Mechanisms**
  - **Attacking Internationalized Software**
  - **Breaking AJAX Web Applications: Vulns 2.0 in Web 2.0**
  - **I'm going to shoot the next person who says VLANS**
- **Whitepapers**
  - Cross Site Reference Forgery (XSRF)
  - Software Penetration Testing
- **Tools**
  - Application: Elzap, SecureCookies, WSBang, WSMap
  - Infrastructure: SecureCisco, SecureBigIP, CiscoIPv6check, SecureWin2003, SecureWinXP
  - Storage: CPT, StorScan
- **Books**
  - Implementing SSH
  - Securing Storage
  - Hacker's Challenge 3




All Challenges & Solutions are Brand New!
HACKING EXPOSED
HACKER'S
CHALLENGE 3
20 Brand-New Forensic Scenarios & Solutions
David Pollino, Bill Pennington, Tony Bradley & Himanshu Dwivedi
Mike Schiffman


WILEY
TIMELY. PRACTICAL. RELIABLE.
Implementing
SSH
Strategies for Optimizing the Secure Shell
Himanshu Dwivedi