iSCSI Security

(Insecure SCSI)

Presenter:

Himanshu Dwivedi

iSEC PARTNERS

Agenda

- **Introduction**
- **iSCSI Attacks**
  - Enumeration
  - Authorization
  - Authentication
- **iSCSI Defenses**

Information Security Partners (iSEC)

- **iSEC Partners**
  - Independent security consulting and product organization
- **Our Focus**
  - Application Security
    - Java, C++ and .NET applications
    - **Attacking Web Services (XML, SOAP) – Alex Stamos and Scott Stender**
  - Network Security
    - Firewalls, Routers/Switches, VPNs, and Operating Systems
  - **Storage Security**
    - **NAS, iSCSI, and SANs**
  - Product Security
    - Software Applications (home grown and commercial off-the shelf)
    - Hardware Appliances (devices)
- **For more information**
  - https://www.isecpartners.com

Introduction

- **iSCSI**

i	=	Internet Protocol
SCSI	=	Small Computer System Interface
iSCSI	=	**Insecure SCSI**

- **What is iSCSI?**
  - iSCSI (Internet Small Computer Systems Interface) provides access to block level data over traditional IP networks
  - SCSI blocks have mostly been used with Fibre Channel SANs
  - Unlike NAS storage devices using CIFS/NFS at the file level, SCSI blocks work at lower levels by offering entire data stores (LUNs) to iSCSI clients

Introduction

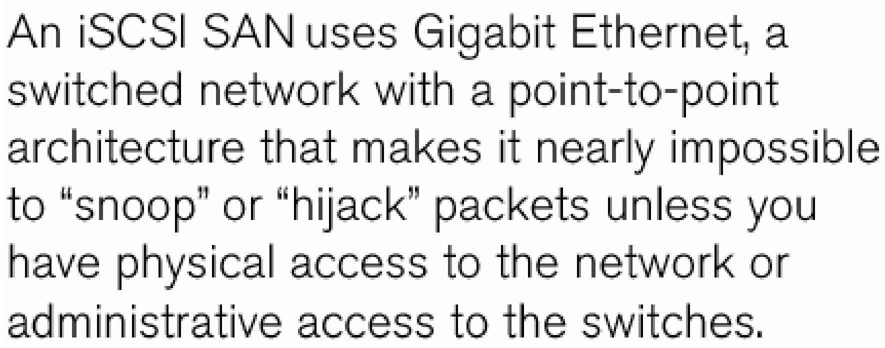
- **Block level vs. File level**
  - File Level: CIFS (SMB) and NFS file systems over a network connection
  - Block Level: The actually drive (not the file system) over a network
  - Simplistic example: A file system versus an entire hard drive

- **Security and iSCSI**
  - Authentication – CHAP (weak)
  - Authorization – Initiator Node Names (spoof-able)
  - Encryption – IPSec shared secret (deployment challenges)

- **Why should we care?**
  - A compromise of a single iSCSI device equates to the compromise of several (10 to 100) operating systems at once!
    - Who cares about admin, root, or system accounts when the entire data store can be compromised?

Introduction

- What *some* vendors say about iSCSI Security



An iSCSI SAN uses Gigabit Ethernet, a switched network with a point-to-point architecture that makes it nearly impossible to "snoop" or "hijack" packets unless you have physical access to the network or administrative access to the switches.

- Implies trusting everyone (employees, vendors, business partners, guests, contractors, consultants, wireless users, and remote VPN users) that is connected to the internal network

Agree to…..

- Remove all file permissions from all folders in every operating system
- Allow everyone to read everyone else's email
- Remove all passwords from databases
- Allow everyone to view HR information (Soc Sec Numbers, Salaries)
- Tell the Auditors that "Internal controls are for sissies"

Introduction

- **iSCSI Architecture Components**
  - iSCSI Initiator: An iSCSI client
  - iSCSI Target: An iSCSI storage device/appliance
  - iSNS (optional): iSCSI Name Services (A table that groups iSCSI Initiators and Targets in Domain Sets for logical segmentation

- **Terms and Definitions**
  - iQN: Initiator Node Name (Identity value for iSCSI clients, similar to MAC addresses)
  - Domain Sets: Logical segmentation of iSCSI entities (Targets and Initiators into separate groups)
  - LUNs: Logical Unit Numbers (A logical array of storage units. One storage entity can be divided into multiple LUNs)

Introduction

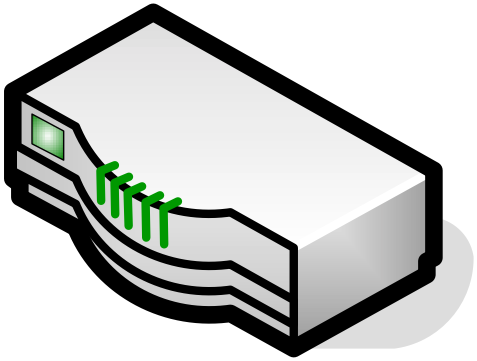
- **iSCSI Initiators**
  - iSCSI Clients
  - Use a regular NIC (IP) with an iSCSI client driver
- **iSCSI Drivers**
  - Microsoft
  - Cisco
  - IBM
  - HP
- **NO special hardware required**
- **Works over existing IP networks**

iSCSI Driver

Regular Operating Sysem

Introduction

- **iSCSI Targets**
  - iSCSI Devices (Appliances)/Servers
  - Offer large volumes of data (block level) over the IP network
- **iSCSI Vendors**
  - Cisco
  - EMC
  - Network Appliance
  - HP
  - IBM
- **Listens on TCP port 3260**



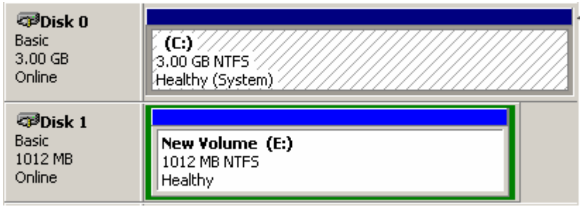
iSCSI Device

Introduction

- **Example iSCSI Architecture**

Local =

Network LUN =

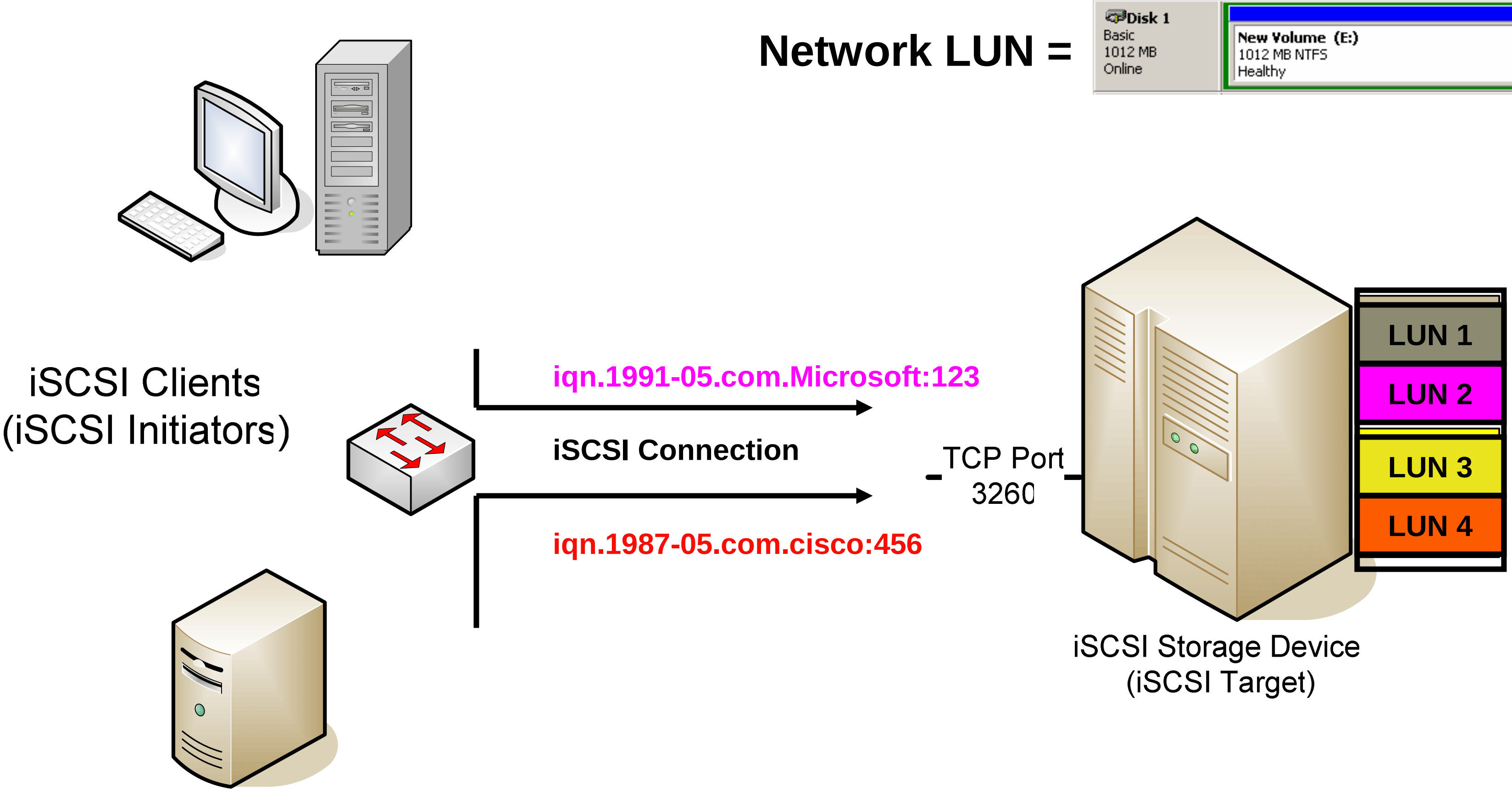


Disk 0
Basic
3.00 GB
Online

(C:)
3.00 GB NTFS
Healthy (System)

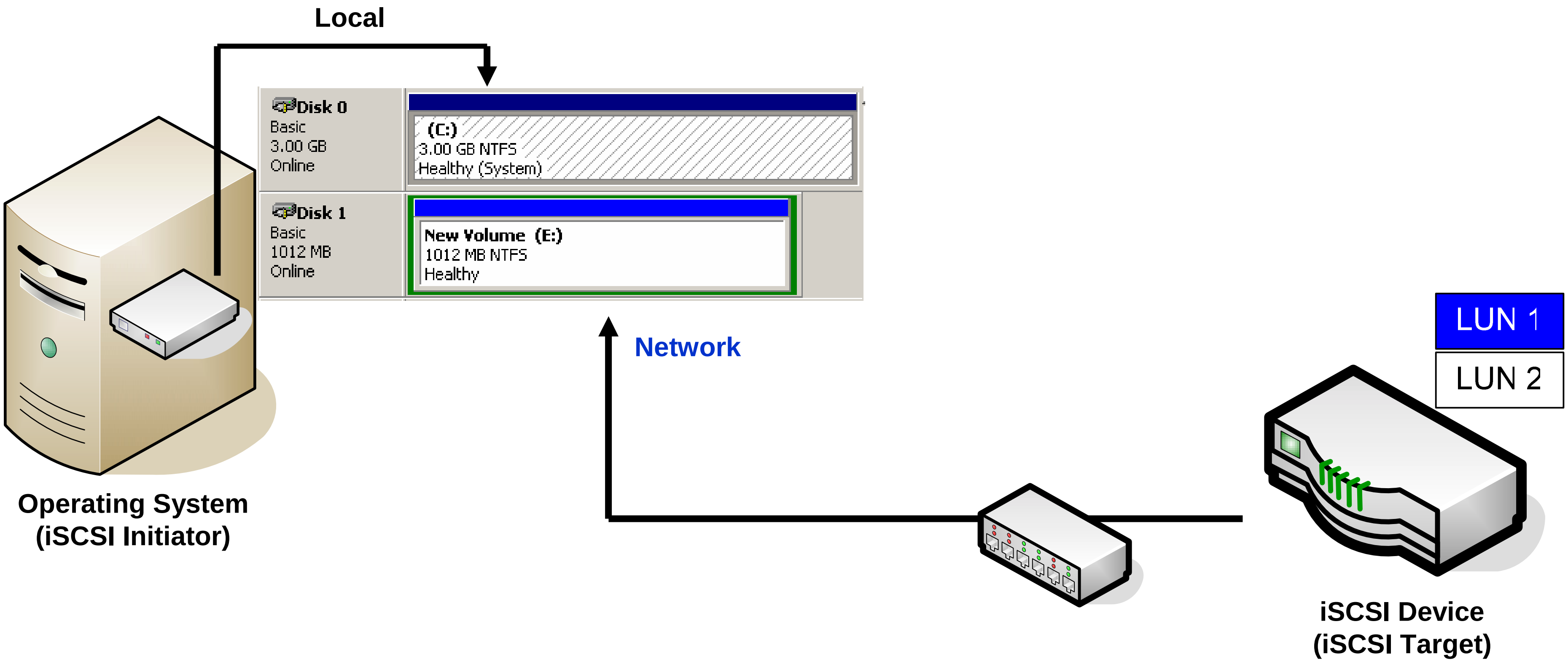
Disk 1
Basic
1012 MB
Online

New Volume (E:)
1012 MB NTFS
Healthy



Introduction

- iSCSI allows block data to be available over the IP network



Local

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

Network

LUN 1

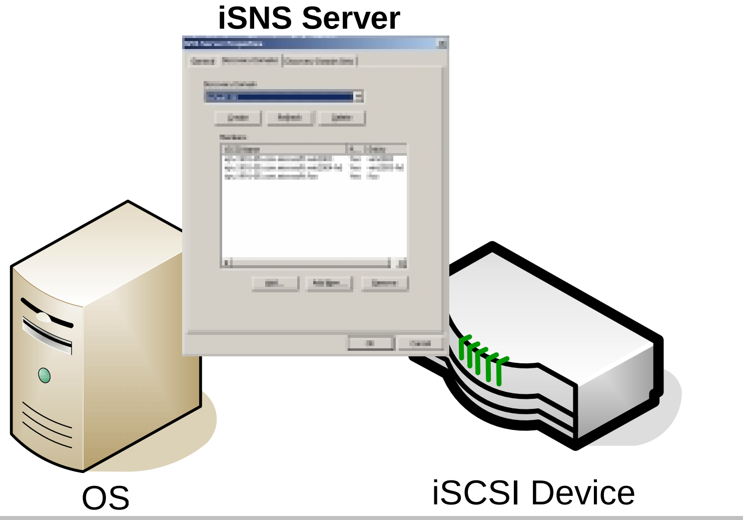
LUN 2

Operating System
(iSCSI Initiator)

iSCSI Device
(iSCSI Target)

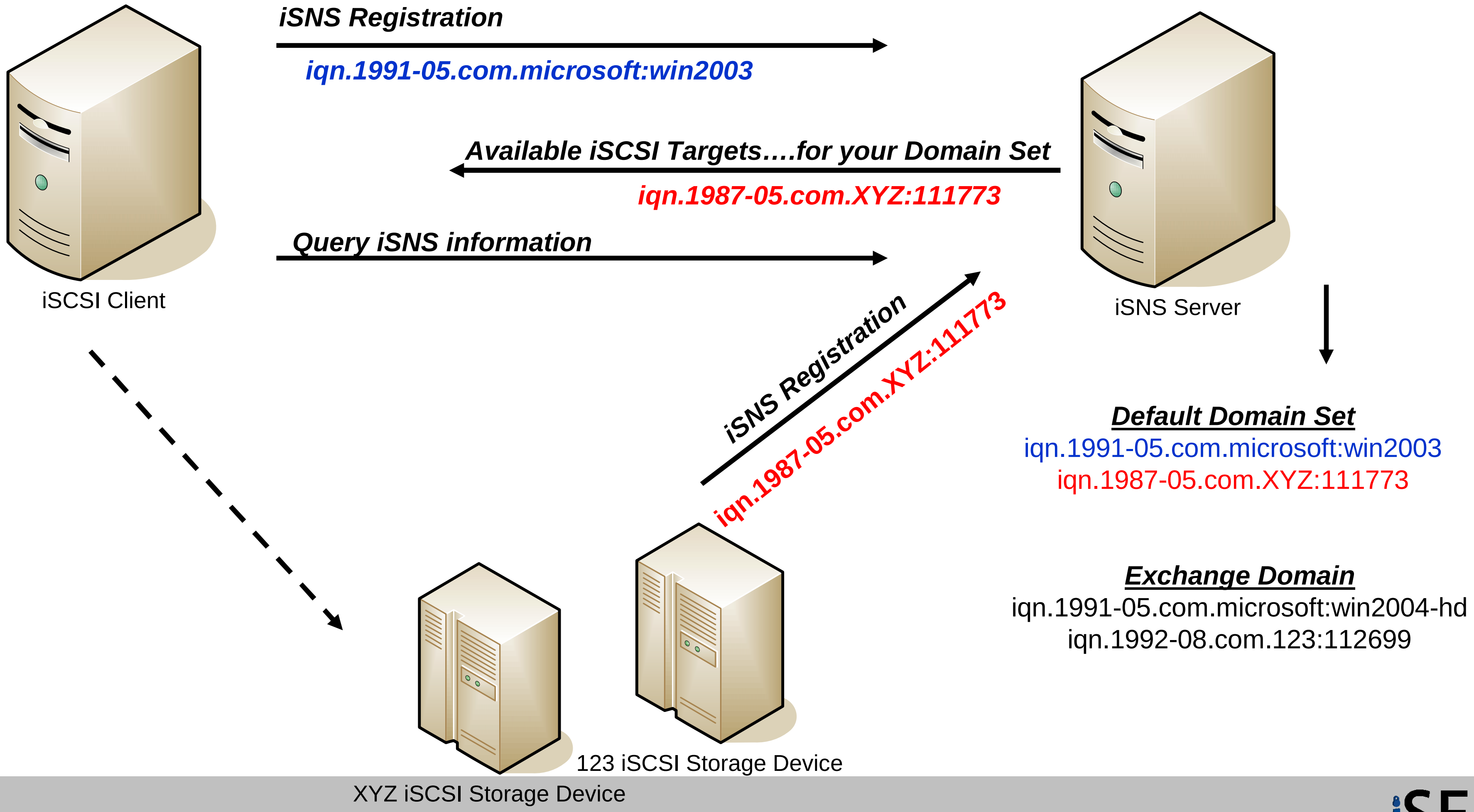
Introduction

- **iSNS Servers (iSCSI Simple Name Services)**
  - Software that runs on an operating system or an iSCSI Device
  - iSCSI initiators and targets register with the iSNS server
    - Similar to DNS
  - An iSNS server is responsible for:
    - Informing iSCSI clients about which iSCSI targets are available on the network
    - Grouping iSCSI clients to their correct Domain Set
    - Informing iSCSI clients what security aspects (if any) they must use to associate to targets
  - Listens on port TCP 3205.



Introduction

- **iSNS Model**



iSNS Registration

iqn.1991-05.com.microsoft:win2003

Available iSCSI Targets….for your Domain Set

iqn.1987-05.com.XYZ:111773

Query iSNS information

iSNS Registration

iqn.1987-05.com.XYZ:111773

iSCSI Client

iSNS Server

123 iSCSI Storage Device

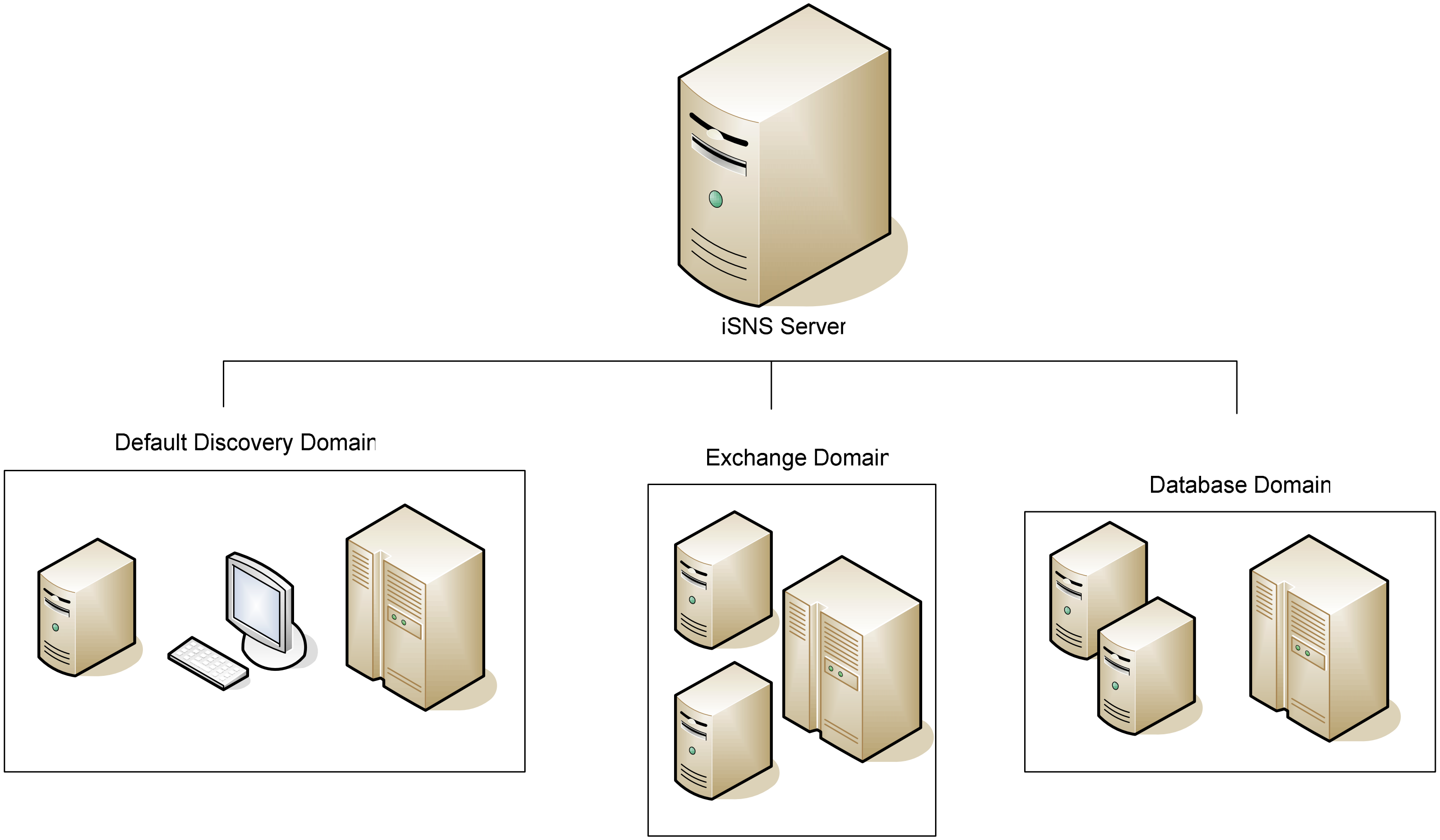
XYZ iSCSI Storage Device

Default Domain Set
iqn.1991-05.com.microsoft:win2003
iqn.1987-05.com.XYZ:111773

Exchange Domain
iqn.1991-05.com.microsoft:win2004-hd
iqn.1992-08.com.123:112699

Introduction

- **iSNS Example**



Introduction

Top 5 iSCSI Security Issues

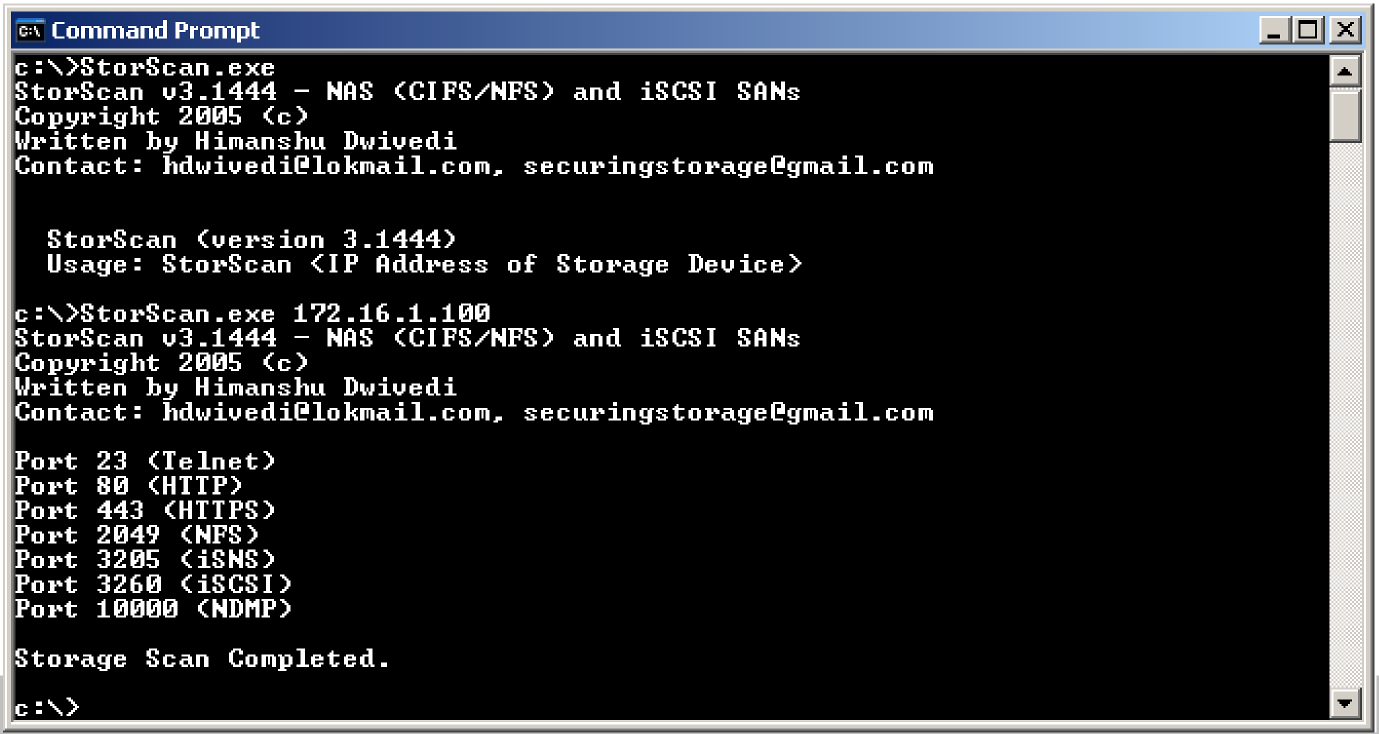
1. **iQN Values are trusted**
   a. iQN are spoof-able, sniff-able, and can be brute-forced
2. **iSCSI Authorization is the only required security entity, which relies on iQN values**
3. **iSCSI Authentication is disabled by default**
4. **iSCSI Authentication uses CHAP**
5. **iSNS servers are not protected**

iSCSI is a clear text protocol

iSCSI Enumeration

iSCSI Enumeration

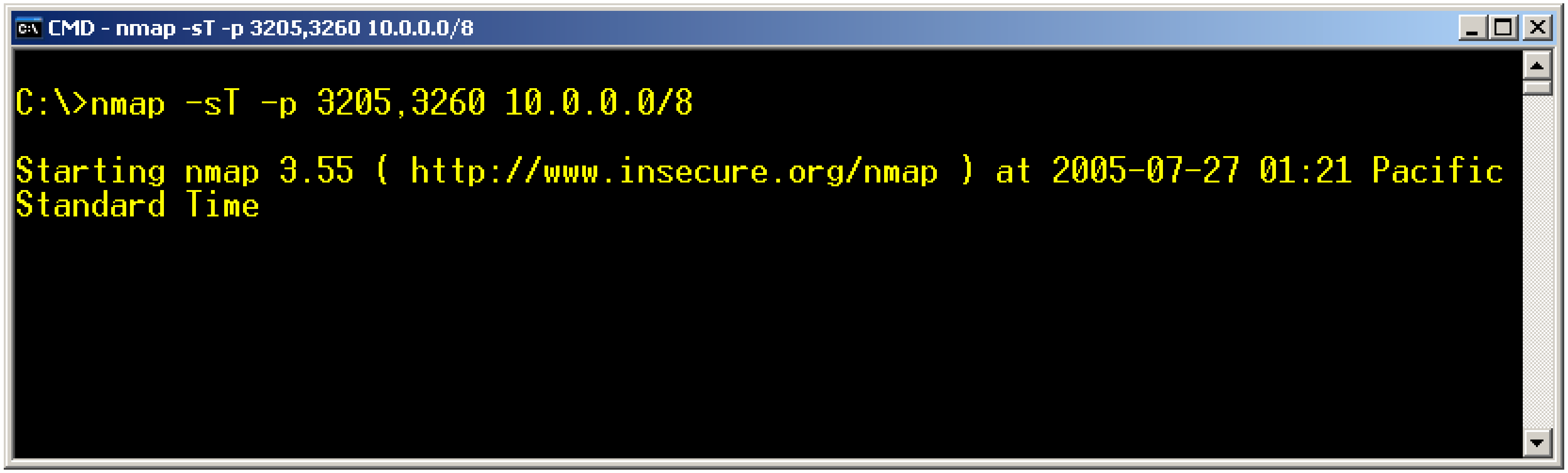
- **Scanning iSCSI Targets (Devices)**
  - TCP port 3260 and 3205
  - StorScan is a focused port scanner for storage devices
    - iSCSI SANs and IP NAS
    - Yes. Nmap is much better, but StorScan is focused (filtered)
  - storscan.exe <range>



```
c:\>StorScan.exe
StorScan v3.1444 - NAS (CIFS/NFS) and iSCSI SANs
Copyright 2005 (c)
Written by Himanshu Dwivedi
Contact: hdwivedi@lokmail.com, securingstorage@gmail.com


  StorScan (version 3.1444)
  Usage: StorScan <IP Address of Storage Device>

c:\>StorScan.exe 172.16.1.100
StorScan v3.1444 - NAS (CIFS/NFS) and iSCSI SANs
Copyright 2005 (c)
Written by Himanshu Dwivedi
Contact: hdwivedi@lokmail.com, securingstorage@gmail.com

Port 23 (Telnet)
Port 80 (HTTP)
Port 443 (HTTPS)
Port 2049 (NFS)
Port 3205 (iSNS)
Port 3260 (iSCSI)
Port 10000 (NDMP)

Storage Scan Completed.

c:\>
```

iSCSI Enumeration

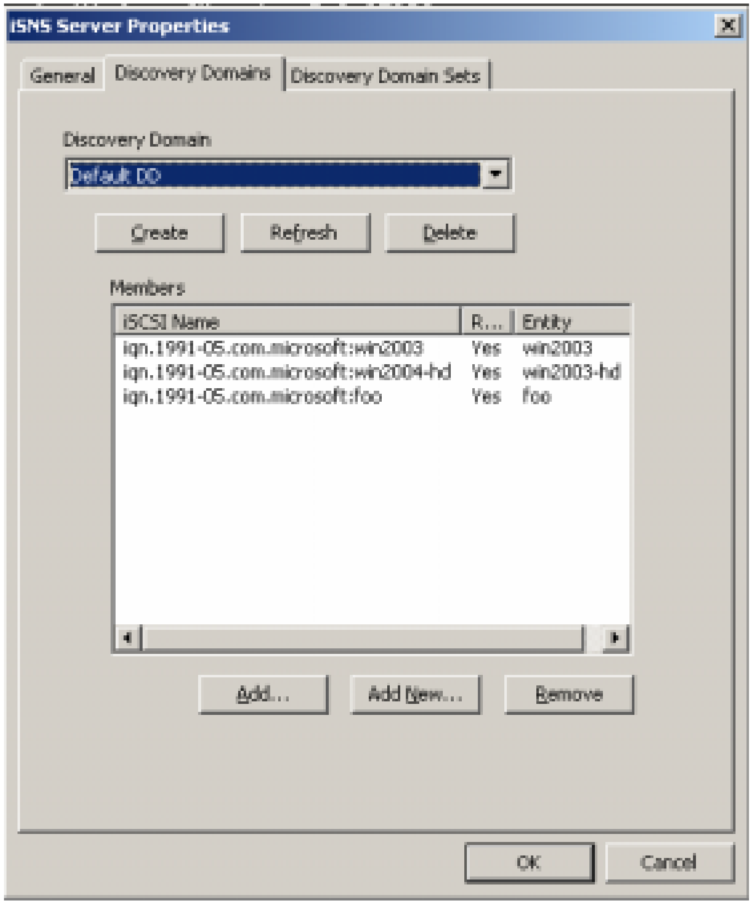
- **Enumeration**
  - iSCSI Targets (iSCSI Devices)
    - Listen on TCP port 3260
  - iSNS
    - Listen on TCP port 3205
  - iSCSI Clients
    - Do not listen on a port, but can be enumerated from the iSNS server



```
C:\>nmap -sT -p 3205,3260 10.0.0.0/8

Starting nmap 3.55 ( http://www.insecure.org/nmap ) at 2005-07-27 01:21 Pacific
Standard Time
```

iSCSI Enumeration

- **iSNS registration**
  - If unique Domain Sets are not created, each iqn will be placed in the Default Domain Set.
  - Any member of a domain set will be able to enumerate/access the other nodes in the same domain set
    - This is why it is important to move nodes out of the Default Domain Set
  - Foo can
    1. Scan for port 3205 and find a iSNS server
    2. Connect to the iSNS server
    3. Enumerate the other iSCSI nodes, which can now be used for iqn spoofing attacks (*described later*)



Discovery Domain: Default DD

Members

iSCSI Name	R...	Entity
iqn.1991-05.com.microsoft:win2003	Yes	win2003
iqn.1991-05.com.microsoft:win2004-hd	Yes	win2003-hd
iqn.1991-05.com.microsoft:foo	Yes	foo

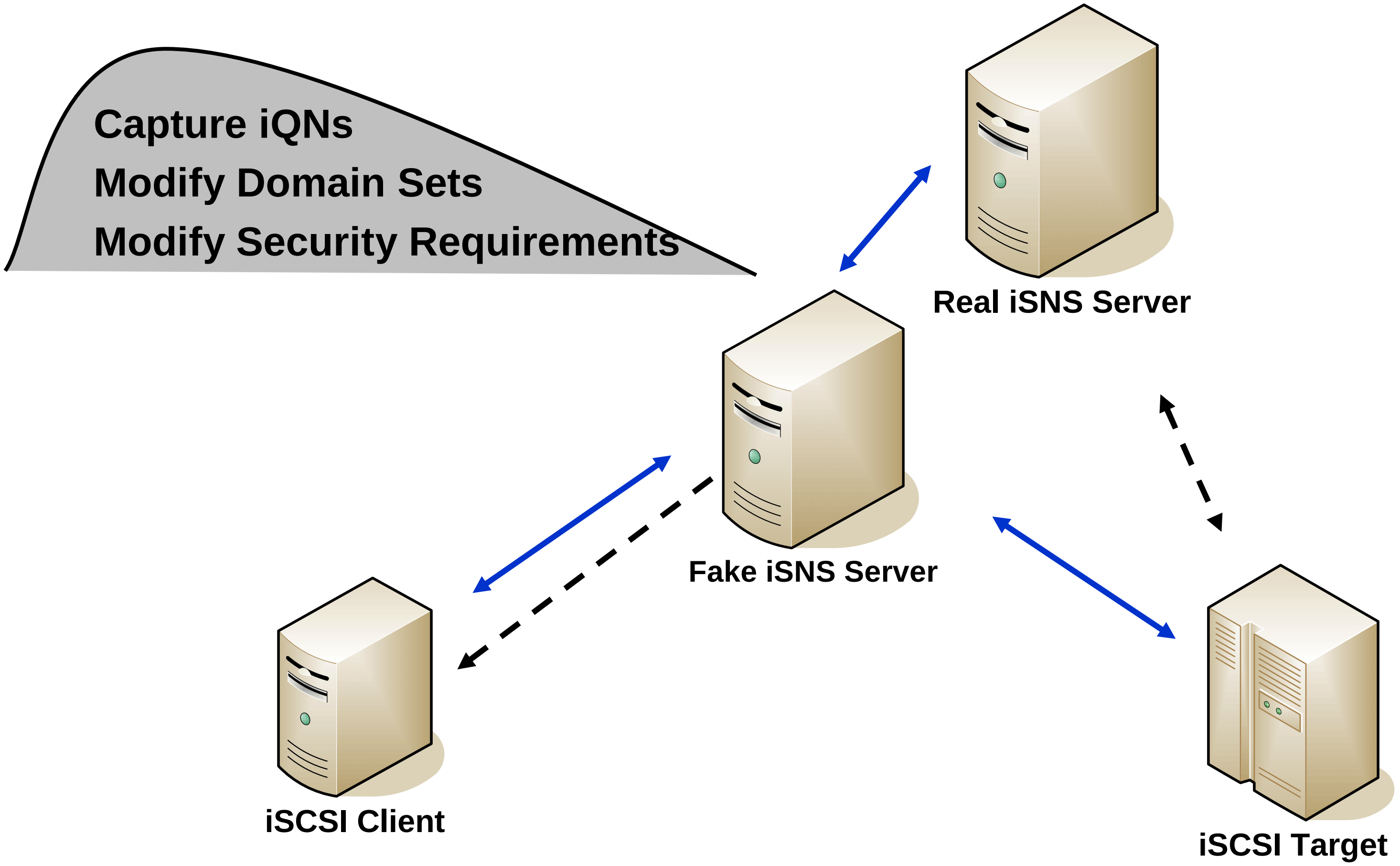
iSCSI Enumeration

- **iSNS Man-in-the-Middle**
  - Identify iSNS server on port 3205
  - Using layer 2 ARP poisoning attacks, a fake iSNS server can replace the real iSNS server
    - The real iSNS will continue to receive iSNS information from targets and clients, but after the fake iSNS has control of the packets
    - This allows the fake iSNS server to
      - View all registrations (both targets and clients)
      - Modify or change Domain Sets
      - Downgrade Domain Sets that require security

        (remove authentication or encryption)

iSCSI Enumeration

- iSNS MITM



Capture iQNs

Modify Domain Sets

Modify Security Requirements

Real iSNS Server

Fake iSNS Server

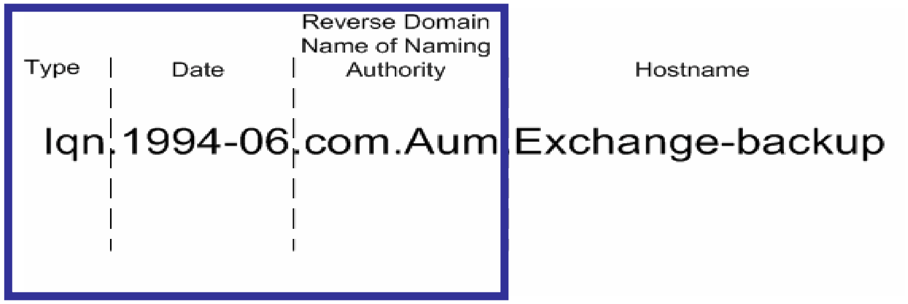
iSCSI Client

iSCSI Target

iSCSI Authorization

iSCSI Authorization

- **iSCSI**
  - Authorization (Required)
    - Required iSCSI Security component
    - Initiator Node Name


Type
Date
Reverse Domain Name of Naming Authority
Hostname
Iqn.1994-06.com.Aum Exchange-backup

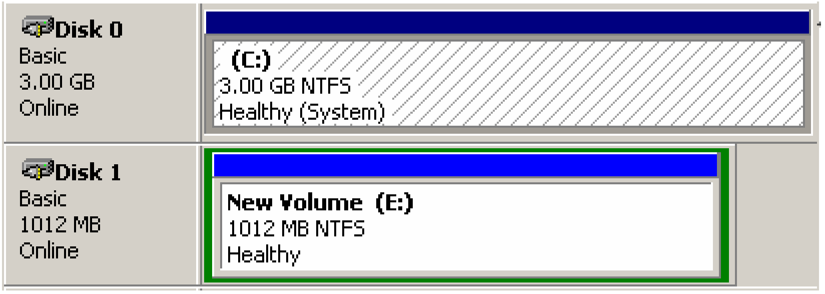
  - Only unknown variable is the end string
    - » iqn.1991-05.com.microsoft:HOSTNAME
    - » iqn.1987-05.com.cisco:xxxxxx
    - » iqn.1992-08.com.ibm:<partition identifier>
  - iQNs traverse the network in CLEAR-TEXT
    - » Easily sniffable, guessable, or enumerated
- An attacker can get access to large amounts of data with little effort

iSCSI Authorization

- **iSCSI Authorization Attack**
  - Sniff iSCSI Communication
    - Port 3260
    - Get Initiator Node Names
  - Spoof the Initiator Node Name
    - Change Initiator name with iSCSI driver
  - See Data
    - Gain access to confidential and sensitive data

iSCSI Security

- **iSCSI Attack Demo**



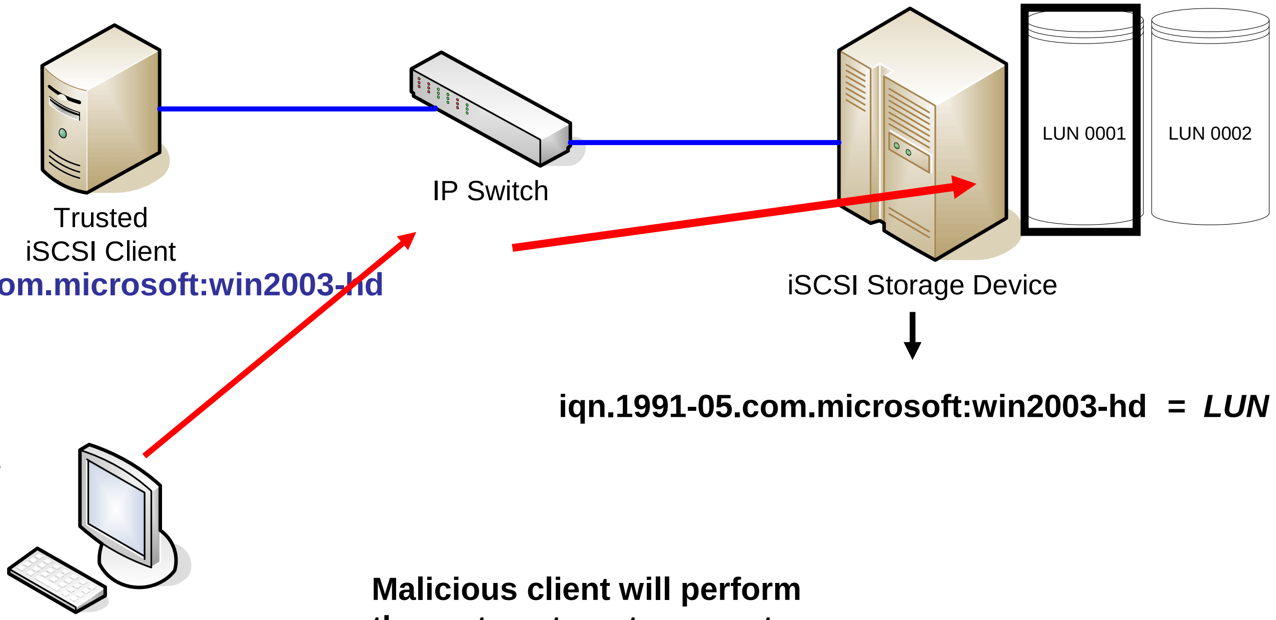
Disk 0
Basic
3.00 GB
Online

(C:)
3.00 GB NTFS
Healthy (System)

Disk 1
Basic
1012 MB
Online

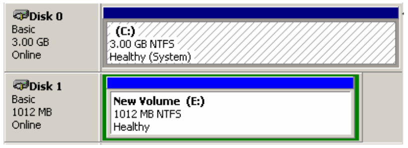
New Volume (E:)
1012 MB NTFS
Healthy

Trusted Client has access to LUN 0001



iqn.1991-05.com.microsoft:win2003-hd

iqn.1991-05.com.microsoft:win2003-hd = ***LUN 0001***



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

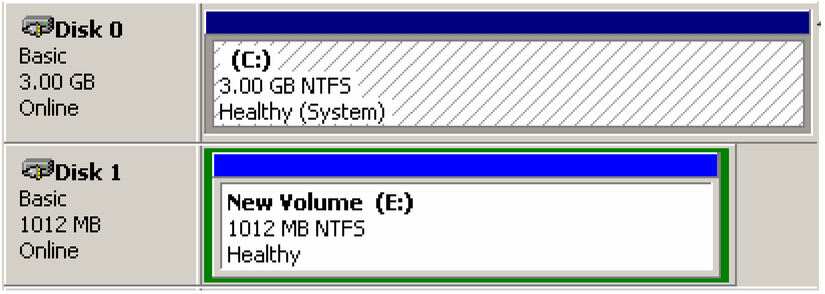
iqn.1991-05.com.microsoft:win2003-hd

iqn.1991-05.com.microsoft:win2003-j1

Malicious client will perform three steps to get access to trusted data:
1. Sniff
2. Spoof
3. See Data

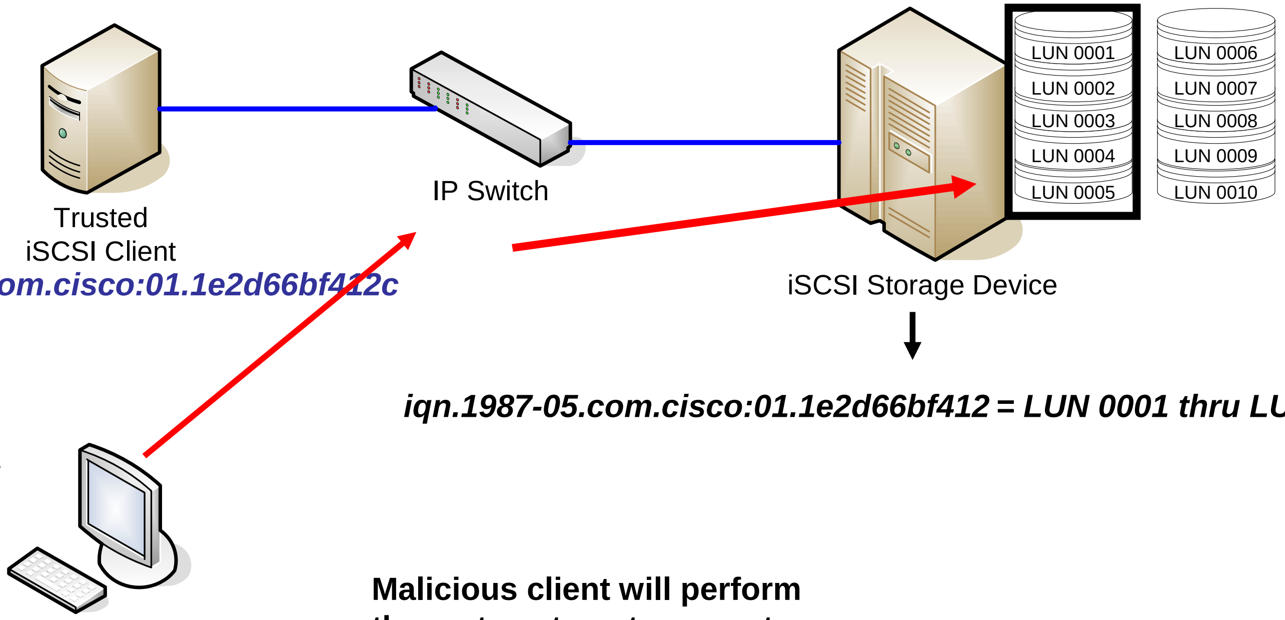
iSCSI Security

- **iSCSI Attack Demo**



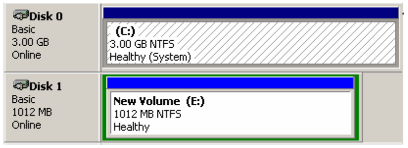
Disk 0 Basic 3.00 GB Online	**(C:)** 3.00 GB NTFS Healthy (System)
Disk 1 Basic 1012 MB Online	**New Volume (E:)** 1012 MB NTFS Healthy

Trusted 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

iqn.1991-05.com.microsoft:win2003

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

1. Sniff

2. Spoof

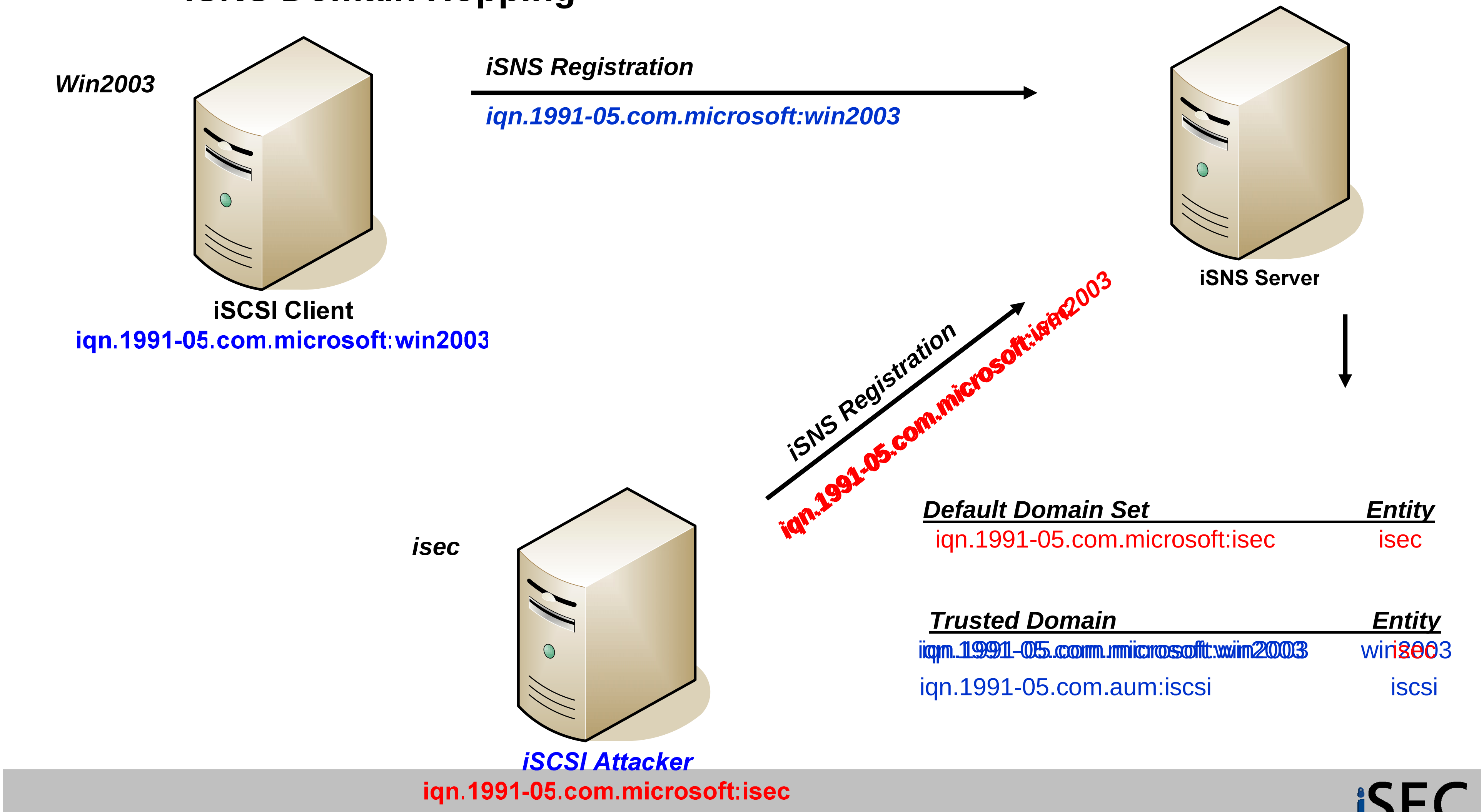
3. See Data

iSNS Domain Hopping

- **iSNS Domain (iGroup) Hopping**
  - Similar to VLAN hopping and Zone hopping (Fibre channel)
  - Discovery Domains/iGroups rely on the iQN value of a node for identification
  - If a node simply spoofs the iQN value to match the iQN of their target, the iSNS server will automatically update and overwrite the legitimate node’s information with the attacker’s spoofed information
- **Domain/iGroup Damage:**
  - At a minimum, this is a Denial of Service Attack
  - At a maximum, this would allow unauthorized hosts to access targets (and their data LUNs) in restricted domains

iSNS Domain Hopping

- **iSNS Domain Hopping**

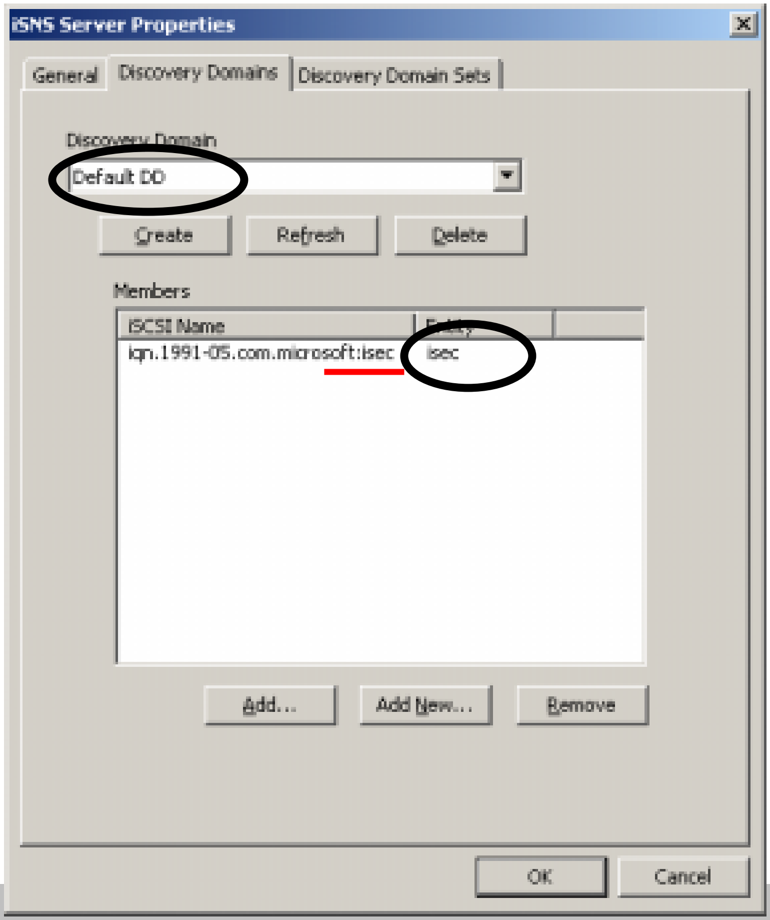

Win2003
iSNS Registration
iqn.1991-05.com.microsoft:win2003
iSCSI Client
iqn.1991-05.com.microsoft:win2003
iSNS Server
iSNS Registration
iqn.1991-05.com.microsoft:win2003
iqn.1991-05.com.microsoft:isec
isec
iSCSI Attacker
iqn.1991-05.com.microsoft:isec

Default Domain Set	***Entity***
iqn.1991-05.com.microsoft:isec	isec

Trusted Domain	***Entity***
iqn.1991-05.com.microsoft:win2003	win2003 isec
iqn.1991-05.com.aum:iscsi	iscsi

iSNS Domain Hopping

Before …

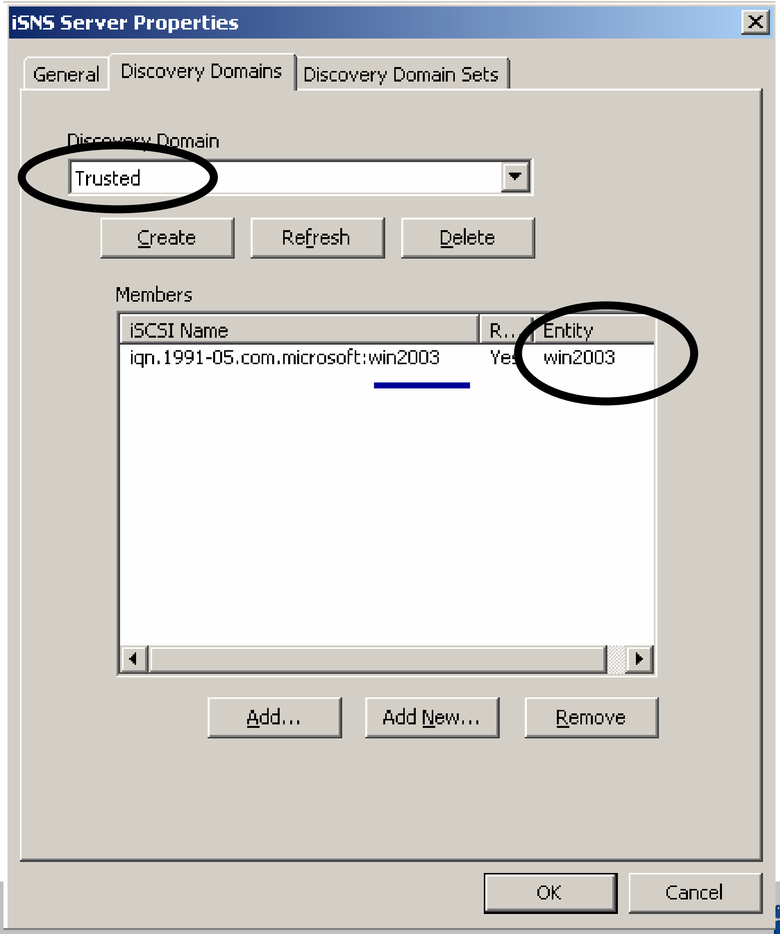


Discovery Domain: Default DD

Members

iSCSI Name	Entity
iqn.1991-05.com.microsoft:isec	isec

After…



Discovery Domain: Trusted

Members

iSCSI Name	R...	Entity
iqn.1991-05.com.microsoft:win2003	Yes	win2003

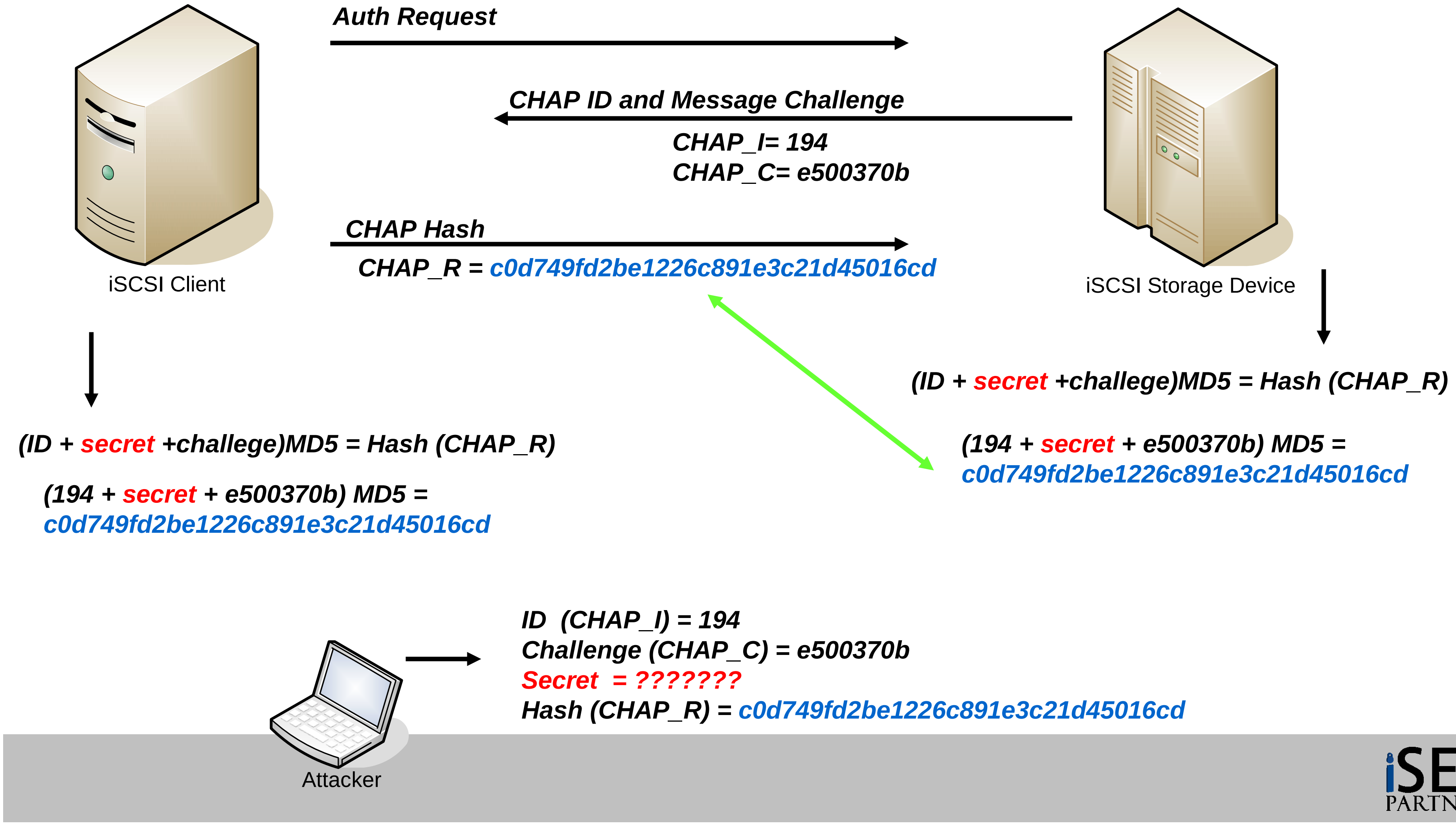
iSCSI Authentication

iSCSI Authentication

- **iSCSI Security**
  - Authentication: *Optional* Security
    - Optional iSCSI Security component
      - Authentication (CHAP)
      - Vulnerable to several attack types:
        - » Sniffing of usernames
        - » Off-line brute force attack of secret (password)
        - » Message reflection attack

iSCSI Authentication

- **iSCSI Attack Demo**



CHAP_I= 194
CHAP_C= e500370b

CHAP_R = c0d749fd2be1226c891e3c21d45016cd

(ID + secret +challege)MD5 = Hash (CHAP_R)

(194 + secret + e500370b) MD5 =
c0d749fd2be1226c891e3c21d45016cd

(ID + secret +challege)MD5 = Hash (CHAP_R)

(194 + secret + e500370b) MD5 =
c0d749fd2be1226c891e3c21d45016cd

ID (CHAP_I) = 194
Challenge (CHAP_C) = e500370b
Secret = ???????
Hash (CHAP_R) = c0d749fd2be1226c891e3c21d45016cd

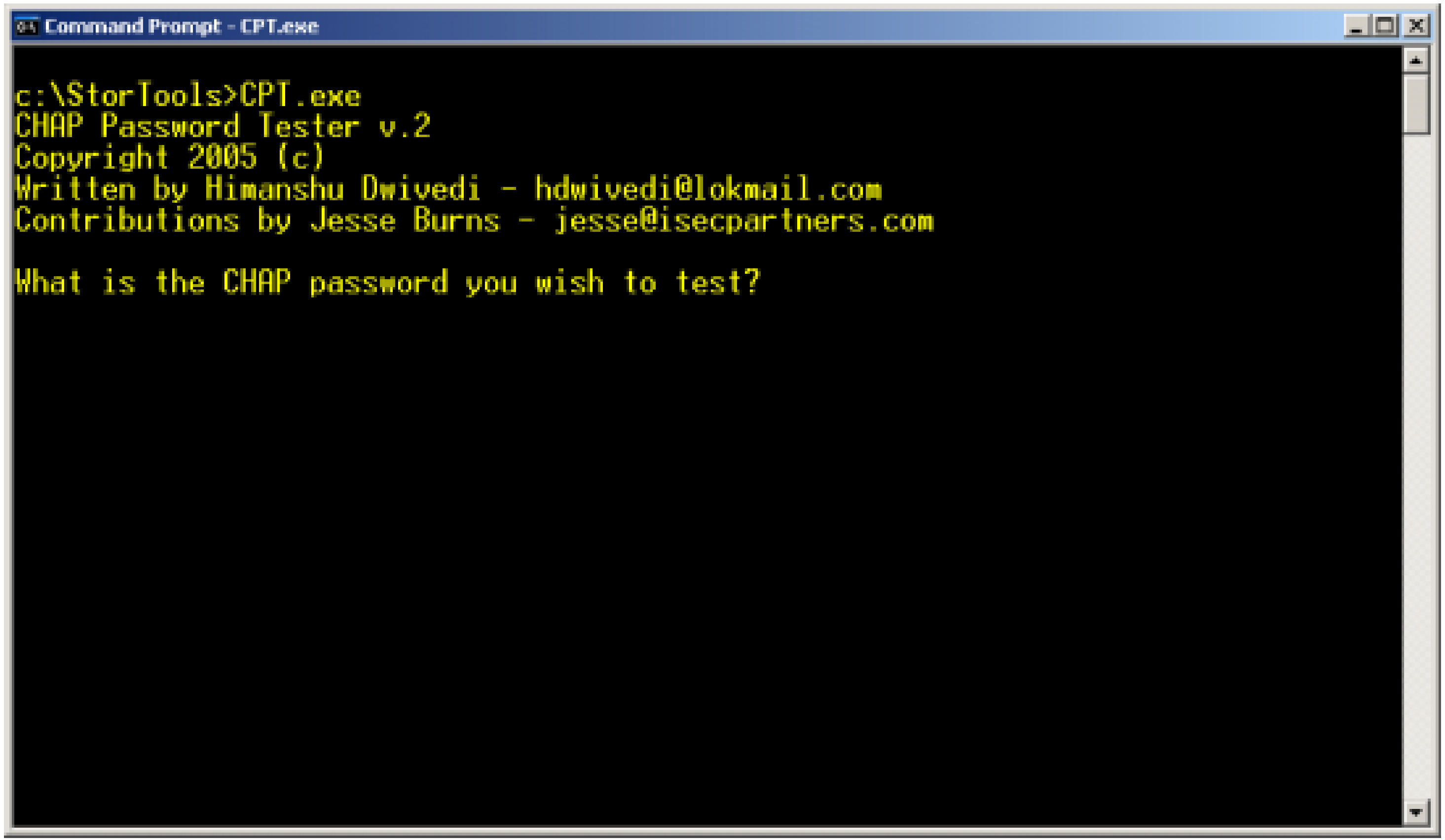
iSCSI Authentication

- **iSCSI Authentication Attack**
  - ***CHAP: (ID + secret +challege)MD5 = Hash (CHAP_R)***
    - ***Sample: (1 + x + 5)/2 = 5***
    - ***Sample: (1 + 1 + 5)/2 != 5***
    - ***Sample: (1 + 2 + 5)/2 != 5***
    - ***Sample: (1 + 3 + 5)/2 != 5***
    - ***Sample: (1 + 4 + 5)/2 = 5***
  - Sniff iSCSI Communication
    - Sniff port 3260
    - Obtain
      - CHAP Username (CHAP_N)
      - CHAP ID (CHAP_I)
      - CHAP Message Challenge (CHAP_C)
      - Resulting Hash (CHAP_R)
  - Brute-force passwords (secret)
    - Off line dictionary attack of every English word
  - Compromise the secret (password)
    - After two hashes match, the password is compromised

iSCSI Authentication: Offline Dictionary Attack

iSCSI CHAP Password Tester …

(www.isecpartners.com/tools.html)



```
c:\StorTools>CPT.exe
CHAP Password Tester v.2
Copyright 2005 (c)
Written by Himanshu Dwivedi - hdwivedi@lokmail.com
Contributions by Jesse Burns - jesse@isecpartners.com

What is the CHAP password you wish to test?
```

iSCSI Authentication: Offline Dictionary Attack

Sniffed (Captured) Entities:

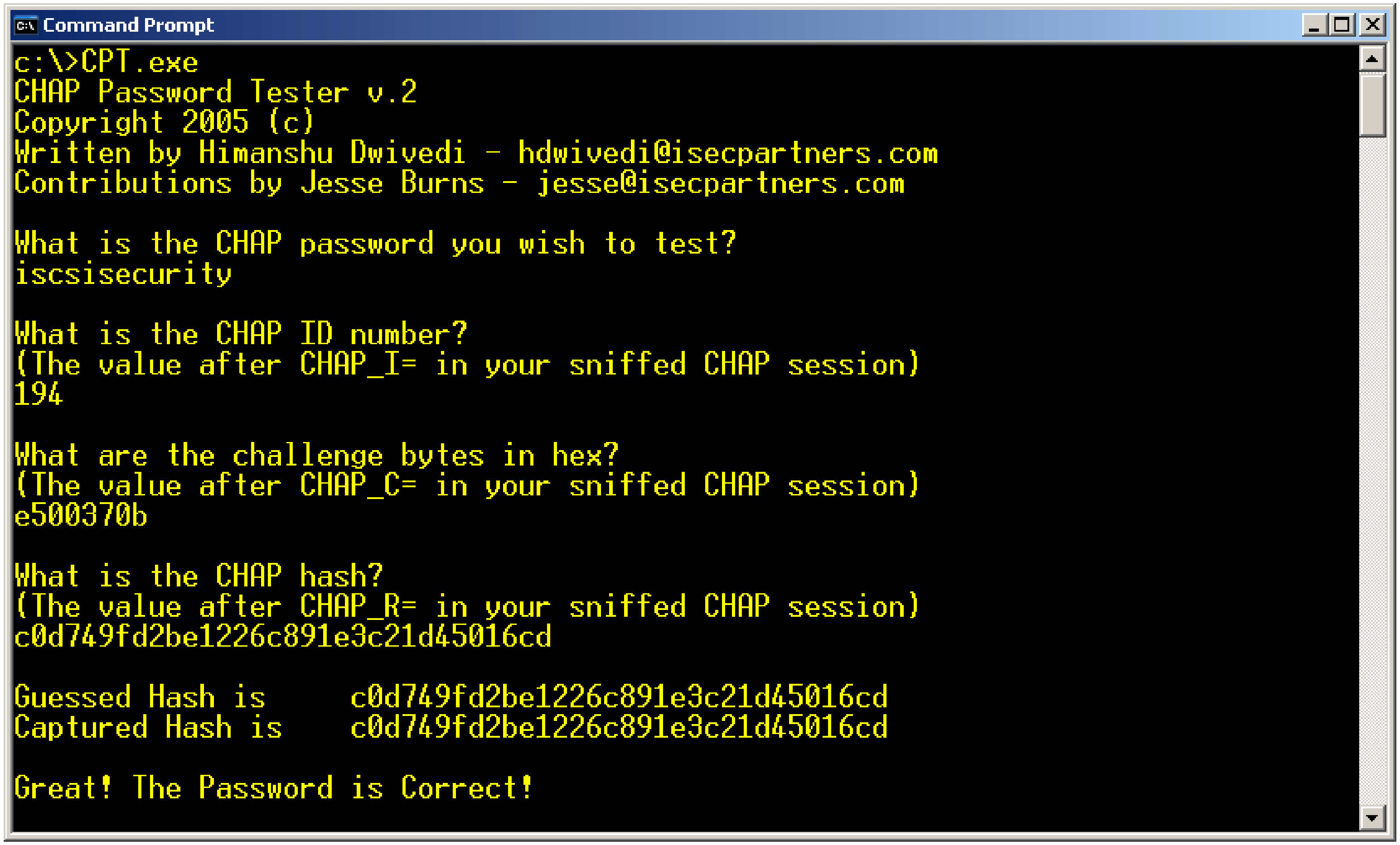
- **ID (CHAP_I): 194**
- **Message Challenge (CHAP_C): e500370b**
- **Secret: ??????**
- **Hash (CHAP_R): c0d749fd2be1226c891e3c21d45016cd**

(ID +	Dictionary Word +	Message Challenge) MD5 =	Hash
194	Hello	e500370b	81d0c90ad83d06bf0f51ce944f9c0341
194	My	e500370b	2db5f956905e85e6fd242a54d9213e9a
194	Name	e500370b	08dd57f2fcb535ae6c3d32716d54c97c
194	Is	e500370b	bc7329be2a9fa99fa596802b6a00424d
194	Kusum	e500370b	13ec91aeb5ea120e971a29ad0e2d0e86
194	And	e500370b	0708568450c40b67fc885e6685579cc4
194	My	e500370b	2db5f956905e85e6fd242a54d9213e9a
194	Voice	e500370b	28b255f4e1ecbe44e8c7827d039b523e
194	Is	e500370b	bc7329be2a9fa99fa596802b6a00424d
194	My	e500370b	2db5f956905e85e6fd242a54d9213e9a
194	Passport	e500370b	4983811b661e3d1dfda16a1c39f2b201
194	Verify	e500370b	629c2a938740d0332042b486db58b8dd
194	Me	e500370b	efb2712166bfafe7fcf6b3c0f0cf60d3
194	iscsisecurity	e500370b	c0d749fd2be1226c891e3c21d45016cd

Actual Secret: iscsisecurity

iSCSI Authentication: Offline Dictionary Attack

iSCSI CHAP Password Tester:



```
c:\>CPT.exe
CHAP Password Tester v.2
Copyright 2005 (c)
Written by Himanshu Dwivedi - hdwivedi@isecpartners.com
Contributions by Jesse Burns - jesse@isecpartners.com

What is the CHAP password you wish to test?
iscsisecurity

What is the CHAP ID number?
(The value after CHAP_I= in your sniffed CHAP session)
194

What are the challenge bytes in hex?
(The value after CHAP_C= in your sniffed CHAP session)
e500370b

What is the CHAP hash?
(The value after CHAP_R= in your sniffed CHAP session)
c0d749fd2be1226c891e3c21d45016cd

Guessed Hash is     c0d749fd2be1226c891e3c21d45016cd
Captured Hash is    c0d749fd2be1226c891e3c21d45016cd

Great! The Password is Correct!
```

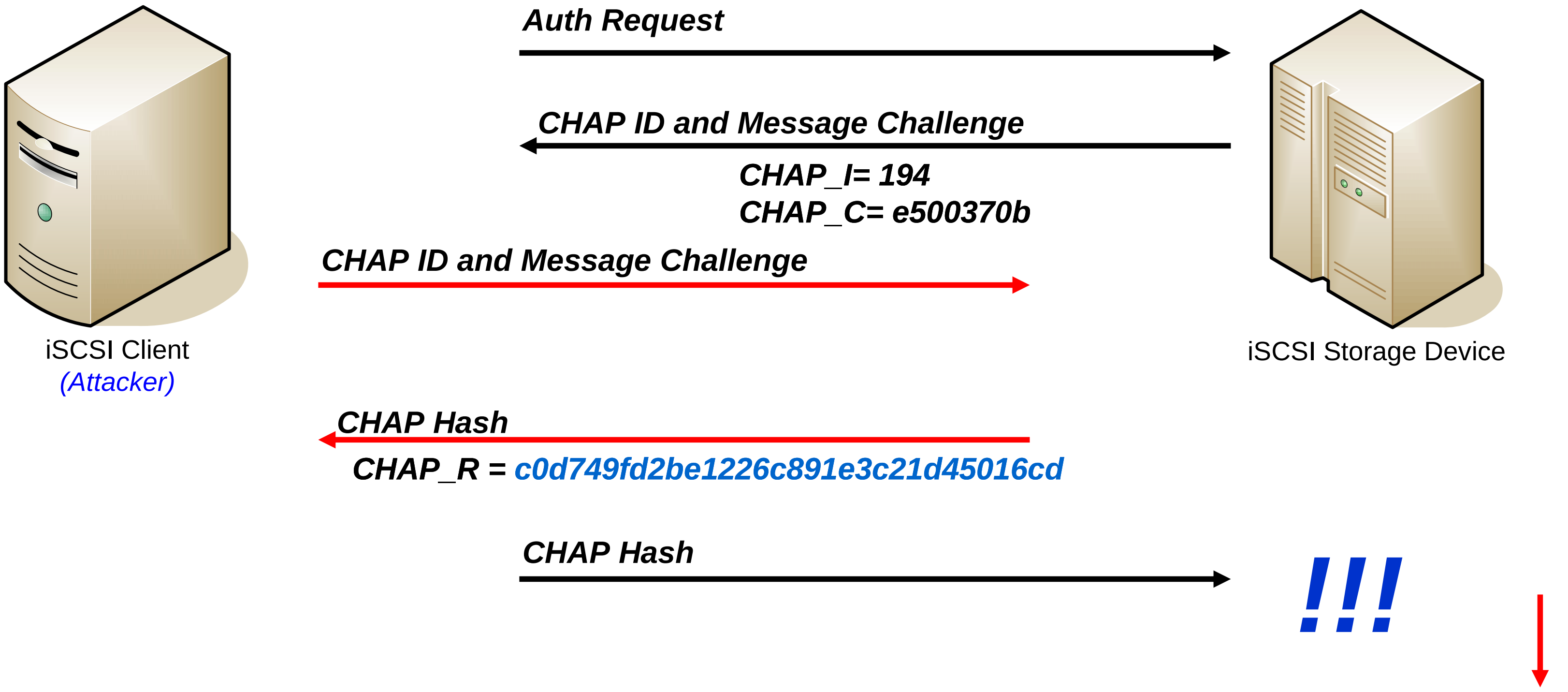
iSCSI Authentication

- **Message Reflection Attacks**
  - Reflection of a CHAP message challenge across multiple connections

- **Overview**
  - An attacker (iSCSI client) would request authentication to a iSCSI target
    - The client receives the CHAP ID and Challenge
  - Since the attacker does not know the secret (password), it cannot formulate the correct MD5 hash. However, the attacker can open a completely separate connection to the target (connection number 2) and force the Target to authenticate to it
    - The RFC states that any iSCSI target must response to authentication requests be default!
  - The Target receives the same ID and Challenge it just sent to the client (but in a different connection) and also knows the correct secret. The target will formulate the correct MD5 hash and pass it back, as if it were trying to authenticate to the client
  - This essentially gives the attacker (the client) the correct MD5 hash to authenticate in the iSCSI Target in the first connection!

iSCSI Authentication

- **Message Reflection**



Auth Request

CHAP ID and Message Challenge

CHAP_I= 194
CHAP_C= e500370b

CHAP ID and Message Challenge

iSCSI Client
(Attacker)

iSCSI Storage Device

CHAP Hash

CHAP_R = c0d749fd2be1226c891e3c21d45016cd

CHAP Hash

!!!

(ID + secret +challege)MD5 = Hash (CHAP_R)

(194 + secret + e500370b) MD5 =
c0d749fd2be1226c891e3c21d45016cd

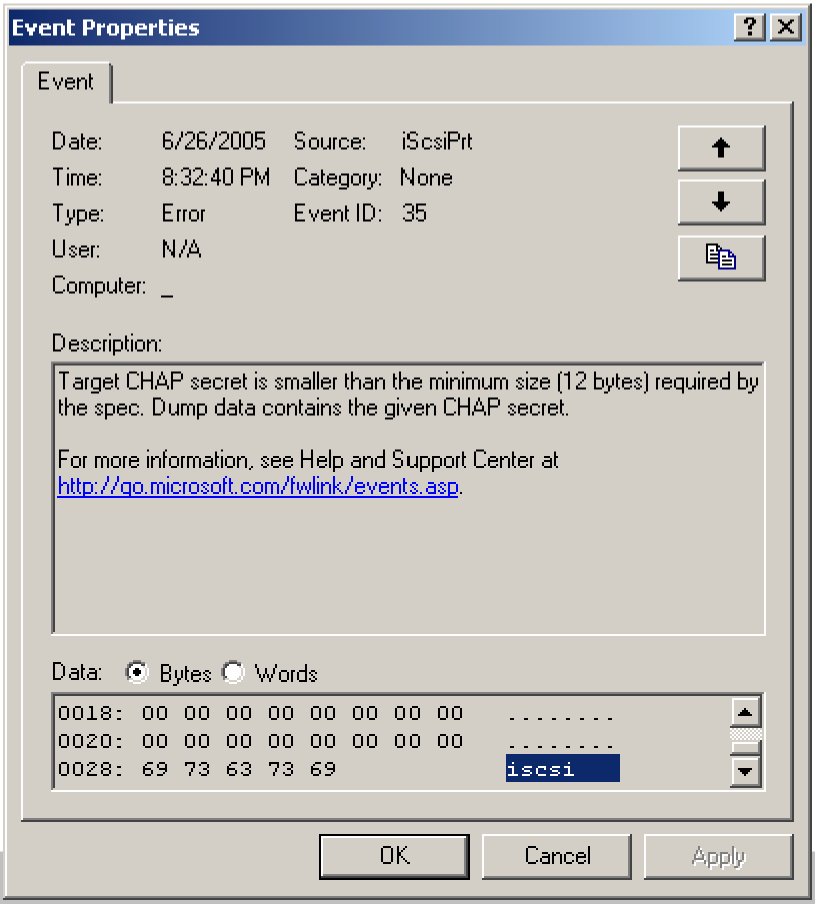
Connection 1 ↔

Connection 2 ↔

iSCSI Petty Problems

iSCSI Petty Problems

- **Microsoft iSCSI Client**
  - Driver logs iSCSI secrets (passwords) that don’t conform to the correct size in the clear in the Event Viewer



Date: 6/26/2005 Source: iScsiPrt
Time: 8:32:40 PM Category: None
Type: Error Event ID: 35
User: N/A
Computer: _

Description:

Target CHAP secret is smaller than the minimum size (12 bytes) required by the spec. Dump data contains the given CHAP secret.

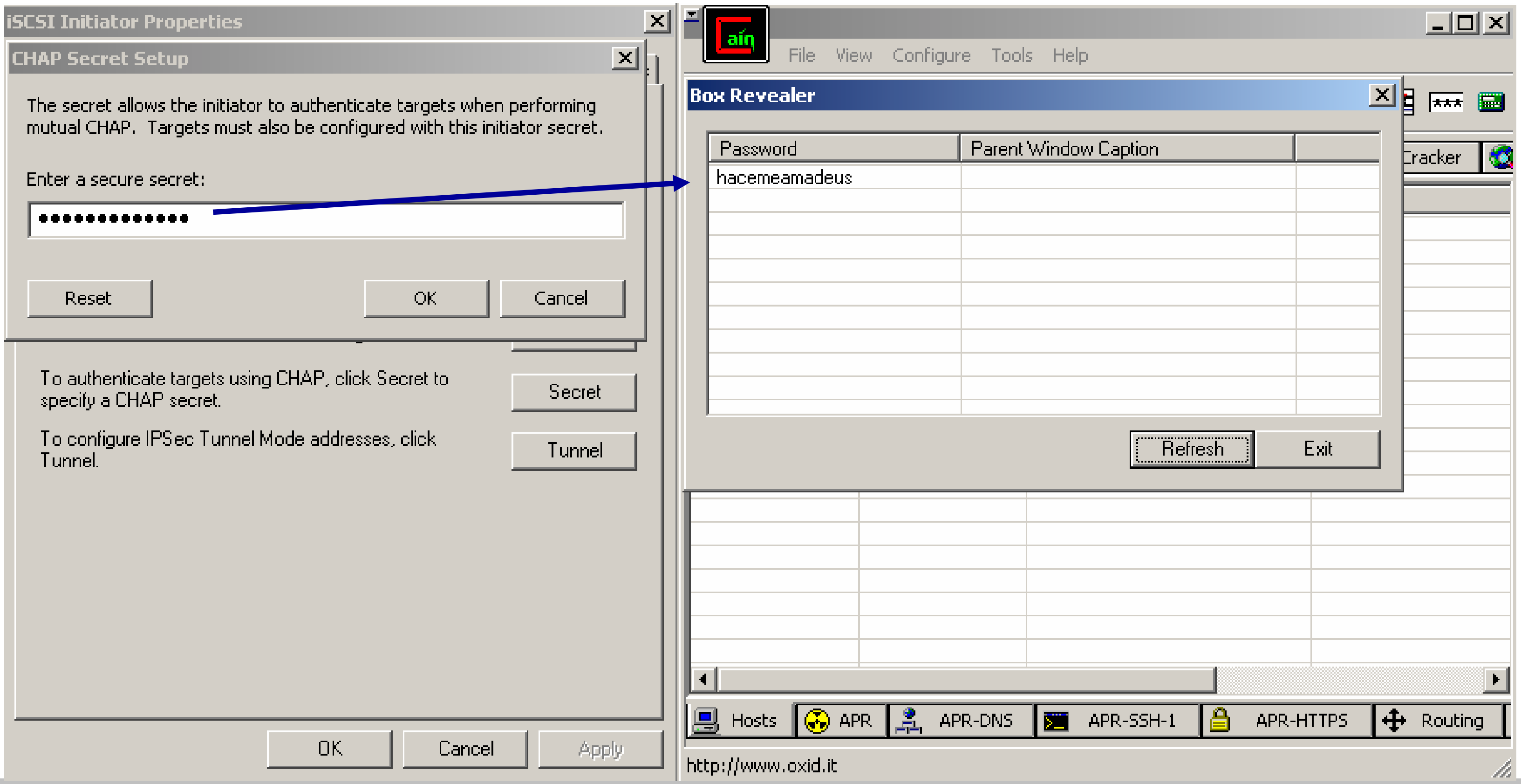
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0018: 00 00 00 00 00 00 00 00    ........
0020: 00 00 00 00 00 00 00 00    ........
0028: 69 73 63 73 69             iscsi
```

iSCSI Petty Problems

- **Microsoft iSCSI Client**
  - The client’s CHAP secret is protected with ‘darkened circles’ but can be revealed with a box revealer



The secret allows the initiator to authenticate targets when performing mutual CHAP. Targets must also be configured with this initiator secret.

Enter a secure secret: ●●●●●●●●●●●●●

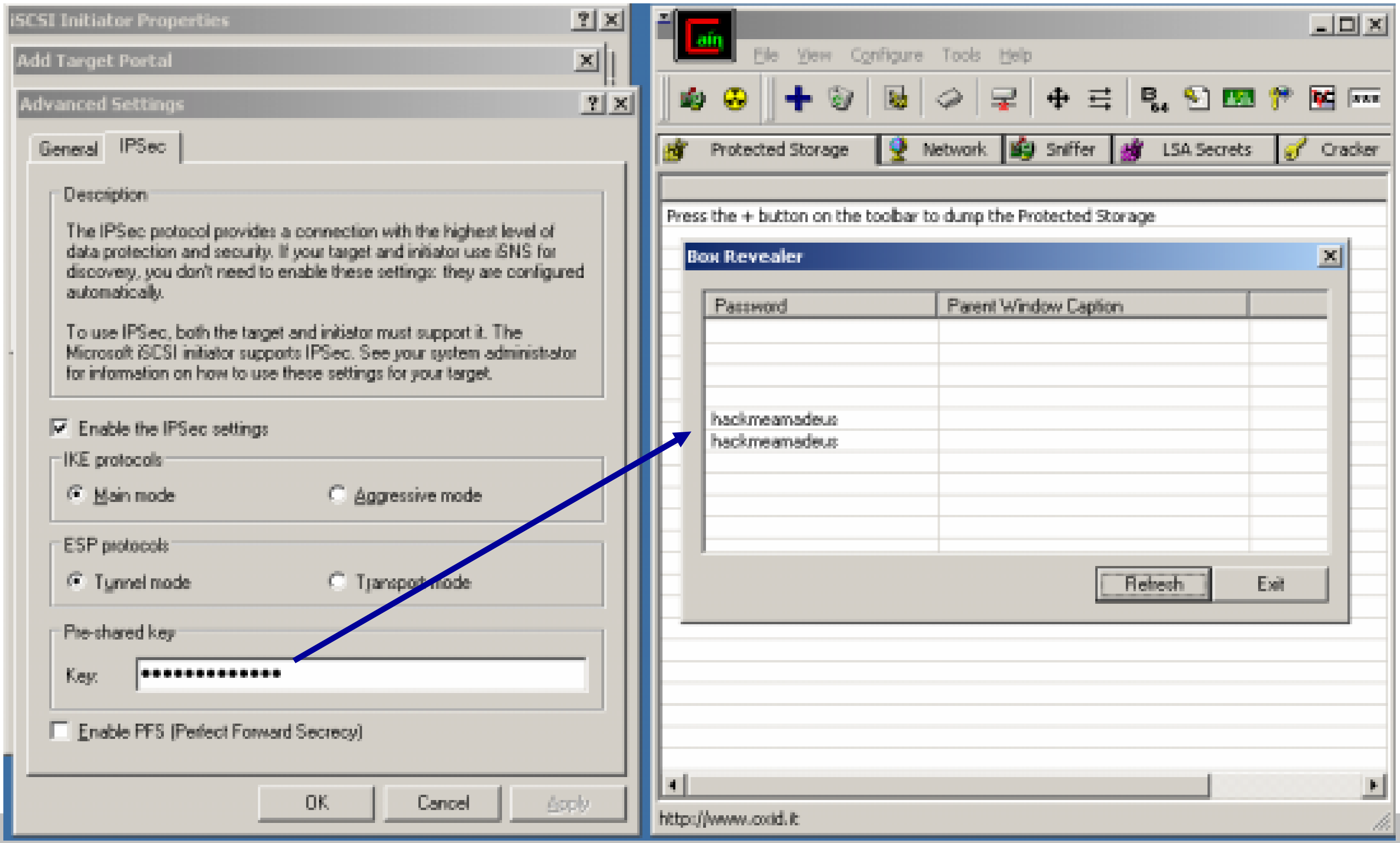
To authenticate targets using CHAP, click Secret to specify a CHAP secret.

To configure IPSec Tunnel Mode addresses, click Tunnel.

Password	Parent Window Caption
hacemeamadeus	

iSCSI Petty Problems

- **Microsoft iSCSI Client**
  - The client’s IPSec key is protected with ‘darkened circles’ but can be revealed with a box revealer



iSCSI Initiator Properties

Add Target Portal

Advanced Settings

Description

The IPSec protocol provides a connection with the highest level of data protection and security. If your target and initiator use iSNS for discovery, you don't need to enable these settings: they are configured automatically.

To use IPSec, both the target and initiator must support it. The Microsoft iSCSI initiator supports IPSec. See your system administrator for information on how to use these settings for your target.

☑ Enable the IPSec settings

IKE protocols

● Main mode ○ Aggressive mode

ESP protocols

● Tunnel mode ○ Transport mode

Pre-shared key

Key: ••••••••••••••

□ Enable PFS (Perfect Forward Secrecy)

Press the + button on the toolbar to dump the Protected Storage

Box Revealer

Password	Parent Window Caption
hackmeamadeus	
hackmeamadeus	

http://www.oxid.it

iSCSI Defenses

iSCSI Defenses

- **How to defend against these threats?**
  - CONFIGURATION, CONFIGURATION, CONFIGURATION
  - Every iSCSI device should be secured just like an other operating system or application

- **Pay no attention to the man behind the curtain!**
  - Audit your iSCSI storage devices/networks and assess the risk!

- **STORAGE need your security loving too!!!**
  - iSCSI storage devices, which hold your DATA, are similar to everything else on the network….
    - Vulnerable to attacks
    - Security holes and weaknesses
    - **Need to be protected and secured**

iSCSI Defenses

Top 10 iSCSI Security Recommendations

- **Specific configurations**
  1. Enable Mutual Authentication
     - Do not rely solely CHAP Auth
  2. Create Multiple Discover Domains
     - Only use the Default Domain Sets for random registrations
  3. Enable CRC checksums for integrity checking
  4. Require iSNS IPSec (where possible)
  5. Do not only rely on iQNs for security authorization values
  6. Enable iSCSI IPSec (where possible)
- **Vendors!**
  7. Incorporate Kerberos
  8. Enable authentication by default
  9. Support iSNS authenticated heartbeats before registrations
  10. Support iSNS security features in the RFC

Questions

Himanshu Dwivedi

- hdwivedi@isecpartners.com or hdwivedi@lokmail.com

Security Books Authored by presenter:

- **Securing Storage**
  - *Publish date: Fall 2005*