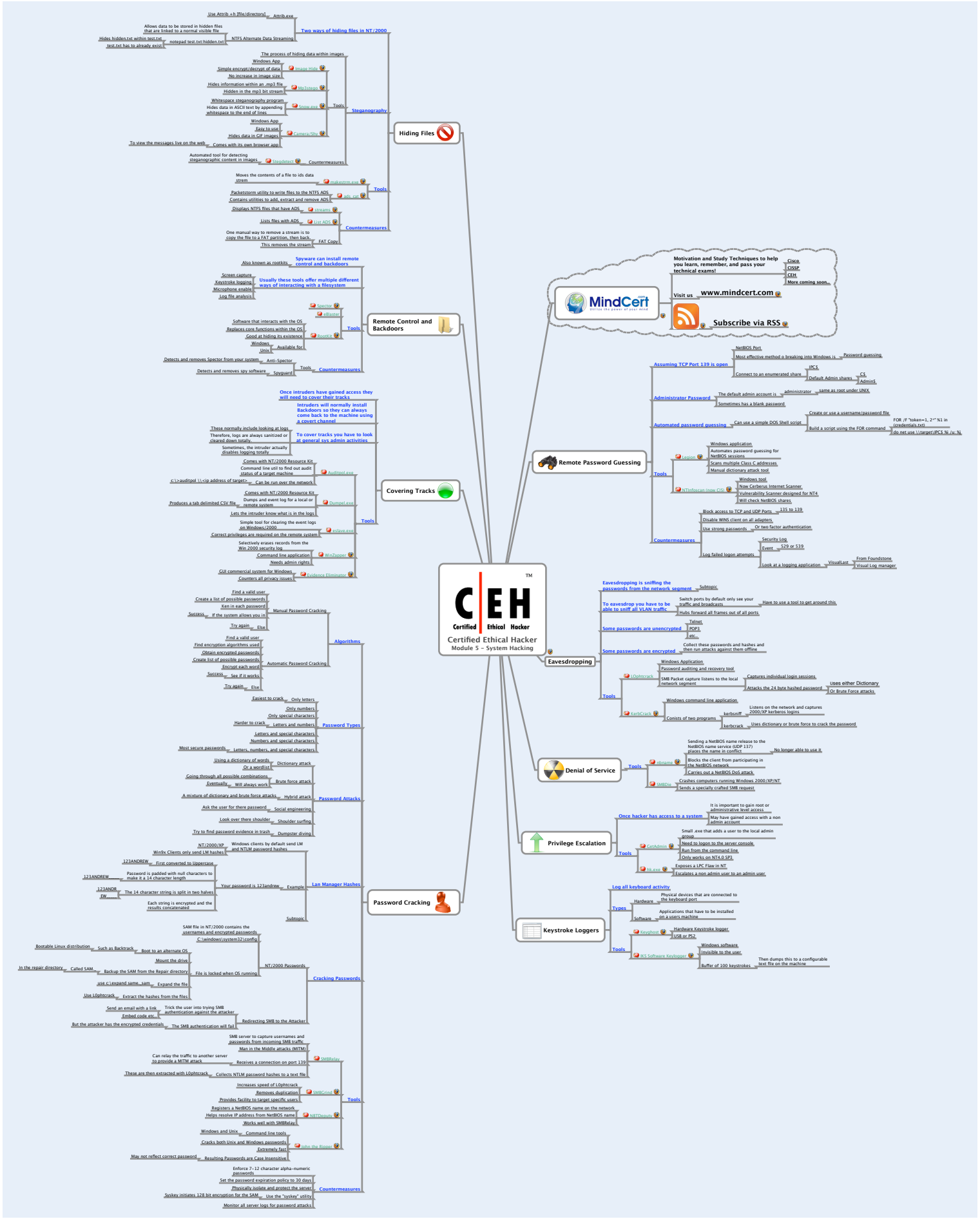
Certified Ethical Hacker
Module 5 - System Hacking
Hiding Files
Two ways of hiding files in NT/2000
Use Attrib +h [file/directory] Attrib.exe
Allows data to be stored in hidden files that are linked to a normal visible file
Hides hidden.txt within test.txt
test.txt has to already exist
NTFS Alternate Data Streaming
notepad test.txt:hidden.txt
Steganography
The process of hiding data within images
Tools
Windows App
Image Hide
Simple encrypt/decrypt of data
No increase in image size
Hides information within an .mp3 file
Mp3stego
Hidden in the mp3 bit stream
Whitespace steganography program
Hides data in ASCII text by appending whitespace to the end of lines
snow.exe
Windows App
Easy to use
Camera/Shy
Hides data in GIF images
To view the messages live on the web
Comes with its own browser app
Countermeasures
Automated tool for detecting steganographic content in images
Stegdetect
Tools
Moves the contents of a file to ids data strem
makestrm.exe
Packetstorm utility to write files to the NTFS ADS
ads_cat
Contains utilities to add, extract and remove ADS
Countermeasures
Displays NTFS files that have ADS
streams
Lists files with ADS
List ADS
One manual way to remove a stream is to copy the file to a FAT partition, then back.
This removes the stream
FAT Copy
Remote Control and Backdoors
Spyware can install remote control and backdoors
Also known as rootkits
Usually these tools offer multiple different ways of interacting with a filesystem
Screen capture
Keystroke logging
Microphone enable
Log file analysis
Tools
Spector
eBlaster
Software that interacts with the OS
Replaces core functions within the OS
Good at hiding its existence
RootKit
Windows
Unix
Available for
Countermeasures
Detects and removes Spector from your system
Anti-Spector
Tools
Detects and removes spy software
Spyguard
Covering Tracks
Once intruders have gained access they will need to cover their tracks
Intruders will normally install Backdoors so they can always come back to the machine using a covert channel
To cover tracks you have to look at general sys admin activities
These normally include looking at logs
Therefore, logs are always sanitized or cleared down totally
Sometimes, the intruder actually disables logging totally
Tools
Comes with NT/2000 Resource Kit
AuditPol.exe
Command line util to find out audit status of a target machine
c:\>auditpol \\<ip address of target>
Can be run over the network
Comes with NT/2000 Resource Kit
Dumpel.exe
Dumps and event log for a local or remote system
Produces a tab delimited CSV file
Lets the intruder know what is in the logs
elsave.exe
Simple tool for clearing the event logs on Windows/2000
Correct privileges are required on the remote system
WinZapper
Selectively erases records from the Win 2000 security log
Command line application
Needs admin rights
Evidence Eliminator
GUI commercial system for Windows
Counters all privacy issues
Password Cracking
Algorithms
Manual Password Cracking
Find a valid user
Create a list of possible passwords
Key in each password
Success
If the system allows you in
Try again
Else
Automatic Password Cracking
Find a valid user
Find encryption algorithms used
Obtain encrypted passwords
Create list of possible passwords
Encrypt each word
Success
See if it works
Try again
Else
Password Types
Easiest to crack
Only letters
Only numbers
Only special characters
Harder to crack
Letters and numbers
Letters and special characters
Numbers and special characters
Most secure passwords
Letters, numbers, and special characters
Password Attacks
Dictionary attack
Using a dictionary of words
Or a wordlist
Brute force attack
Going through all possible combinations
Eventually
Will always work
Hybrid attack
A mixture of dictionary and brute force attacks
Social engineering
Ask the user for there password
Shoulder surfing
Look over there shoulder
Dumpster diving
Try to find password evidence in trash
Lan Manager Hashes
NT/2000/XP
Windows clients by default send LM and NTLM password hashes
Win9x Clients only send LM hashes
Example
123ANDREW
First converted to Uppercase
123ANDREW
Password is padded with null characters to make it a 14 character length
Your password is 123andrew
123ANDR
EW
The 14 character string is split in two halves
Each string is encrypted and the results concatenated
Subtopic
Cracking Passwords
NT/2000 Passwords
SAM file in NT/2000 contains the usernames and encrypted passwords
C:\windows\system32\config
File is locked when OS running
Such as Backtrack
Bootable Linux distribution
Boot to an alternate OS
Mount the drive
Backup the SAM from the Repair directory
In the repair directory
Called SAM
Expand the file
use c:\expand same..sam
Extract the hashes from the files
Use L0phtcrack
Redirecting SMB to the Attacker
Trick the user into trying SMB authentication against the attacker
Send an email with a link
Embed code etc..
The SMB authentication will fail
But the attacker has the encrypted credentials
Tools
Man in the Middle attacks (MITM)
SMB server to capture usernames and passwords from incoming SMB traffic
SMBRelay
Receives a connection on port 139
Can relay the traffic to another server to provide a MITM attack
Collects NTLM password hashes to a text file
These are then extracted with L0phtcrack
SMBGrind
Increases speed of L0phtcrack
Removes duplication
Provides facility to target specific users
NBTDetect
Registers a NetBIOS name on the network
Helps resolve IP address from NetBIOS name
Works well with SMBRelay
John the Ripper
Windows and Unix
Command line tools
Cracks both Unix and Windows passwords
Extremely fast
Resulting Passwords are Case Insensitive
May not reflect correct password
Countermeasures
Enforce 7–12 character alpha-numeric passwords
Set the password expiration policy to 30 days
Physically isolate and protect the server
Syskey initiates 128 bit encryption for the SAM
Use the "syskey" utility
Monitor all server logs for password attacks
Eavesdropping
Eavesdropping is sniffing the passwords from the network segment
Subtopic
To eavesdrop you have to be able to sniff all VLAN traffic
Switch ports by default only see your traffic and broadcasts
Have to use a tool to get around this
Hubs forward all frames out of all ports
Some passwords are unencrypted
Telnet
POP3
etc..
Some passwords are encrypted
Collect these passwords and hashes and then run attacks against them offline
Tools
LOphtcrack
Windows Application
Password auditing and recovery tool
KerbCrack
SMB Packet capture listens to the local network segment
Captures individual login sessions
Attacks the 24 byte hashed password
Uses either Dictionary
Or Brute Force attacks
Windows command line application
Consists of two programs
kerbsniff
Listens on the network and captures 2000/XP kerberos logins
kerbcrack
Uses dictionary or brute force to crack the password
Denial of Service
Tools
nbname
Sending a NetBIOS name release to the NetBIOS name service (UDP 137) places the name in conflict
No longer able to use it
Blocks the client from participating in the NetBIOS network
Carries out a NetBIOS DoS attack
SMBDie
Crashes computers running Windows 2000 /XP/NT
Sends a specially crafted SMB request
Privilege Escalation
Once hacker has access to a system
It is important to gain root or administrative level access
May have gained access with a non admin account
Tools
GetAdmin
Small .exe that adds a user to the local admin group
Need to logon to the server console
Run from the command line
Only works on NT4.0 SP3
hk.exe
Exposes a LPC Flaw in NT
Escalates a non admin user to an admin user.
Keystroke Loggers
Log all keyboard activity
Types
Hardware
Physical devices that are connected to the keyboard port
Software
Applications that have to be installed on a users machine
Tools
Keyghost
Hardware Keystroke logger
USB or PS2.
PC Software Keylogger
Windows software
Invisible to the user
Buffer of 100 keystrokes
Then dumps this to a configurable text file on the machine
Remote Password Guessing
Assuming TCP Port 139 is open
NetBIOS Port
Most effective method o breaking into Windows is
Password guessing
Connect to an enumerated share
IPC$
Default Admin shares
C$
Admin$
Administrator Password
The default admin account is
administrator
same as root under UNIX
Sometimes has a blank password
Automated password guessing
Can use a simple DOS Shell script
Create or use a username/password file
Build a script using the FOR command
FOR /F "token=1, 2*" %1 in (credentials.txt) do net use \\target\IPC$ %2 /u: %1
Tools
Legion
Windows application
Automates password guessing for NetBIOS sessions
Scans multiple Class C addresses
Manual dictionary attack tool
NTInfoScan.(now CIS)
Windows tool
Now Cerberus Internet Scanner
Vulnerability Scanner designed for NT4
Will check NetBIOS shares
Countermeasures
Block access to TCP and UDP Ports
135 to 139
Disable WINS client on all adapters
Use strong passwords
Or two factor authentication
Log failed logon attempts
Security Log
Event
529 or 539
Look at a logging application
VisualLast
From Foundstone
Visual Log manager
MindCert
Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
Cisco
CISSP
CEH
More coming soon..
Visit us
www.mindcert.com
Subscribe via RSS