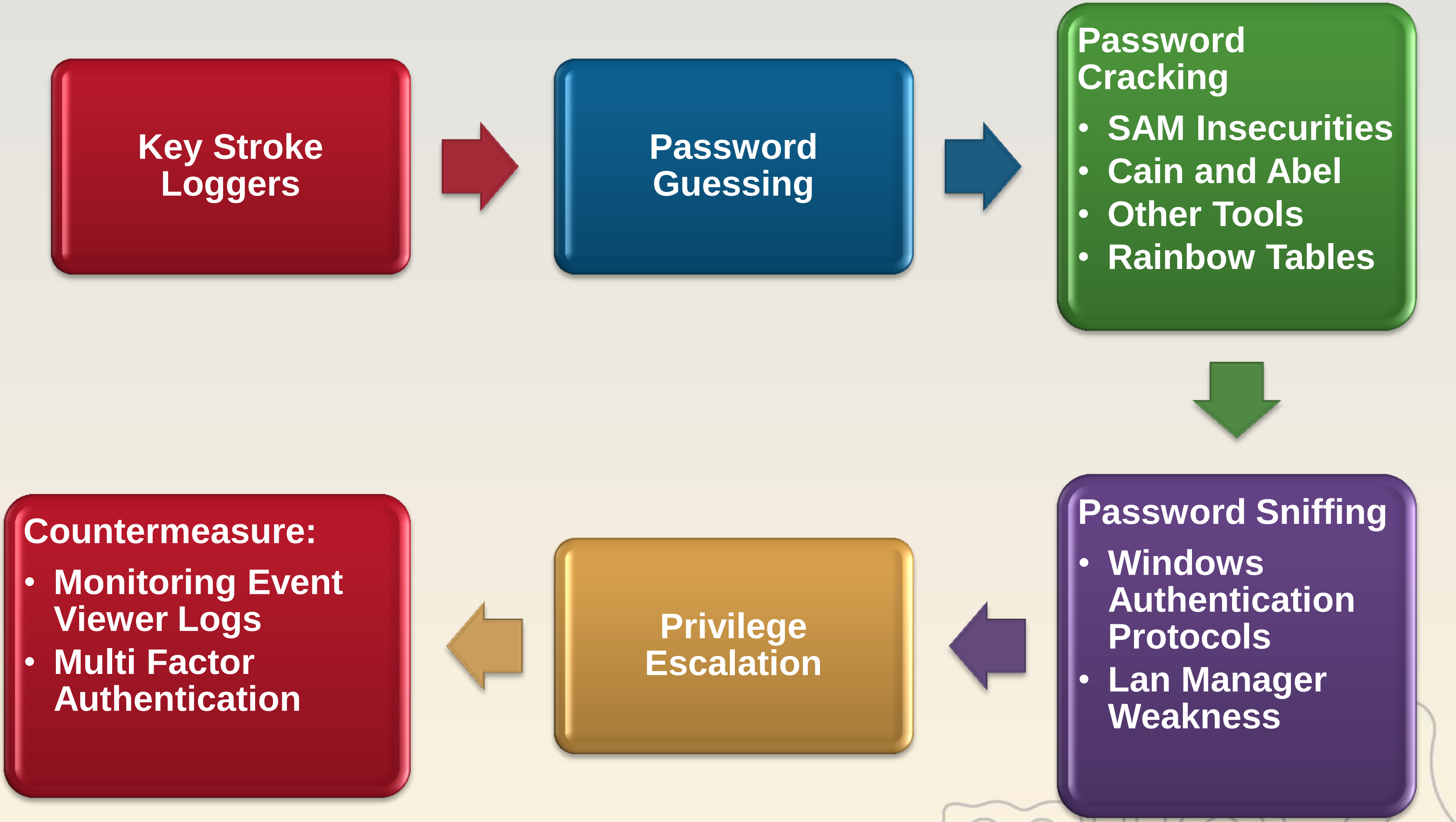
Windows Hacking

Overview



Key Stroke Loggers

Password Guessing

Password Cracking

- SAM Insecurities
- Cain and Abel
- Other Tools
- Rainbow Tables

Password Sniffing

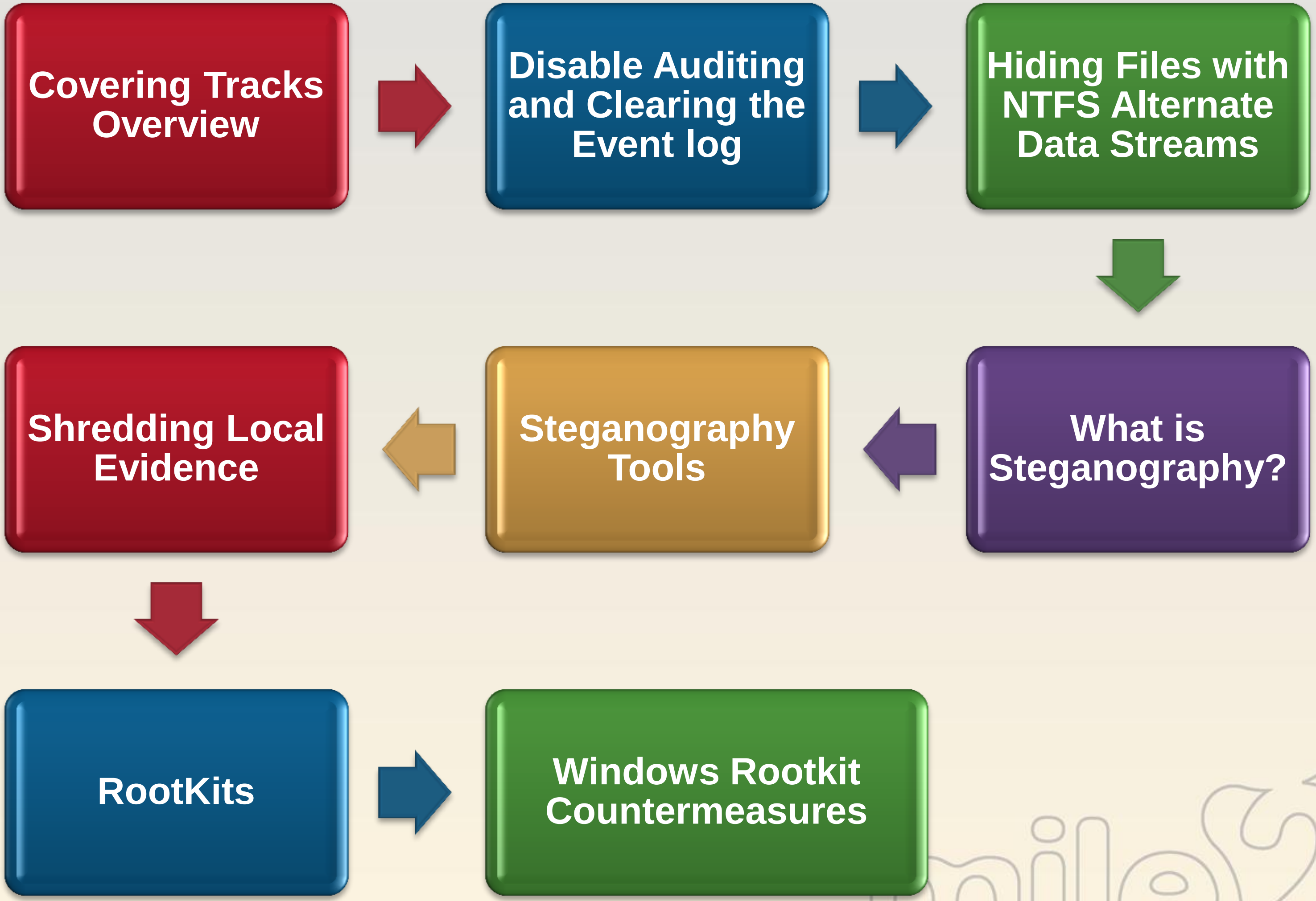
- Windows Authentication Protocols
- Lan Manager Weakness

Privilege Escalation

Countermeasure:

- Monitoring Event Viewer Logs
- Multi Factor Authentication

Overview



Covering Tracks Overview

Disable Auditing and Clearing the Event log

Hiding Files with NTFS Alternate Data Streams

What is Steganography?

Steganography Tools

Shredding Local Evidence

RootKits

Windows Rootkit Countermeasures

Types of Password Attacks

Social attacks

- Social engineering
- Shoulder surfing
- Dumpster diving

Digital attacks

- Keystroke loggers
- Password cracking
- Dictionary/Brute force attacks
- Rainbow Tables

Keystroke Loggers

Keystroke loggers are one way of obtaining usernames and passwords, as well as other information.

Keyloggers can be software based (see chart below) or hardware based. (www.keyghost.com)

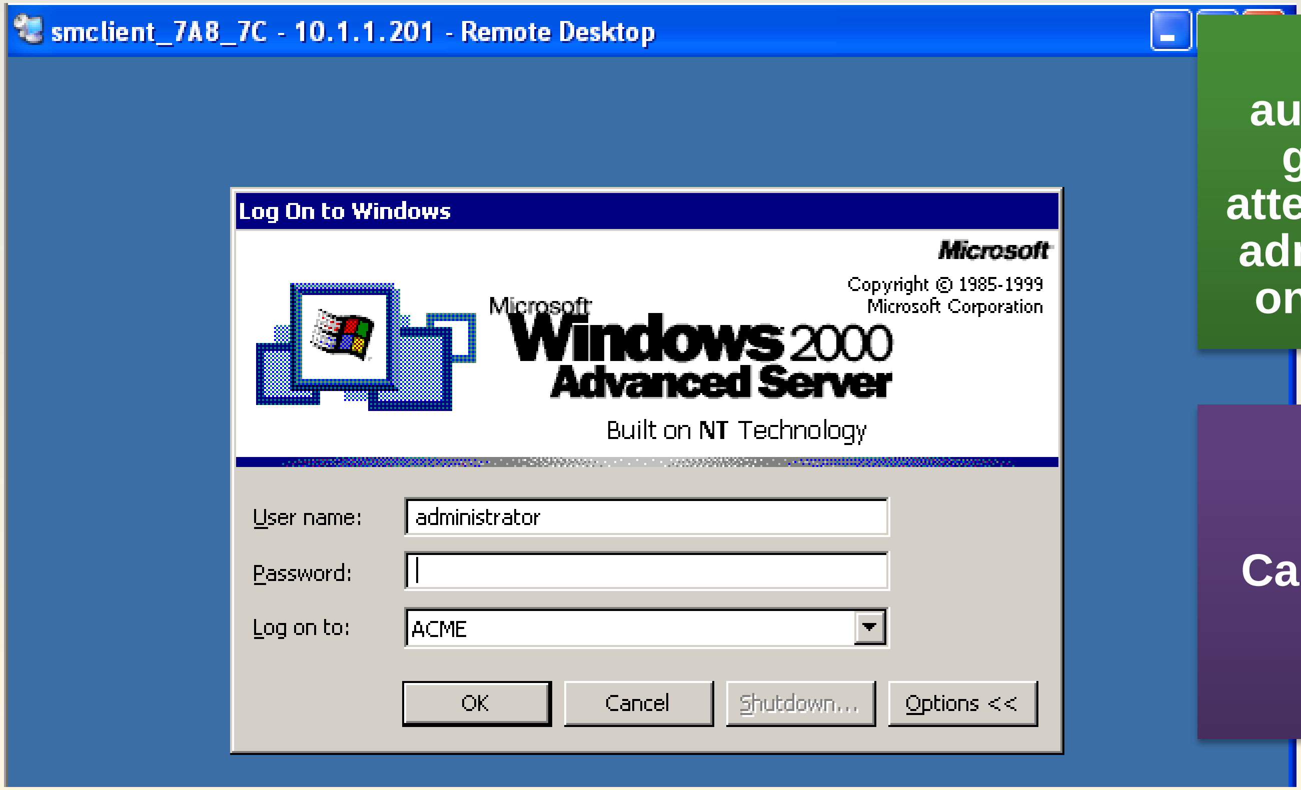
Software-based keyloggers

iSpyNow	www.exploreanywhere.com
PC Activity Monitor Pro	www.keylogger.org
remoteSpy	www.ispynow.com
Spector	www.spectorsoft.com
KeyCaptor	www.keylogger-software.com

Password Guessing

Password guessing involves actually attempting to log onto the target.

Hackers can write a script or use an automated tool to enter credentials to various servers: FTP, telnet, terminal server, mapping a drive to c$


smclient_7A8_7C - 10.1.1.201 - Remote Desktop

Log On to Windows

User name: administrator

Password:

Log on to: ACME

Tsgrinder is an automated password guessing tool that attempts to login to the administrator account on Terminal Servers.

Do not forget Cain, Obiwan, Brutus, and THC-Hydra!

Password Cracking LM/NTLM Hashes

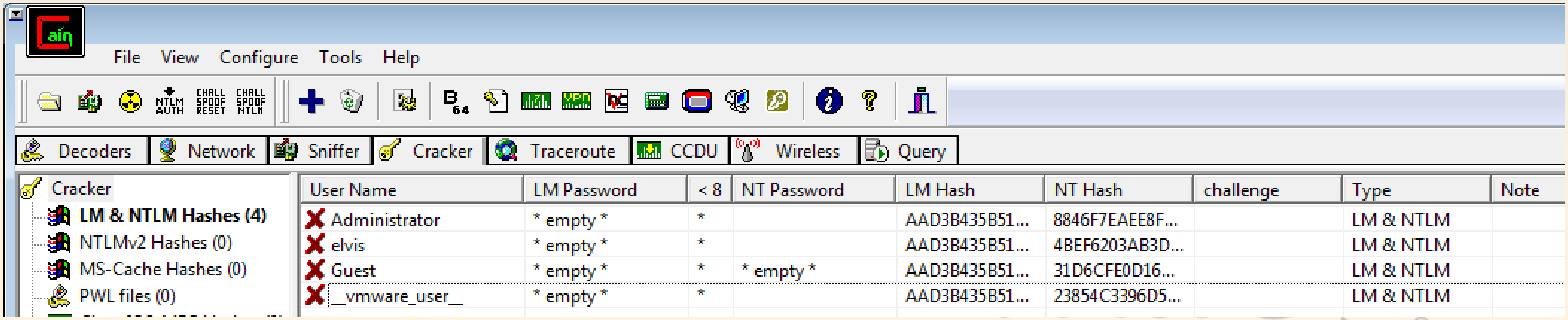
Password cracking involves obtaining the password hash and performing offline attacks against it.

Both the SAM database and the AD database store a user’s password in two formats (by default):

- LanMan hash: max length 14 characters, UPPERCASE only.
- NT hash: max length 127 characters, mixed case.

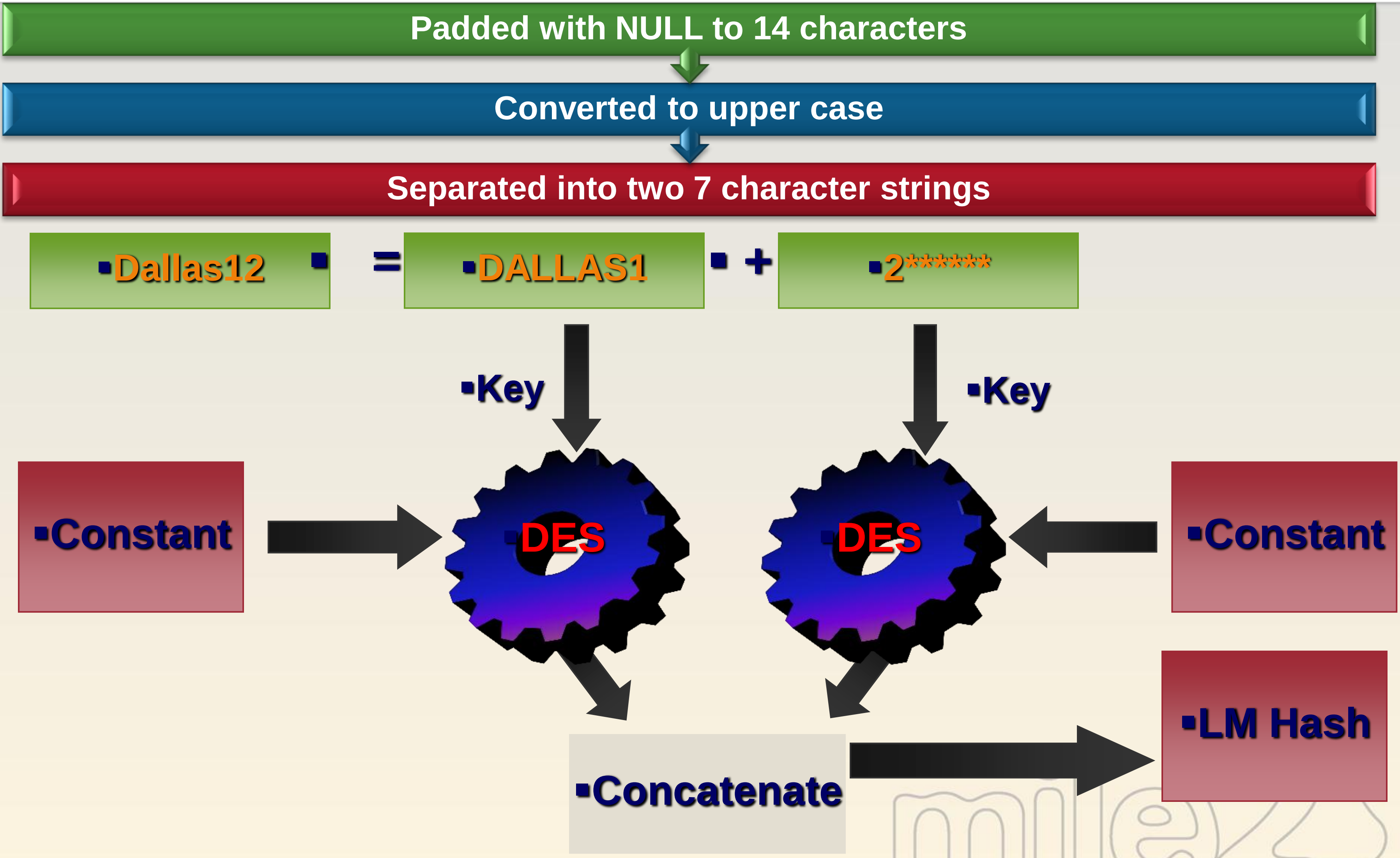
Before encrypting the password to create the LanMan hash, the 14 character string is split and each half is encrypted separately.

The LanMan version of the password is easier to crack.



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
✗ Administrator	* empty *	*		AAD3B435B51...	8846F7EAEE8F...		LM & NTLM	
✗ elvis	* empty *	*		AAD3B435B51...	4BEF6203AB3D...		LM & NTLM	
✗ Guest	* empty *	*	* empty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM	
✗ __vmware_user__	* empty *	*		AAD3B435B51...	23854C3396D5...		LM & NTLM	

LM Hash Encryption



Padded with NULL to 14 characters

Converted to upper case

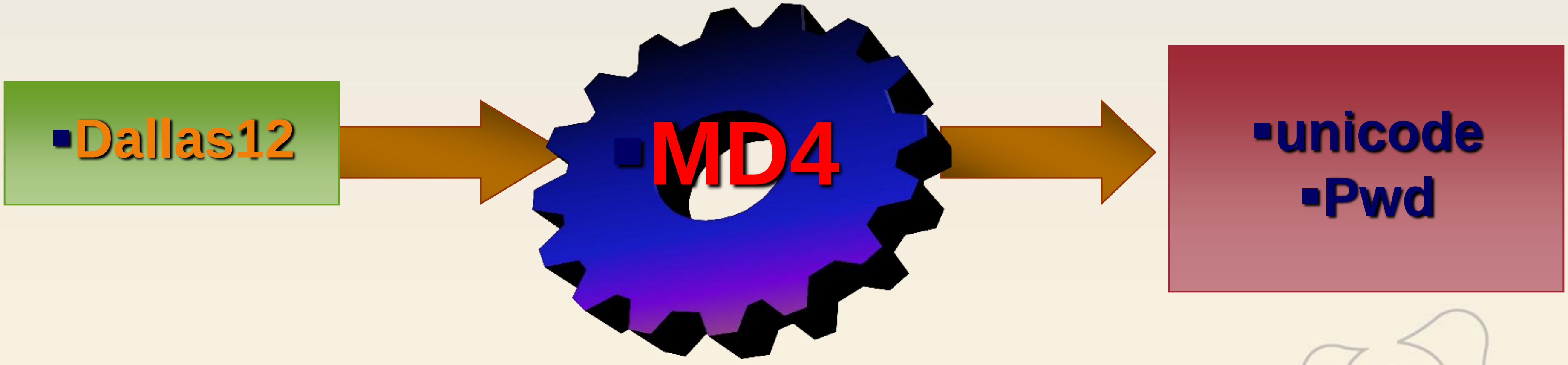
Separated into two 7 character strings

Dallas12 = DALLAS1 + 2******

NT Hash Generation

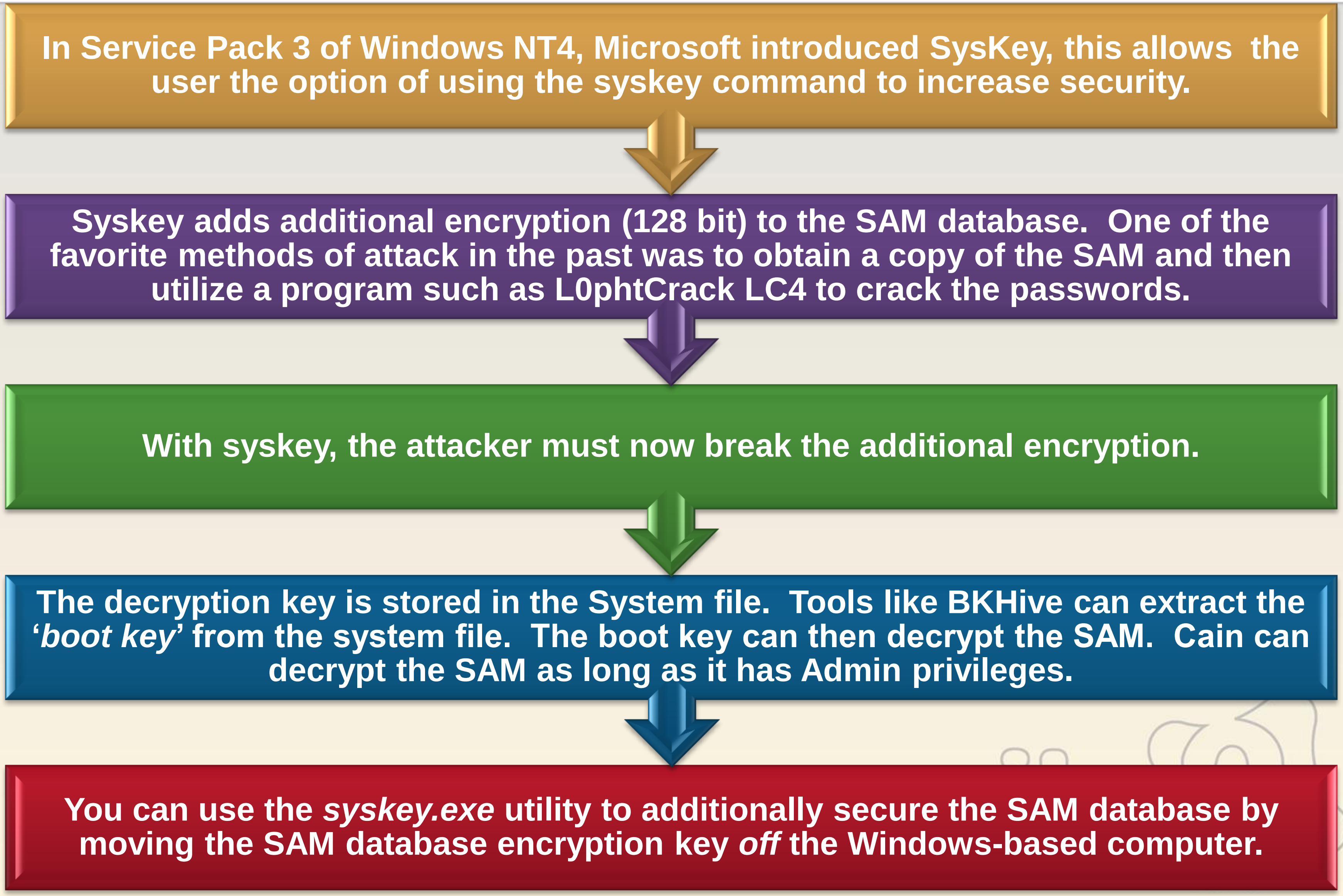
Hash the password

Store it



- Dallas12
- MD4
- unicode
- Pwd

Syskey Encryption



In Service Pack 3 of Windows NT4, Microsoft introduced SysKey, this allows the user the option of using the syskey command to increase security.

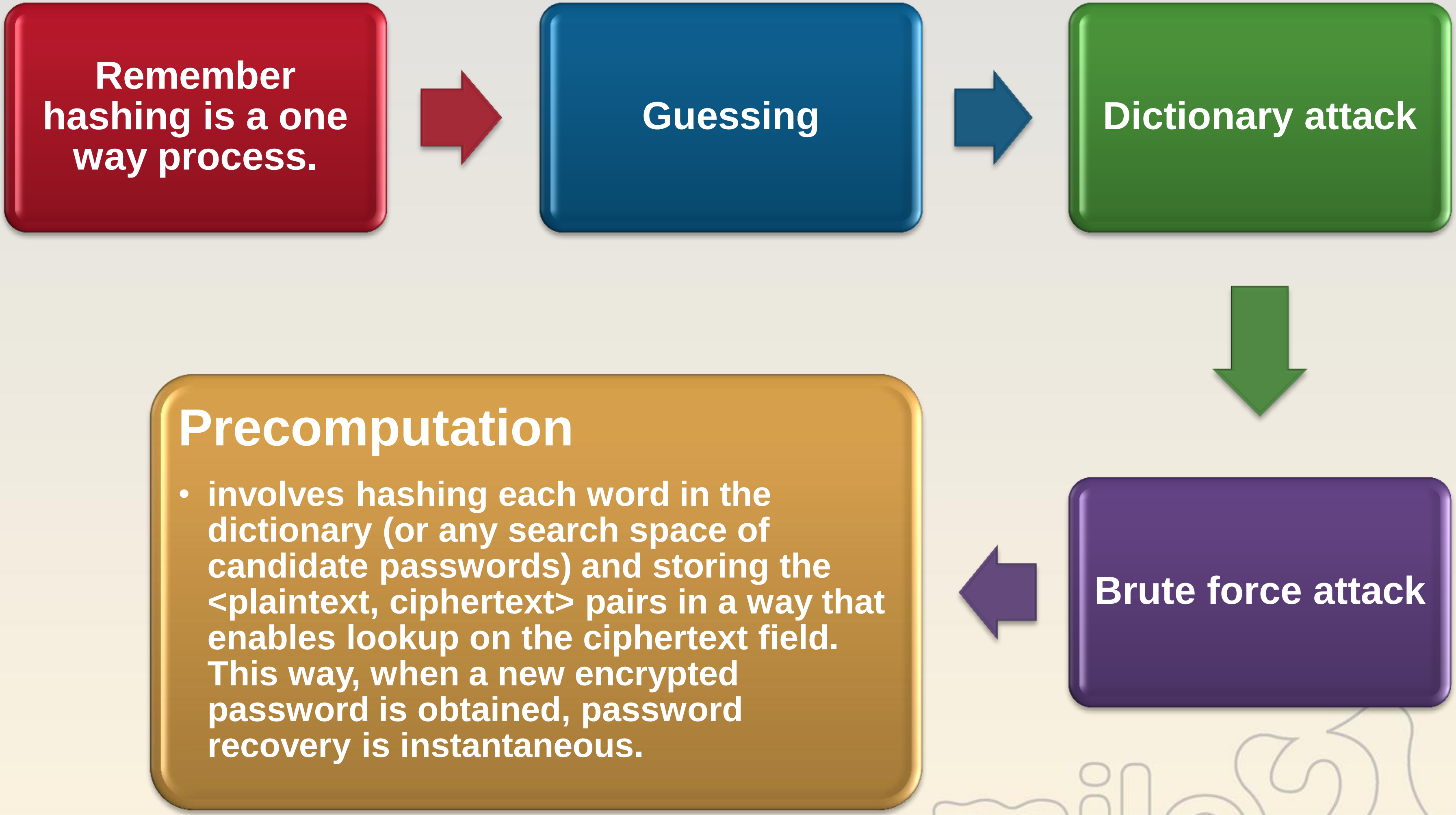
Syskey adds additional encryption (128 bit) to the SAM database. One of the favorite methods of attack in the past was to obtain a copy of the SAM and then utilize a program such as L0phtCrack LC4 to crack the passwords.

With syskey, the attacker must now break the additional encryption.

The decryption key is stored in the System file. Tools like BKHive can extract the ‘*boot key*’ from the system file. The boot key can then decrypt the SAM. Cain can decrypt the SAM as long as it has Admin privileges.

You can use the *syskey.exe* utility to additionally secure the SAM database by moving the SAM database encryption key *off* the Windows-based computer.

Cracking Techniques



Remember hashing is a one way process.

Guessing

Dictionary attack

Brute force attack

Precomputation

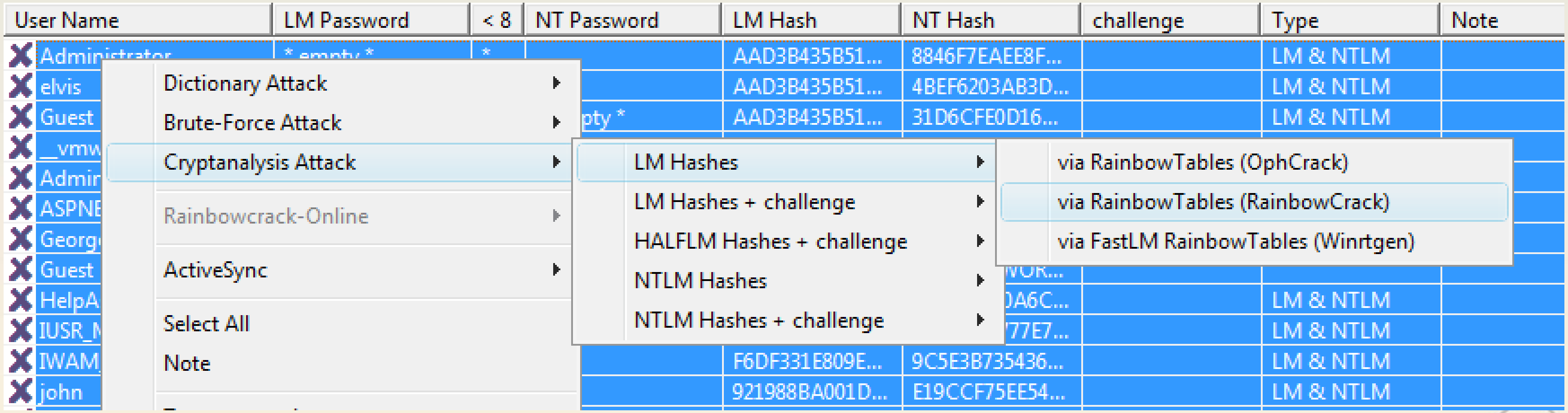
- involves hashing each word in the dictionary (or any search space of candidate passwords) and storing the <plaintext, ciphertext> pairs in a way that enables lookup on the ciphertext field. This way, when a new encrypted password is obtained, password recovery is instantaneous.

http://en.wikipedia.org/wiki/Password_cracking

Precomputation Detail

By applying a time-memory tradeoff, a middle ground can be reached - a search space of size N can be turned into an encrypted database of size O(N2/3) in which searching for an encrypted password takes time O(N2/3).

Cryptanalysis using local Rainbow Tables

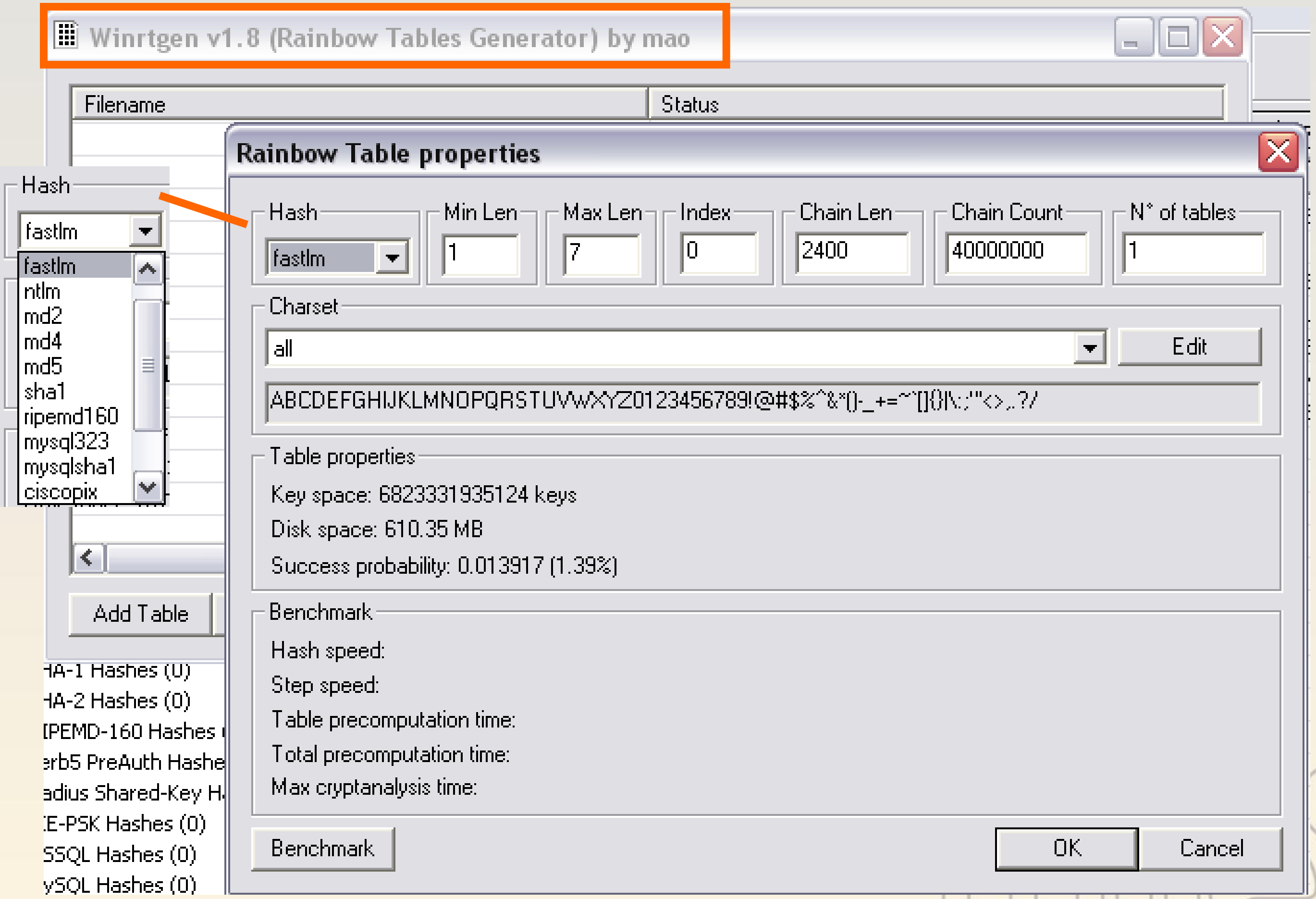


User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type	Note
Administrator	* empty *	*		AAD3B435B51...	8846F7EAEE8F...		LM & NTLM	
elvis				AAD3B435B51...	4BEF6203AB3D...		LM & NTLM	
Guest			pty *	AAD3B435B51...	31D6CFE0D16...		LM & NTLM	
__vmw								
Admin								
ASPNE								
Georg								
Guest					WOR...			
HelpA					0A6C...		LM & NTLM	
IUSR_N					77E7...		LM & NTLM	
IWAM				F6DF331E809E...	9C5E3B735436...		LM & NTLM	
john				921988BA001D...	E19CCF75EE54...		LM & NTLM	

http://en.wikipedia.org/wiki/Password_cracking

Creating Rainbow Tables

Generating tables:


Winrtgen v1.8 (Rainbow Tables Generator) by mao

Rainbow Table properties

Hash	Min Len	Max Len	Index	Chain Len	Chain Count	N° of tables
fastlm	1	7	0	2400	40000000	1

Charset: all

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"<>,.?/

Table properties

Key space: 6823331935124 keys

Disk space: 610.35 MB

Success probability: 0.013917 (1.39%)

Benchmark

Hash speed:

Step speed:

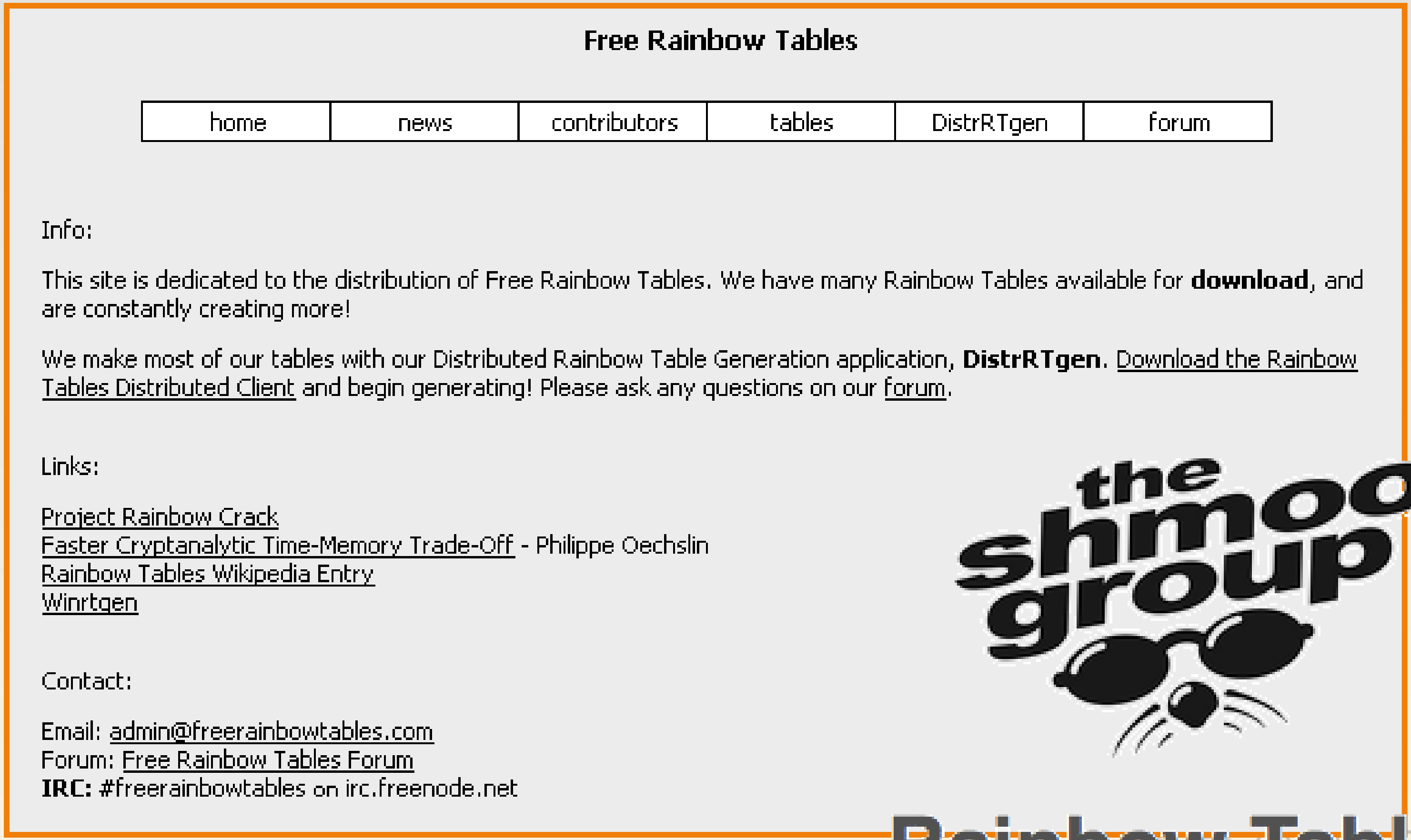
Table precomputation time:

Total precomputation time:

Max cryptanalysis time:

Free Rainbow Tables

http://www.freerainbowtables.com/ → **http://rainbowtables.shmoo.com/**



Free Rainbow Tables

Info:

This site is dedicated to the distribution of Free Rainbow Tables. We have many Rainbow Tables available for **download**, and are constantly creating more!

We make most of our tables with our Distributed Rainbow Table Generation application, **DistrRTgen**. Download the Rainbow Tables Distributed Client and begin generating! Please ask any questions on our forum.

Links:

Project Rainbow Crack
Faster Cryptanalytic Time-Memory Trade-Off - Philippe Oechslin
Rainbow Tables Wikipedia Entry
Winrtgen

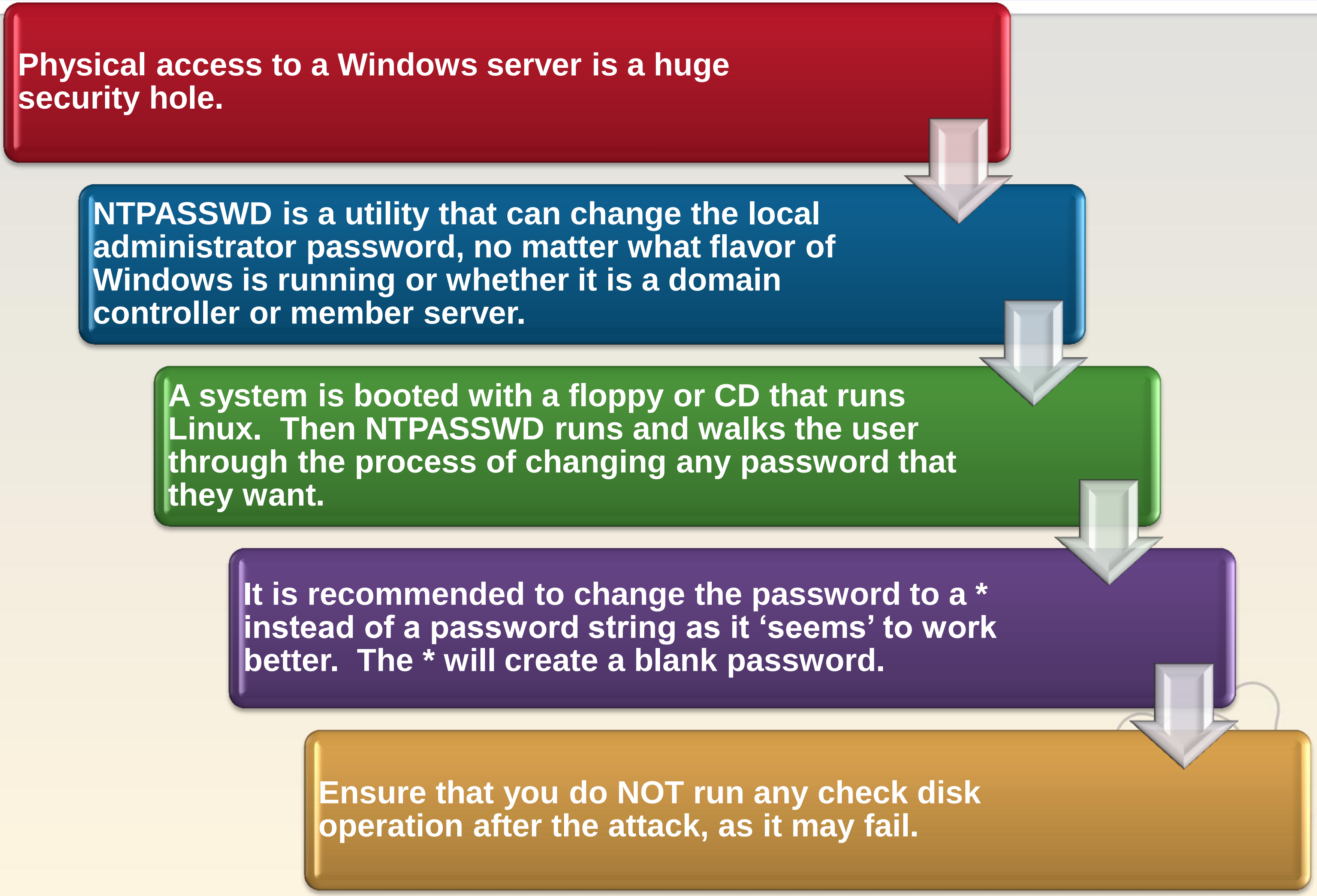
Contact:

Email: admin@freerainbowtables.com
Forum: Free Rainbow Tables Forum
IRC: #freerainbowtables on irc.freenode.net

the shmoo group

Rainbow Tables

NTPASSWD:Hash Insertion Attack



Physical access to a Windows server is a huge security hole.

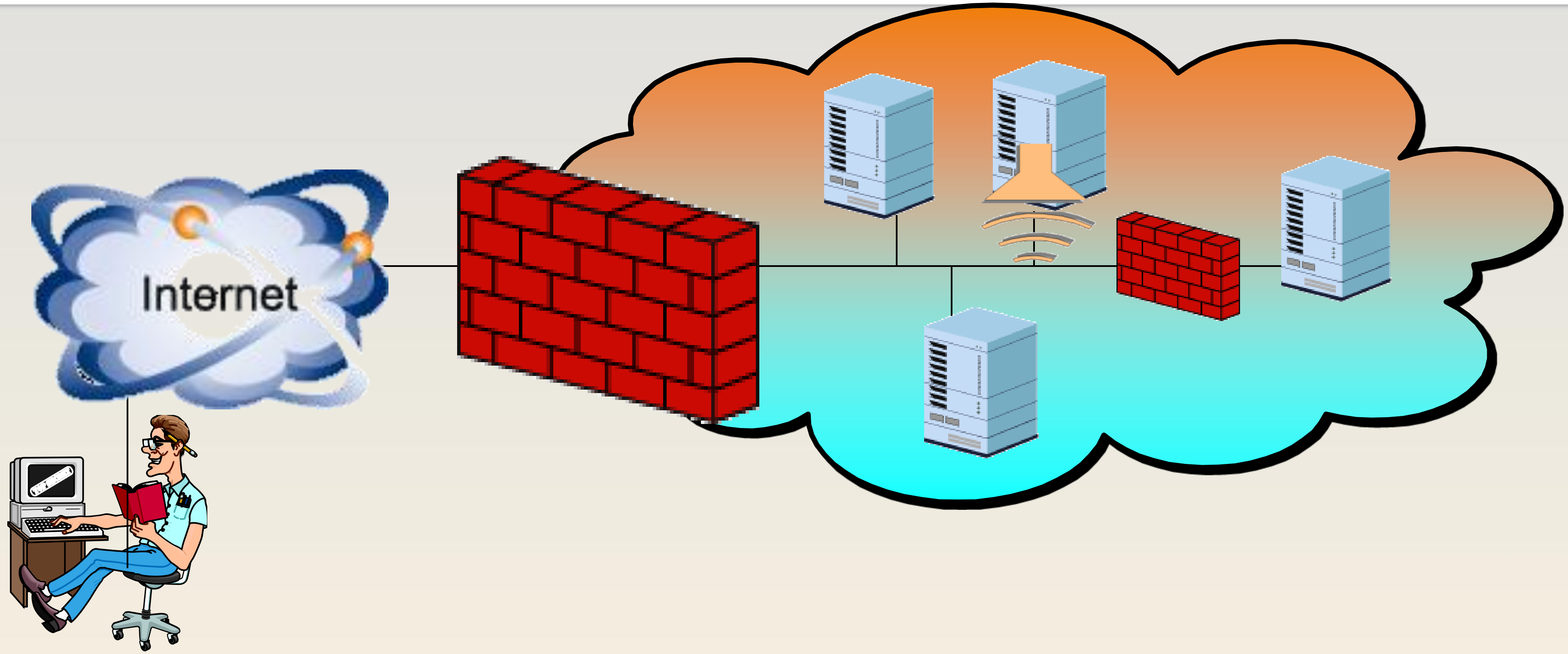
NTPASSWD is a utility that can change the local administrator password, no matter what flavor of Windows is running or whether it is a domain controller or member server.

A system is booted with a floppy or CD that runs Linux. Then NTPASSWD runs and walks the user through the process of changing any password that they want.

It is recommended to change the password to a * instead of a password string as it ‘seems’ to work better. The * will create a blank password.

Ensure that you do NOT run any check disk operation after the attack, as it may fail.

Password Sniffing



- Break in! Could employ technical, physical or social engineering attacks.
- Install sniffer and log to file.
- Retrieve capture file and read usernames and passwords.
- We will cover this in more detail in Module 12.

Windows Authentication Protocols

LM authentication

- Used by Windows 95/98
- Uses DES

NTLM authentication

- Created with NT 3.51
- Uses DES & MD4

NTLM v2

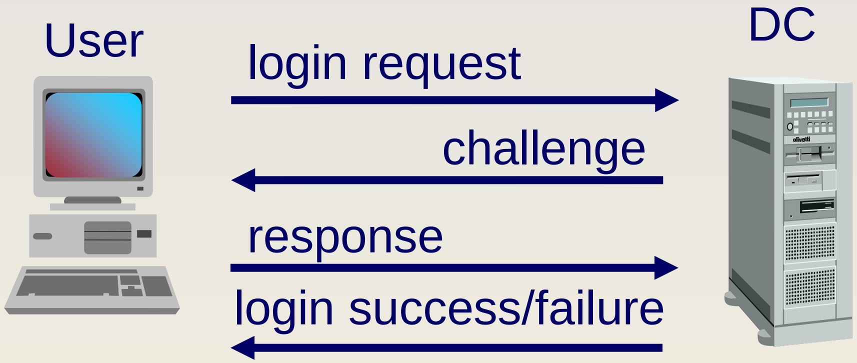
- Created with NT 4 service pack 3
- Uses MD4 & MD5

Kerberos

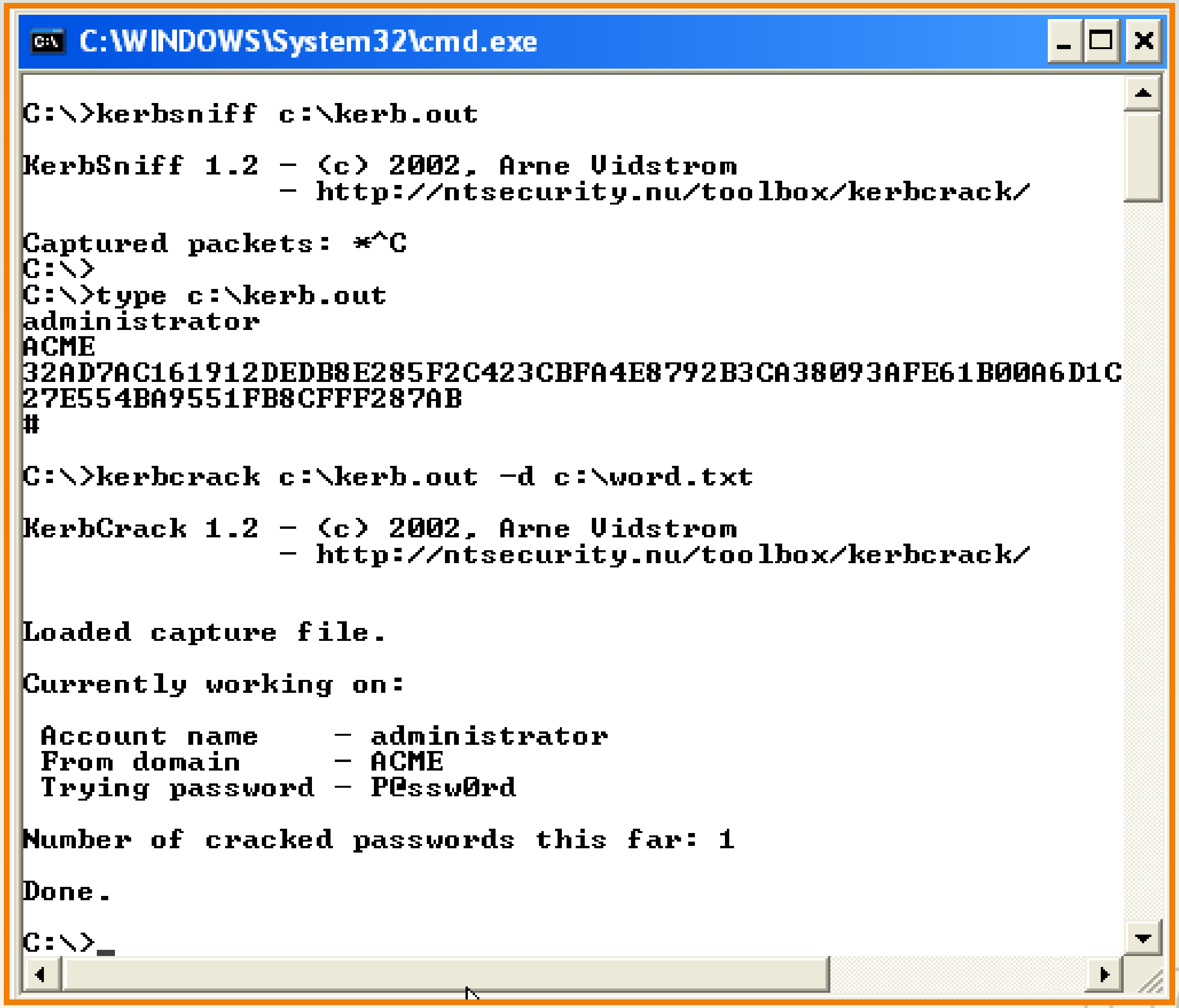
- Created by MIT in 1988
- Kerberos v5 implemented with Windows 2000

An administrator can specify which of these protocols a Windows machine will send by configuring “LanMan Authentication Level”

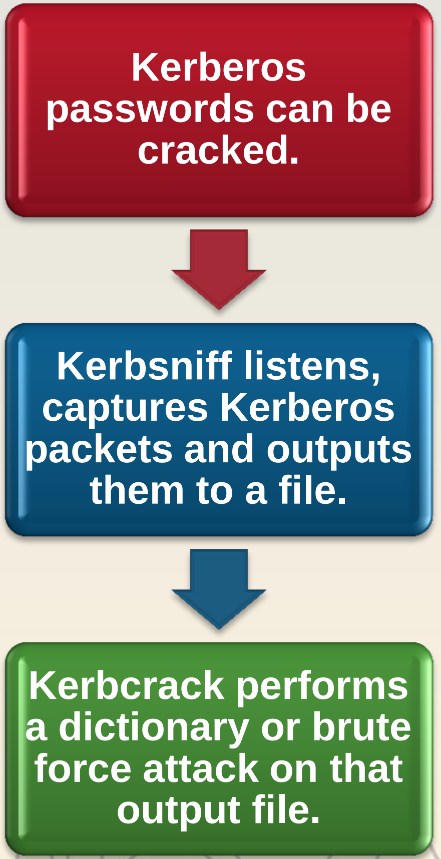
“Challenge/response” process



Hacking Tool: Kerbsniff & KerbCrack



```
C:\>kerbsniff c:\kerb.out

KerbSniff 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/

Captured packets: *^C
C:\>
C:\>type c:\kerb.out
administrator
ACME
32AD7AC161912DEDB8E285F2C423CBFA4E8792B3CA38093AFE61B00A6D1C
27E554BA9551FB8CFFF287AB
#

C:\>kerbcrack c:\kerb.out -d c:\word.txt

KerbCrack 1.2 - (c) 2002, Arne Vidstrom
              - http://ntsecurity.nu/toolbox/kerbcrack/


Loaded capture file.

Currently working on:

 Account name     - administrator
 From domain      - ACME
 Trying password - P@ssw0rd

Number of cracked passwords this far: 1

Done.

C:\>_
```



Kerberos passwords can be cracked.

Kerbsniff listens, captures Kerberos packets and outputs them to a file.

Kerbcrack performs a dictionary or brute force attack on that output file.

Countermeasure: Monitoring Logs

Logging is of no use if you never analyze the logs.

Monitoring multiple servers’ event logs is time consuming if there is no automated method for collecting the logs.

There are many Windows event log management tools available.
Here are just a few:

Languard S.E.L.M.	www.gfi.com
Event Log Management Suite	www.doriansoftware.com
Event Tracker	www.eventlogmanager.com
Sentry Pro	www.infopulse.ro/eng
Sentry II	www.engagent.com
ServScan	www.omnitrend.com

Hard Disk Security

Whole hard drive encryption reduces the risk of data theft.

Commercial and free/open source products available:

- DriveCrypt Plus
- PGP
- BitLocker
- TrueCrypt

May support password, biometric, or USB/doggle unlocking.

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

Breaking HD Encryption

You need to steal the key from RAM.

If the computer boots to the normal login screen you can steal the key even if the computer is turned off.

If the computer boots to a pre-boot screen, it is safe unless stolen after this password is typed in.

http://citp.princeton.edu/memory/media/

Tokens & Smart Cards

Multifactor Authentication:

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

RSA SecurID SID800

RSA SecurID SD520

BlackBerry with
RSA SecurID software token

USB Tokens

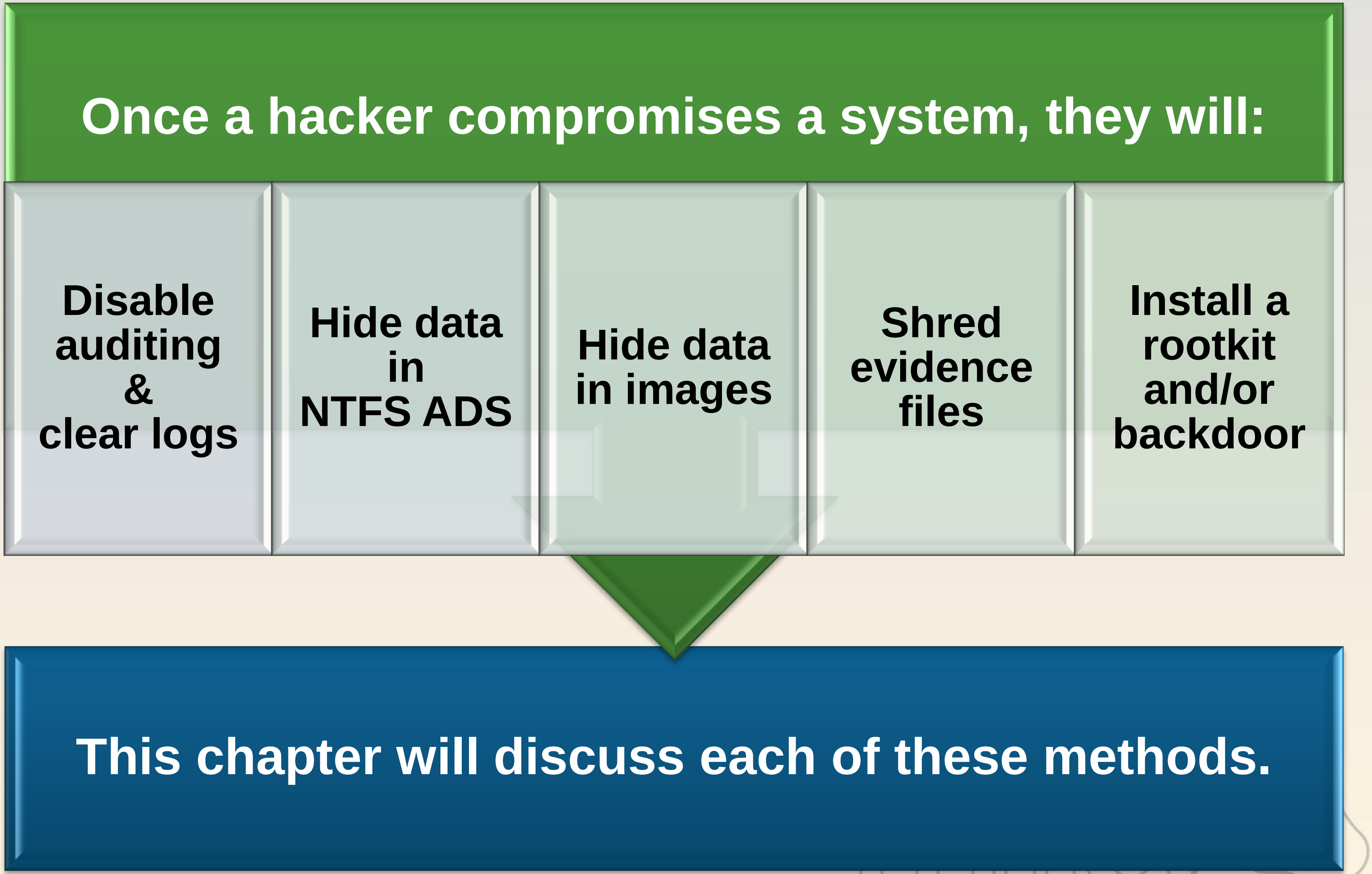
iKey™ 2032 is a compact, two-factor authentication token client security for network authentication, e-mail encryption, and digital signing applications. Its low-cost, compact design, and standard USB interface make it easier to deploy than smartcards or one-time PIN tokens.

YubiKey
a unique USB-key for instant and strong authentication to networks and services

http://www.safenet-inc.com

http://www.yubico.com/products/yubikey/

Covering Tracks Overview

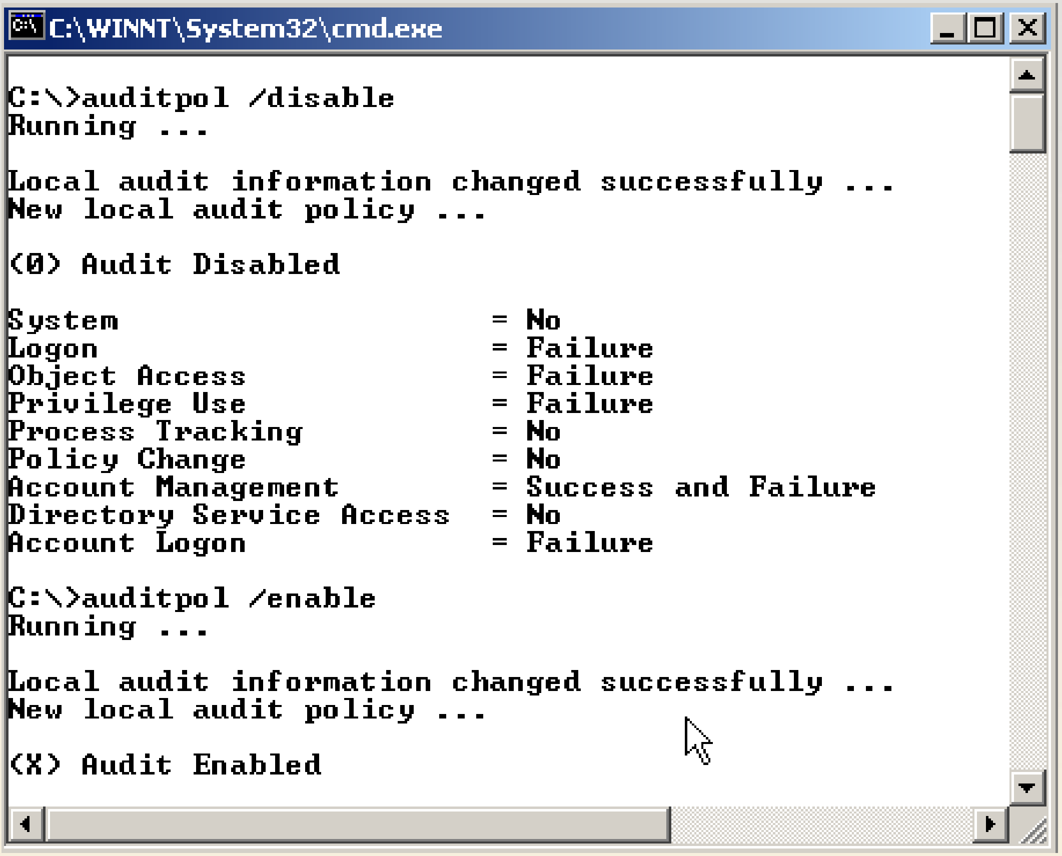


Once a hacker compromises a system, they will:

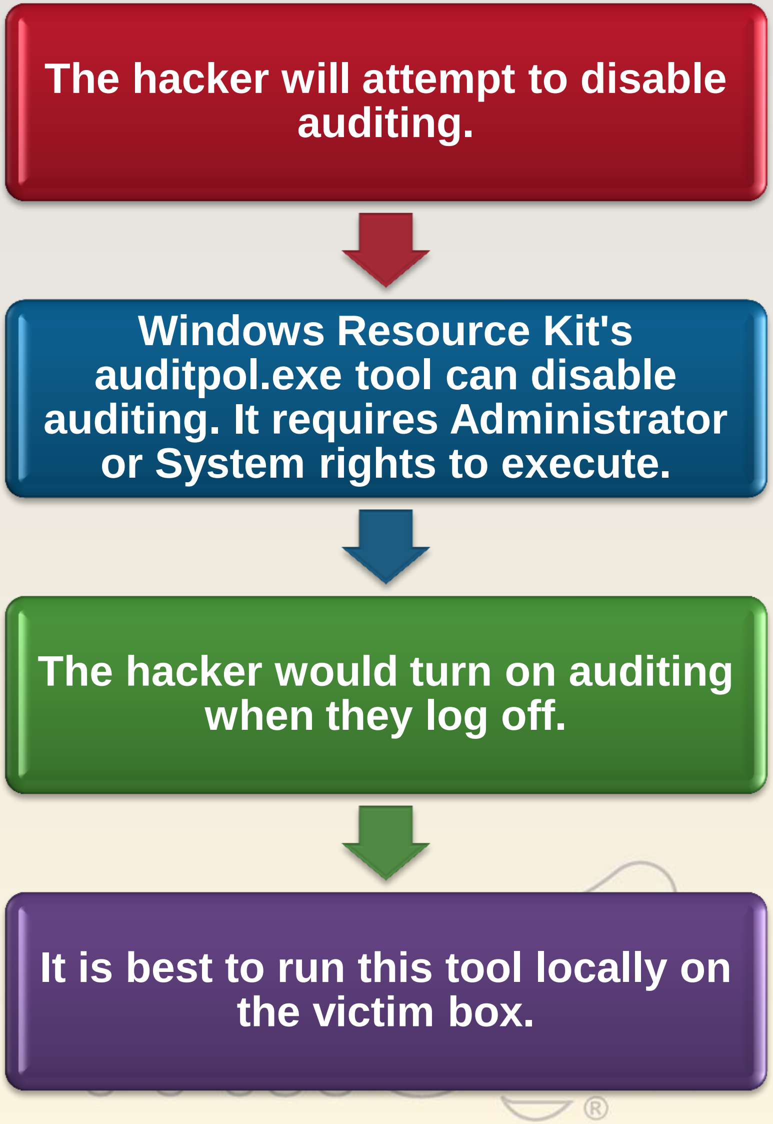
- Disable auditing & clear logs
- Hide data in NTFS ADS
- Hide data in images
- Shred evidence files
- Install a rootkit and/or backdoor

This chapter will discuss each of these methods.

Disabling Auditing



```
C:\>auditpol /disable
Running ...

Local audit information changed successfully ...
New local audit policy ...

(0) Audit Disabled

System                    = No
Logon                     = Failure
Object Access             = Failure
Privilege Use             = Failure
Process Tracking          = No
Policy Change             = No
Account Management        = Success and Failure
Directory Service Access  = No
Account Logon             = Failure

C:\>auditpol /enable
Running ...

Local audit information changed successfully ...
New local audit policy ...

(X) Audit Enabled
```



The hacker will attempt to disable auditing.

Windows Resource Kit's auditpol.exe tool can disable auditing. It requires Administrator or System rights to execute.

The hacker would turn on auditing when they log off.

It is best to run this tool locally on the victim box.

Clearing and Event log

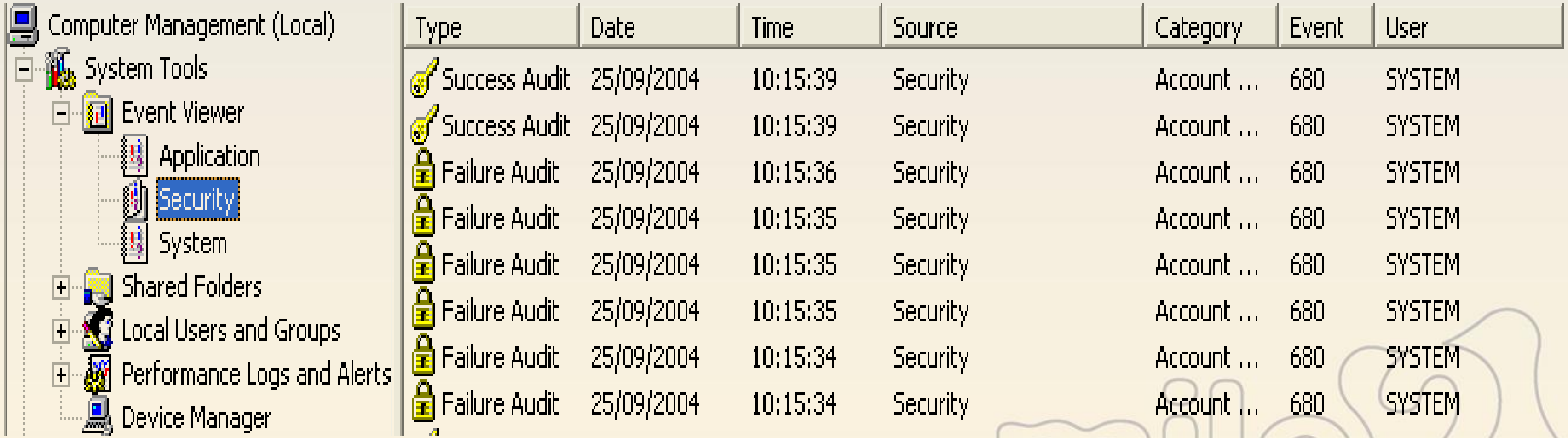
The hacker will clear event logs in order to hide his previous actions.

The problem is that when a log is cleared using Event Viewer, it will remove all entries but create one record stating that the event log has been cleared by 'Hacker'

Another alternative is to use the program elsave.exe to clear the Windows event log. This program does not leave one record behind.

For example, to clear the security log on machine 192.168.1.12:

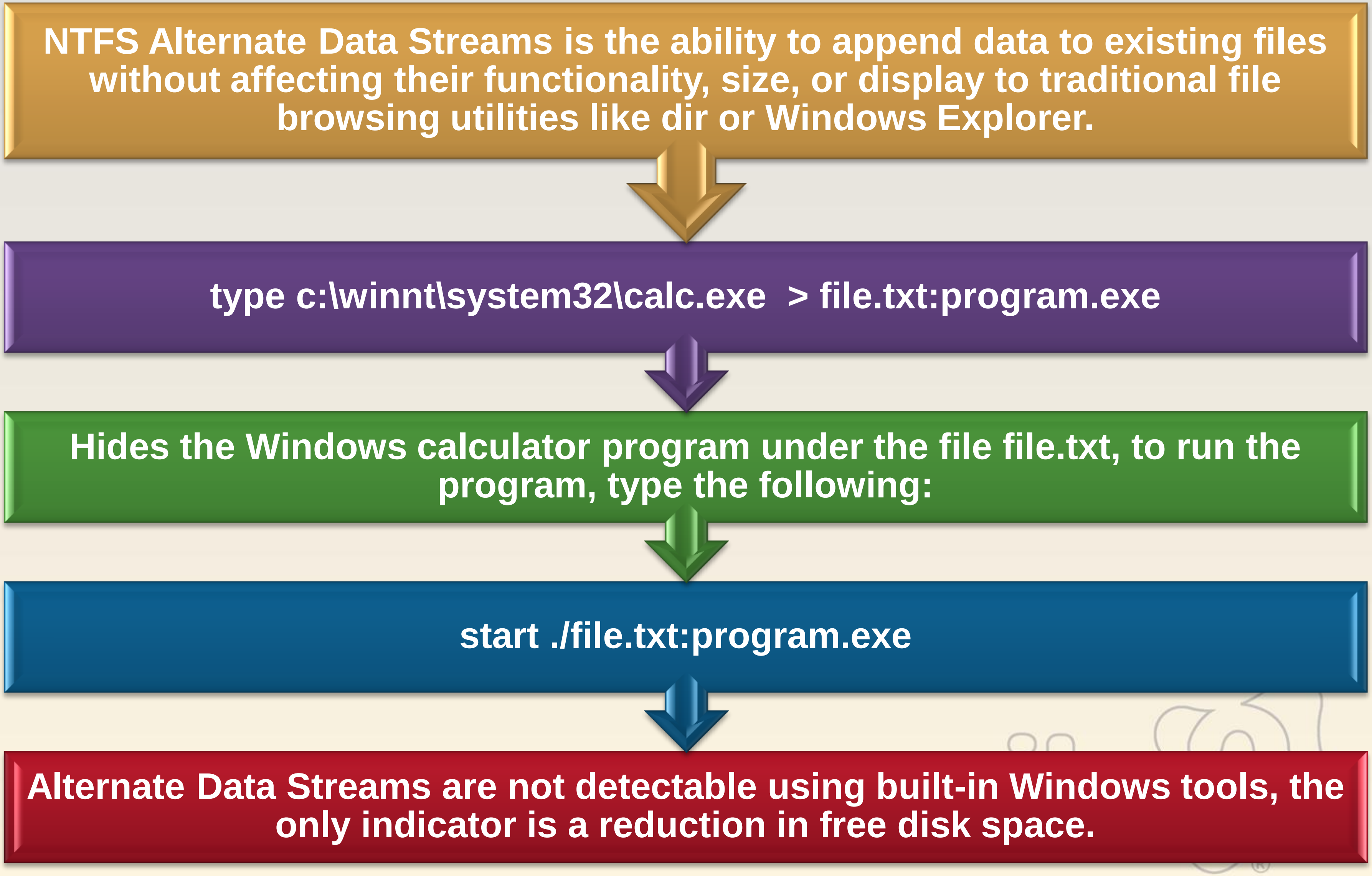
```
elsave –l security  –s  \\192.168.1.12  -C
```



Type	Date	Time	Source	Category	Event	User
Success Audit	25/09/2004	10:15:39	Security	Account ...	680	SYSTEM
Success Audit	25/09/2004	10:15:39	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:36	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:35	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:34	Security	Account ...	680	SYSTEM
Failure Audit	25/09/2004	10:15:34	Security	Account ...	680	SYSTEM

WinZapper is another option: **http://www.ntsecurity.nu/toolbox/winzapper/**

Hiding Files with NTFS Alternate Data Stream



NTFS Alternate Data Streams is the ability to append data to existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer.

```
type c:\winnt\system32\calc.exe  > file.txt:program.exe
```

Hides the Windows calculator program under the file file.txt, to run the program, type the following:

```
start ./file.txt:program.exe
```

Alternate Data Streams are not detectable using built-in Windows tools, the only indicator is a reduction in free disk space.

NTFS Streams countermeasures

Scan your systems for Alternate Data Streams on a regular basis. Use ADS detection tools like:

- LADS - www.heysoft.de/nt/ep-lads.htm
- streams - www.sysinternals.com
- LNS - www.ntsecurity.nu/toolbox/lns/
- CrucialADS - www.crucialsecurity.com
- Stream Explorer - www.rekenwonder.com/streamexplorer.htm

If you detect files that have ADS attached, copy those files to FAT and then back to NTFS to lose hidden content.

- However, this also erases all security settings on the file

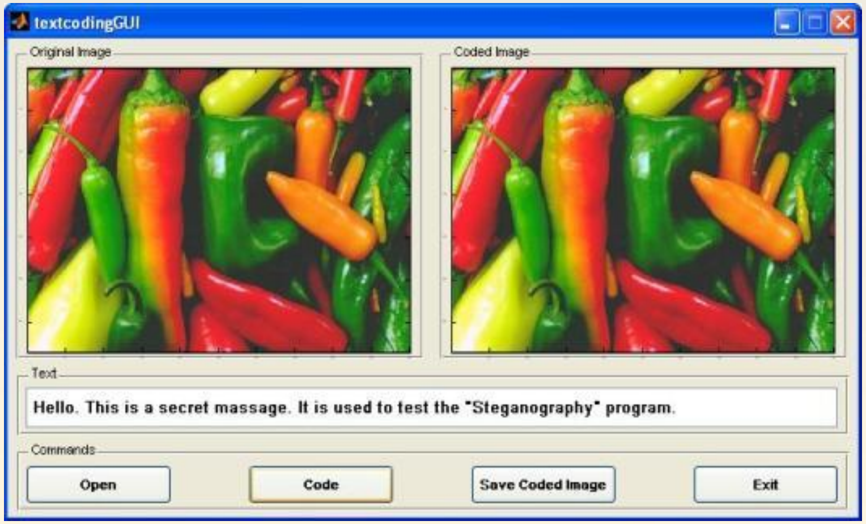
What is Steganography

Steganography takes one piece of information and hides it within another.

Computer files (images, sounds, recordings, even disks) contain unused or insignificant areas of data.

Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance).

The files can then be sent or transported without anyone knowing what really lies inside of them.



Hello. This is a secret massage. It is used to test the "Steganography" program.

Steganography Tools

There are various freeware, shareware, and commercial programs for hiding text in .bmp, .jpg, .wav or mp3 files.

The data that is inserted into the image is encrypted, making it less detectable. Often, adding the data does not increase the file size.

Example stenography tools:

- Cryptobola (www.cryptobola.com/index.htm)
- GIFShuffle (www.darkside.com.au/gifshuffle/)
- http://www.stegoarchive.com/
- http://www.jjtc.com/Steganography/tools.html

Some example stenography detection programs include:

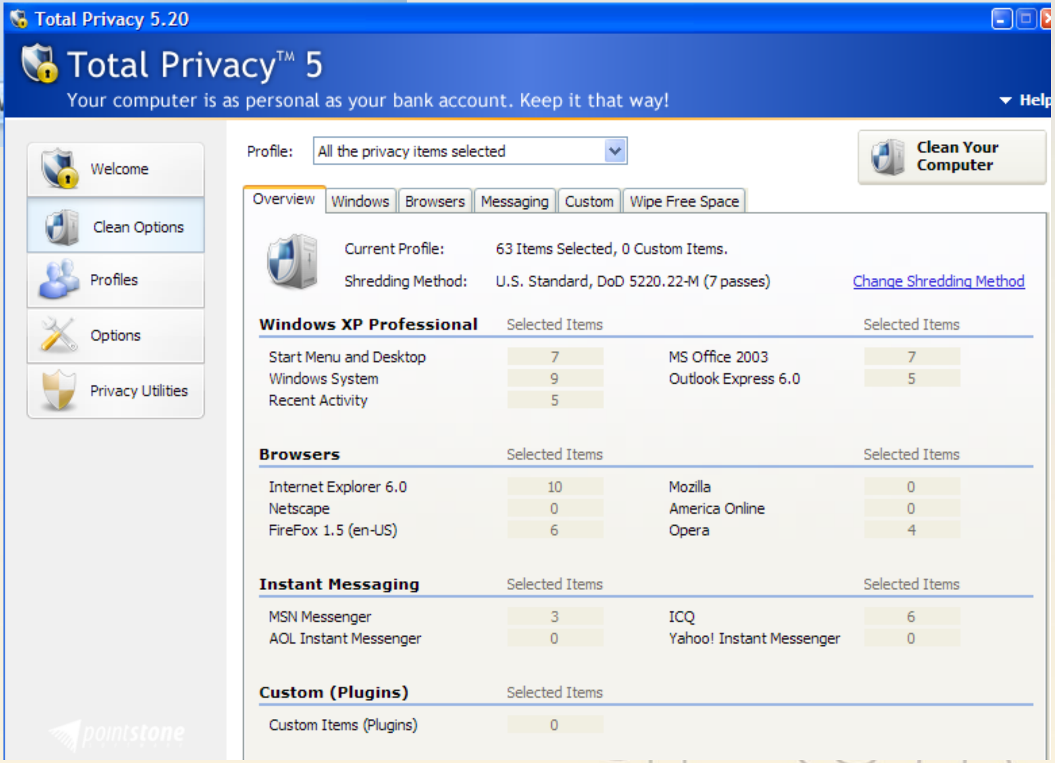
- Stegdetect (http://www.outguess.org/detection.php)
- Stego Suite (http://www.wetstonetech.com)

Shedding Files Left Behind

Total Privacy 5!

Yes, you can surf the Internet without protection - but you might not like the results!

Protect your computer from Prying Eyes!



Total Privacy 5.20

Total Privacy™ 5

Your computer is as personal as your bank account. Keep it that way!

Profile: All the privacy items selected

Current Profile: 63 Items Selected, 0 Custom Items.

Shredding Method: U.S. Standard, DoD 5220.22-M (7 passes)

Windows XP Professional	Selected Items		Selected Items
Start Menu and Desktop	7	MS Office 2003	7
Windows System	9	Outlook Express 6.0	5
Recent Activity	5		

Browsers	Selected Items		Selected Items
Internet Explorer 6.0	10	Mozilla	0
Netscape	0	America Online	0
FireFox 1.5 (en-US)	6	Opera	4

Instant Messaging	Selected Items		Selected Items
MSN Messenger	3	ICQ	6
AOL Instant Messenger	0	Yahoo! Instant Messenger	0

Custom (Plugins)	Selected Items
Custom Items (Plugins)	0

With Total Privacy, you get total confidence and peace of mind for secure computer use by completely and permanently removing all traces and history of your recent activity.

↓

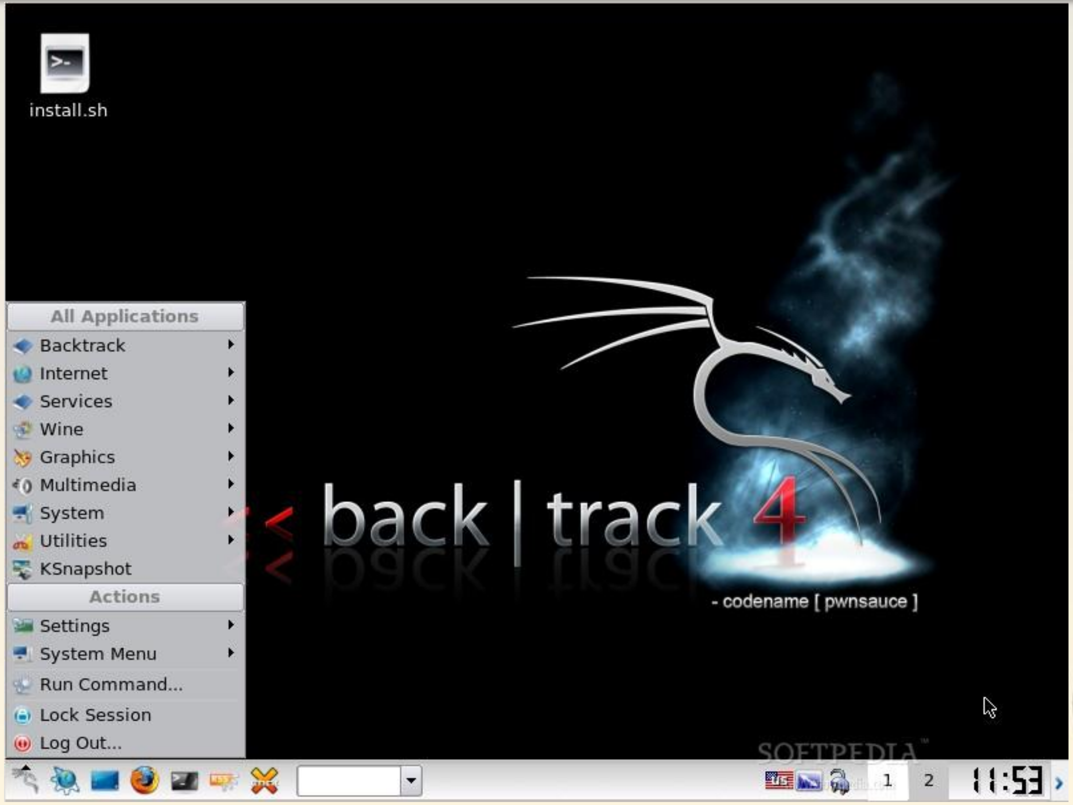
Total Privacy also helps optimize performance by deleting all those unnecessary temporary files, install/uninstall records, and by cleaning your Internet browser cache.

Leaving No Local Trace

By using any of the powerful Linux Live CD's designed to audit IT security, an attacker can protect themselves from locally cached evidence.

The CD is a ROM format, therefore any evidence stored in RAM is wiped when the machine is rebooted.

This will offer some protection if the attackers machine is seized by Law Enforcement Officers.



Tor: Anonymous Internet Access

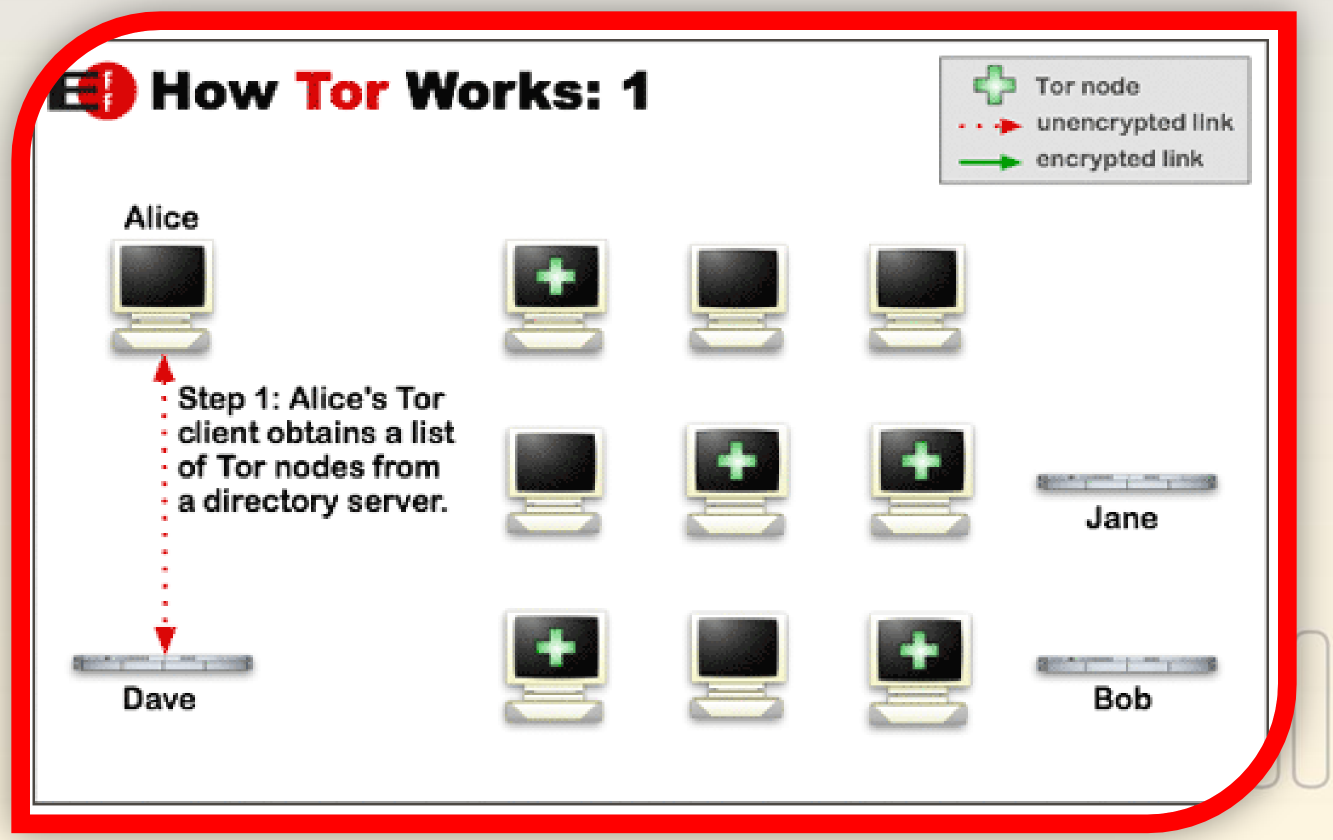
Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features.

The U.S. Navy uses Tor for open source intelligence gathering. Law enforcement uses Tor for visiting or surveillance of sites without leaving government IP addresses in their logs and for security during sting operations.

http://www.torproject.org/

How Tor Works

Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several servers that cover your tracks so no observer, at any single point, can tell where the data came from or where it's going.

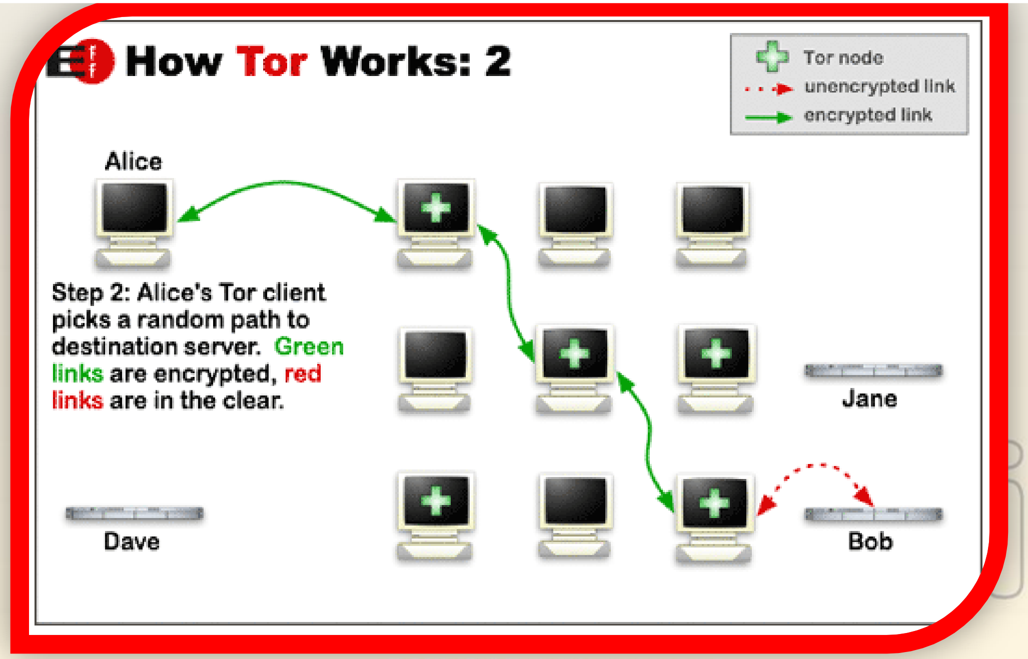

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob

How Tor Works

To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through servers on the network.

- **The circuit is extended one hop at a time and each server along the way knows only which server gave it data and which server it is giving data to. No individual server ever knows the complete path taken.**

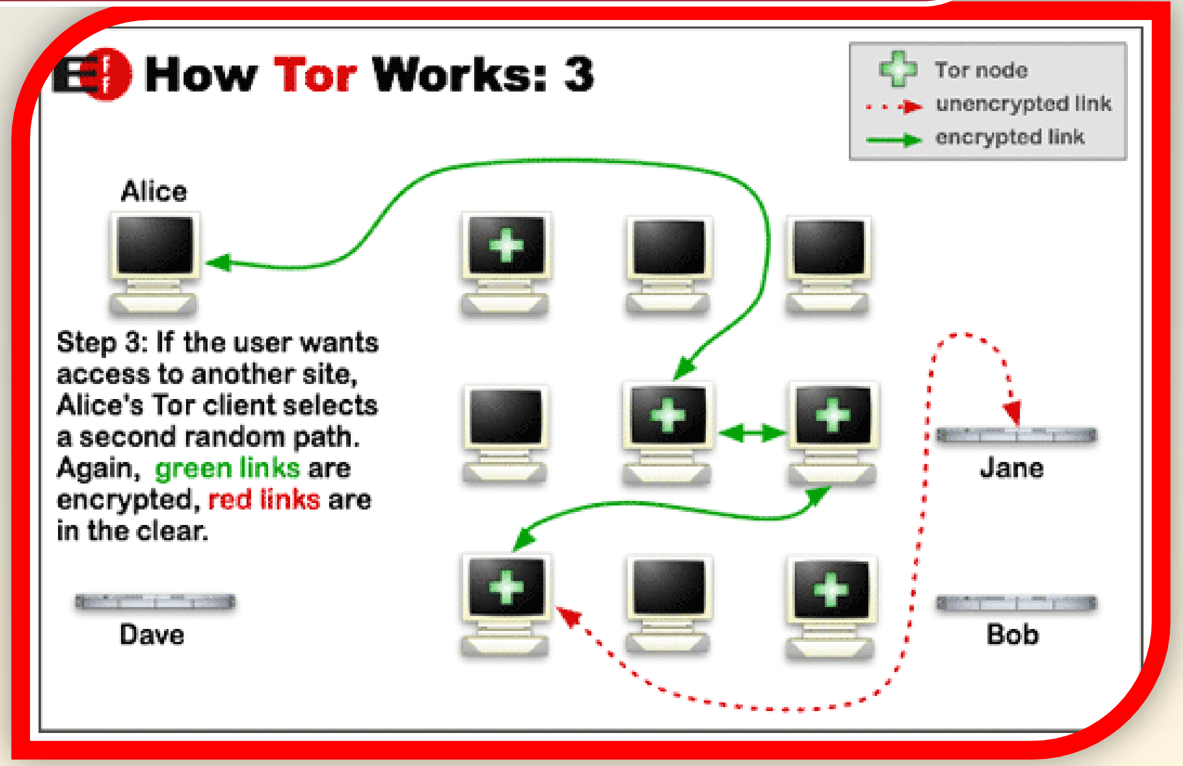
The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How Tor Works

Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each server sees no more than one hop in the circuit, neither an eavesdropper nor a compromised server can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support.



Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

TOR + OpenVPN= Janus VM

www.janusvm.com

A VMWare appliance providing anonymity and privacy!!

FEATURES -
* Works with WiFi.
* Support multiple users in a LAN.
* Protects you from most man-in-the-middle attacks.
* Protects you from Javascript, Java, and Flash based side-channel privacy attacks.
* Protects your identity and your true location by masking your IP Address.
* Encrypts and re-routes your DNS request and ALL TCP traffic to ensure strong privacy.
* Strips out most privacy sensitive information your web browser may leak.
* Blocks popups, annoying ads, banners, and other obnoxious Internet junk.
* Very simple setup and operation.
* Works transparently for applications using TCP. (No UDP or ICMP support)

Follow the video instructions to deploy and configure the Janus VM.

Encrypted Tunnel Notes:

Remember an encrypted tunnel has advantages for both the security conscious user and malicious hacker:

Users can better protect against malware, Trojans, and man in the middle attacks.

Hackers can use an encrypted tunnel to pipe data; commands and control remote sessions undetected.

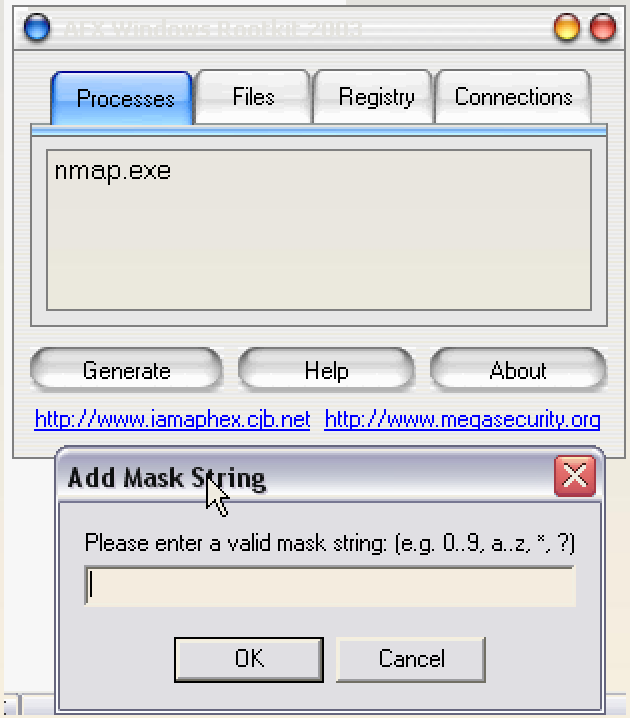
The IDS, IPS and Firewall can not read what is in the encrypted tunnel.

Hacking Tool: RootKit

The primary purpose of a rootkit is to allow an attacker unregulated and undetected access to a compromised system repeatedly.

Rootkits are used by hackers for various reasons:

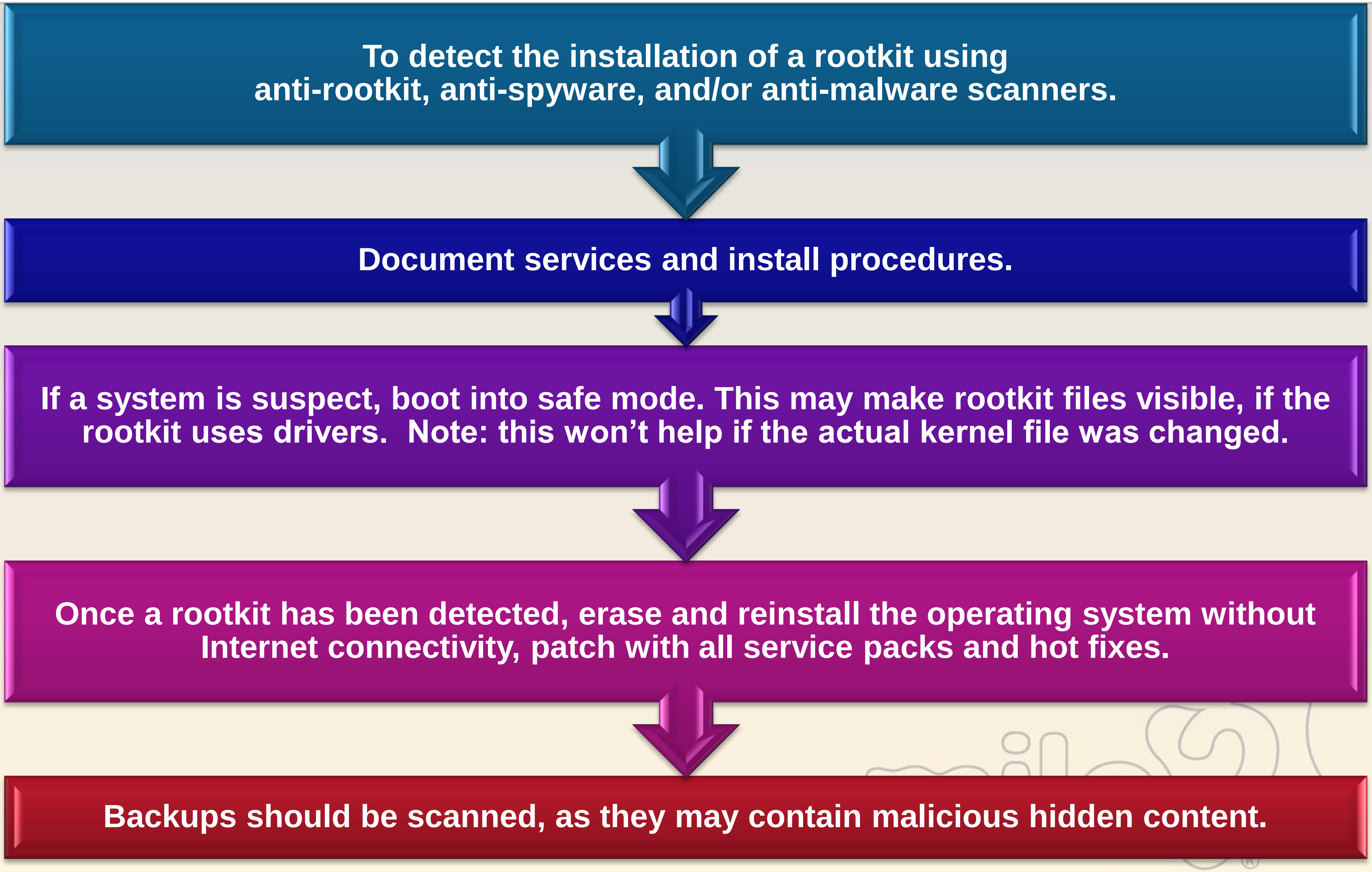
- Hide backdoor processes
- Elevate process privileges
- Hide files
- Hide registry entries
- Disable auditing and edit event logs
- Redirect executable files
- Hide device drivers
- Hide user accounts



nmap.exe

Please enter a valid mask string: (e.g. 0..9, a..z, *, ?)

Windows RootKit Countermeasures



To detect the installation of a rootkit using anti-rootkit, anti-spyware, and/or anti-malware scanners.

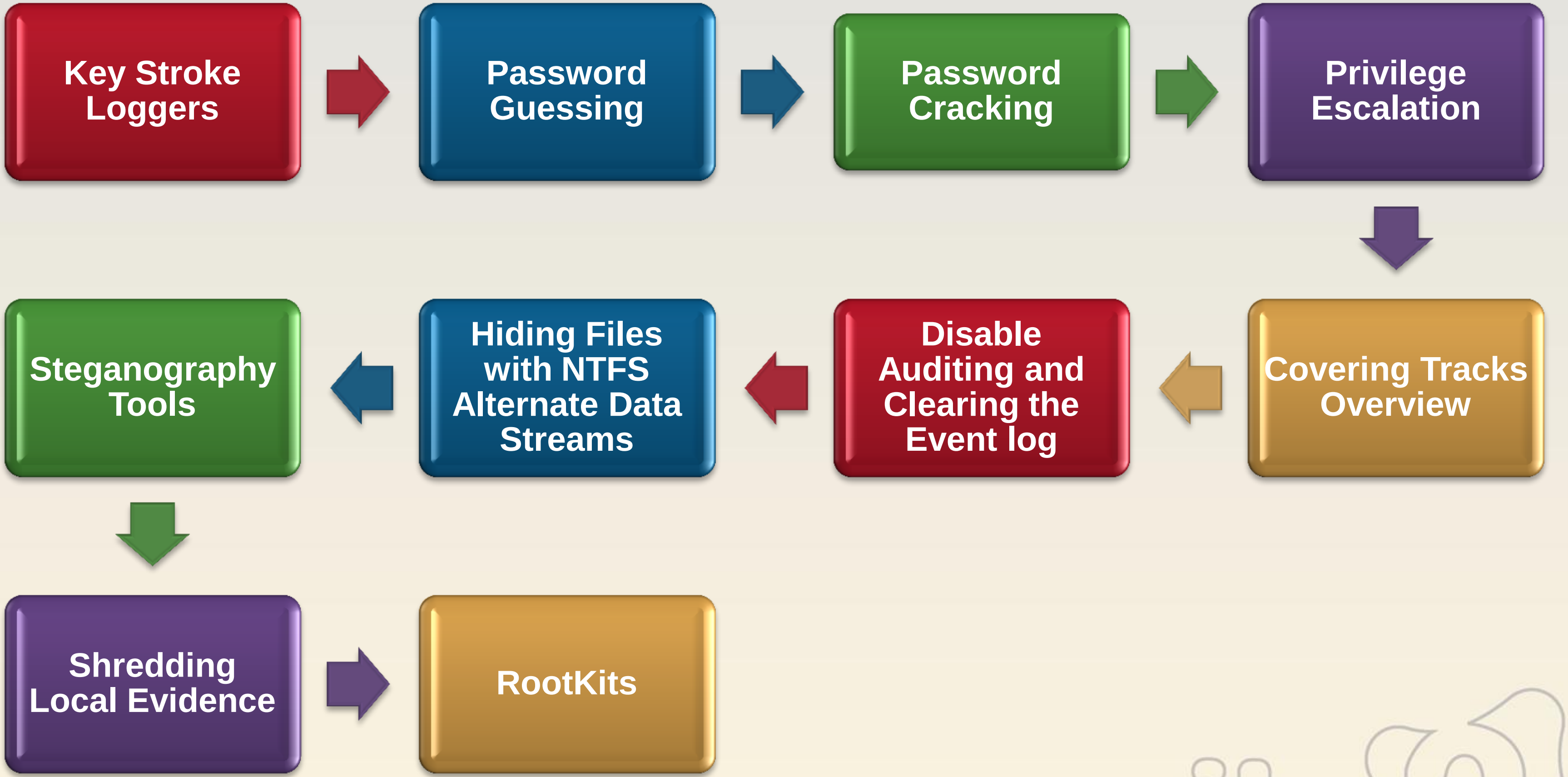
Document services and install procedures.

If a system is suspect, boot into safe mode. This may make rootkit files visible, if the rootkit uses drivers. Note: this won’t help if the actual kernel file was changed.

Once a rootkit has been detected, erase and reinstall the operating system without Internet connectivity, patch with all service packs and hot fixes.

Backups should be scanned, as they may contain malicious hidden content.

Review



Key Stroke Loggers

Password Guessing

Password Cracking

Privilege Escalation

Covering Tracks Overview

Disable Auditing and Clearing the Event log

Hiding Files with NTFS Alternate Data Streams

Steganography Tools

Shredding Local Evidence

RootKits

Module 8 Lab
Hacking Windows