

# Hacking Exposed 7

## Network Security Secrets & Solutions

### Chapter 4 Hacking Windows

# Reasons for Windows Security Problems

- Backward Compatibility
  - Very important at businesses
  - Enabled by default
  - Causes many security problems
- Proliferation of features
- Average 70 MS security bulletins per year

# MS Security Bulletin Statistics

Microsoft Security Bulleti  Sicuro | https://docs.microsoft.com/en-us/security-updates/securitybulletinsummaries/2017/ms17-mar

 Microsoft

Docs Windows Microsoft Azure Visual Studio Office More ▾

Home / Security Bulletin Summaries / 2017 / MS17-mar

Filter by title

- Security Updates
- > Security Advisories
- ✓ Security Bulletin Summaries
  - 2017
    - MS17-mar
    - MS17-feb
    - MS17-jan
  - > 2016
  - > 2015
  - > 2014
  - > 2013
  - > 2012
  - > 2011
  - > 2010

## Microsoft Security Bulletin Summary for March 2017

10/11/2017 • 54 minutes to read • Contributors 

Published: March 14, 2017 | Updated: August 8, 2017

**Version:** 4.0

This bulletin summary lists security bulletins released for March 2017.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit [Microsoft Technical Security Notifications](#).

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see the section, **Other Information**.

As a reminder, the [Security Updates Guide](#) will be replacing security bulletins. Please see our blog post, [Furthering our commitment to security updates](#), for more details.

 Feedback  
 Share  
Theme  
Light ▾

### In this article

- Executive Summaries
- Exploitability Index
- Affected Software
- Detection and Deployment and Guidance
- Acknowledgments
- Other Information

## Security Update Guide

[Subscribe](#)

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the security risks and help keep your systems protected.

[All](#)   [Deployments](#)   [Vulnerabilities](#)   [Advisories](#)[Select date range](#) ▾[Edit](#)

<a href="#">Keyword</a>	<a href="#">Product Family</a>	<a href="#">Max Severity</a>	<a href="#">Impact</a>	<a href="#">Platform</a>	<a href="#">Release notes</a>
-------------------------	--------------------------------	------------------------------	------------------------	--------------------------	-------------------------------

<a href="#">Release ...</a>	<a href="#">Product</a>	<a href="#">Platform</a>	<a href="#">Impact</a>	<a href="#">Max Severity</a>	<a href="#">Article</a>	<a href="#">Download</a>	<a href="#">Batch</a>
-----------------------------	-------------------------	--------------------------	------------------------	------------------------------	-------------------------	--------------------------	-----------------------

[2024-Mar Release Notes](#)

Mar 7, 2024	Microsoft Edge (Chromium-based)	-	-	-	<a href="#">Release Notes</a>	Security Update	12
-------------	---------------------------------	---	---	---	-------------------------------	-----------------	----

Mar 7, 2024	Microsoft Edge (Chromium-based)	-	-	-	<a href="#">Release Notes</a>	Security Update	12
-------------	---------------------------------	---	---	---	-------------------------------	-----------------	----

Mar 7, 2024	Microsoft Edge (Chromium-based)	-	-	-	<a href="#">Release Notes</a>	Security Update	12
-------------	---------------------------------	---	---	---	-------------------------------	-----------------	----

Mar 7, 2024	Microsoft Edge for Android	-	-	-	-	-	-
-------------	----------------------------	---	---	---	---	---	---

[2024-Feb Release Notes](#)

Feb 29, 2024	Microsoft Edge (Chromium-based)	-	-	-	<a href="#">Release Notes</a>	Security Update	12
--------------	---------------------------------	---	---	---	-------------------------------	-----------------	----

# Prelude

- Vulnerabilities
  - Trivially exploited configuration vulnerabilities
    - NetBIOS null sessions, simple IIS buffer overflow
  - More complex ones
    - Heap exploits, end-user attack through Internet Explorer
- Hacker focus changed
  - Network services, kernel drivers, applications
- Factors of risk: Popularity and Complexity
  - Popular Windows vulnerabilities: Code Red, Nimda, Slammer, Blaster, Netsky, Gimmiv, EternalBlu, NotPetya, etc.
  - NT 3.51 → Windows 7: tenfold in code size
- Improvements: New security-related features
  - Reduced default network services, host firewall enabled by default, user account control (UAC), etc.

Map Source: www.visualroute.com



Sat Jan 25 05:29:00 2003 (UTC)

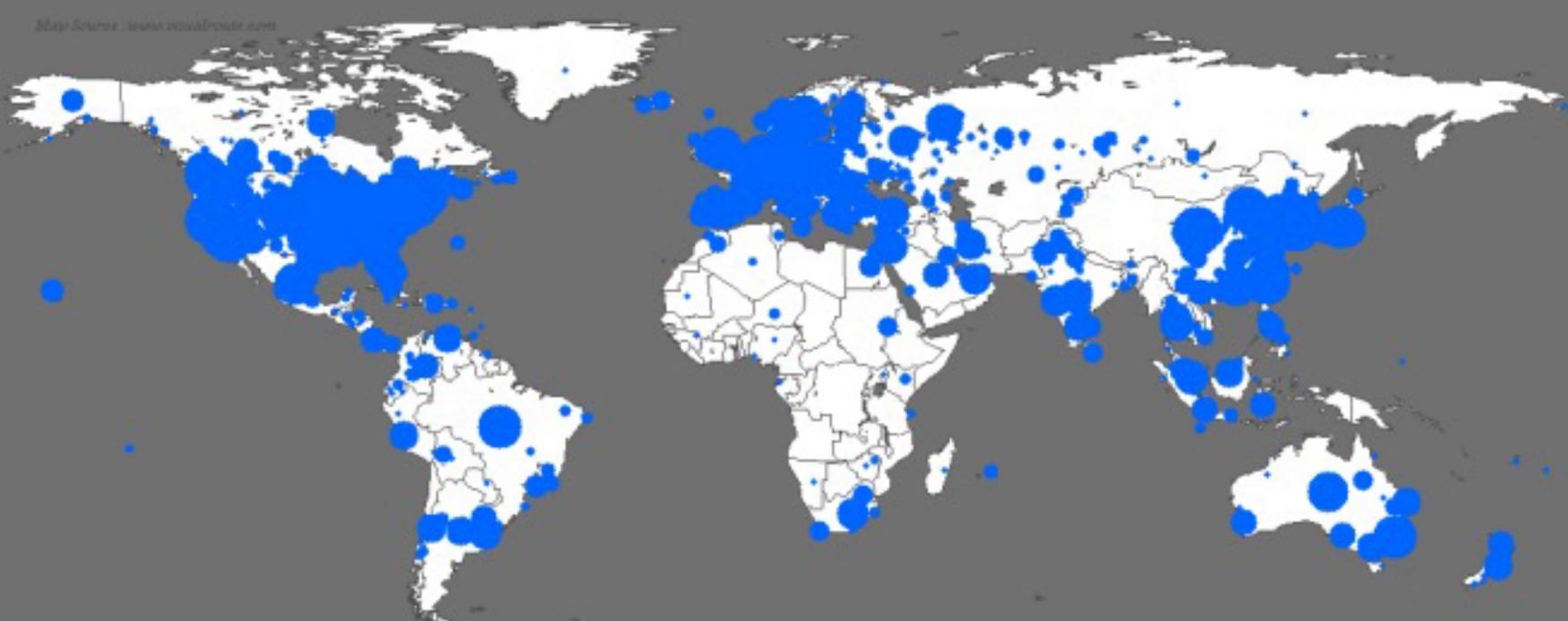
Number of hosts infected with Sapphire: 0

<http://www.caida.org>

Copyright (C) 2003 UC Regents

Pictures taken from *The Spread of the Sapphire/Slammer Worm*, by David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver

Map Source: www.mapdivide.com



Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

<http://www.caida.org>

Copyright (C) 2003 UC Regents

Pictures taken from *The Spread of the Sapphire/Slammer Worm*, by David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver

 User Account Control X

Do you want to allow the following program to make changes to this computer?



Program name: Registry Editor

Verified publisher: Microsoft Windows

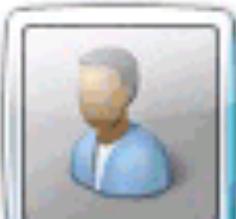
File origin: Hard drive on this computer

---

To continue, type an administrator password, and then click Yes.



FABRIKAM\summer



Use another account

# ZERODIUM Payouts for Desktops/Servers\*

Up to \$1,000,000									
Up to \$500,000									
Up to \$250,000									
Up to \$200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE  Win/Linux			4.002 Sendmail RCE  Linux	4.003 Postfix RCE  Linux	4.004 Dovecot RCE  Linux	4.005 Exim RCE  Linux	2.005 nginx RCE  Linux
Up to \$100,000		3.002 Safari RCE+LPE  Mac	3.003 Edge RCE+LPE  Win	3.004 Firefox RCE+LPE  Win	5.003 Word/Excel RCE  Win	7.001 WordPress RCE  Linux	7.002 cPanel/WHM RCE  Linux	7.003 Plesk RCE  Linux	7.004 Webmin RCE  Linux
Up to \$80,000	6.002 VMware WS VME  Win/Linux					5.004 Adobe PDF RCE+SBX  Win	5.005 WinRAR RCE  Win	5.006 7-Zip RCE  Win	6.003 Windows LPE/SBX  Win
Up to \$50,000	6.004 USB LPE  Win/Mac	8.001 Antivirus RCE  Win			5.007 WinZip RCE  Win	5.008 tar RCE  Linux	6.005 macOS LPE/SBX  Mac	6.006 Linux LPE  Linux	6.007 BSD LPE  BSD
Up to \$10,000	9.001 Routers RCE	8.002 Antivirus LPE  Win	7.005 phpBB RCE  Linux	7.006 vBulletin RCE  Linux	7.007 MyBB RCE  Linux	7.008 Joomla RCE  Linux	7.009 Drupal RCE  Linux	7.010 Roundcube RCE  Linux	7.011 Horde RCE  Linux
*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.									
1.001 Win RCE Zero Click  Win									

# Hacking Windows

- Unauthenticated attacks
  - Remote network exploits
- Authenticated attacks
  - Insider: escalating, extracting password
- Windows security features
  - OS Countermeasures and best practices

# Unauthenticated Attacks

# Four Vectors

- **Authentication Spoofing (password)**
- **Network Services**
- **Client Software Vulnerabilities**
- **Device Drivers**

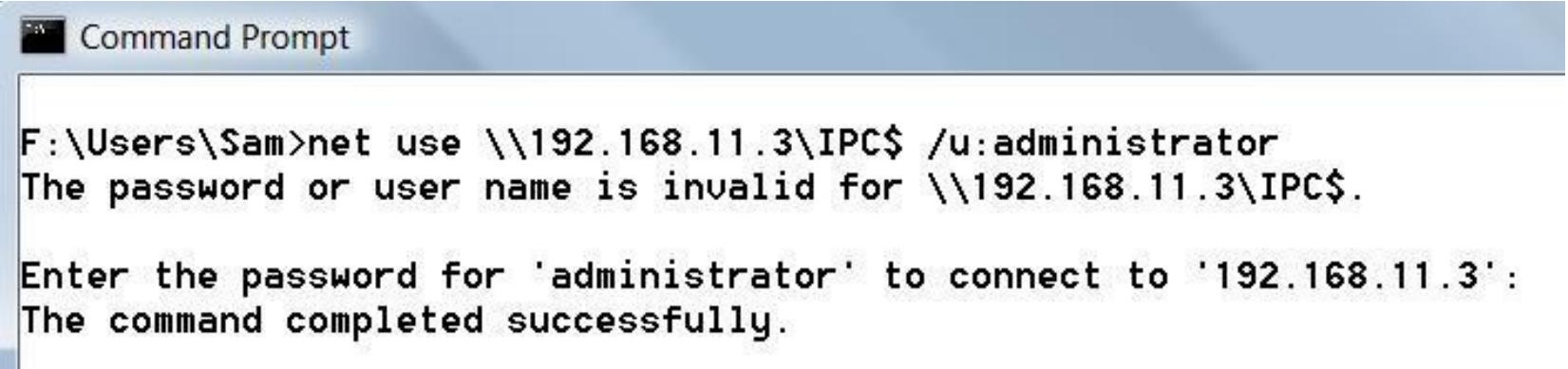
**Protect weakness in these areas**

# Authentication Spoofing Attacks

# Services to Attack

- **Traditional target:** Server Message Block (SMB)
  - TCP ports 445 and 139
- Microsoft Remote Procedure Call (MSRPC)
  - TCP port 135
- Terminal Services
  - TCP port 3389
- SQL
  - TCP 1443 and UDP 1434
- SharePoint and other Web services
  - TCP 80 and 443

# Password Guessing from the Command Line



A screenshot of a Windows Command Prompt window titled "Command Prompt". The window contains the following text:

```
F:\Users\Sam>net use \\192.168.11.3\IPC$ /u:administrator
The password or user name is invalid for \\192.168.11.3\IPC$.

Enter the password for 'administrator' to connect to '192.168.11.3':
The command completed successfully.
```

- Accounts may lock out after too many guesses

# A Password Guessing Script

- Put password – user name pairs in a file named credentials.txt

```
[file: credentials.txt]
password      username
""           Administrator
password      Administrator
admin         Administrator
administrator Administrator
secret        Administrator
etc. . . .
```

Now we can feed this file to our FOR command, like so:

```
C:\>FOR /F "tokens=1,2*" %i in (credentials.txt) do net use \\target\IPC$ %i /u:%j
```

- Tools: enum, Brutus, THC Hydra, Medusa, Venom, TSGrinder, many more.

# Password-Guessing Countermeasures

- Use a network firewall to restrict access to SMB services on TCP 139 and 445
- Use host-resident features of Windows to restrict access to SMB
  - IPSec filters
  - Windows Firewall
- Disable SMB services (on TCP 139 and 445)
- Enforce the use of strong/long passwords using policy
- Set an account-lockout threshold and ensure that it applies to the built-in Administrator account
- Enable audit account logon failures and regularly review Event Logs
- **Use all of them** for defense in depth

# Security Policy

- SECPOL.MSC at a Command Prompt



# Audit Policy



- Use a log analysis tool to check the logs – Microsoft Dumpel

```
C:\> dumpel -e 529 -f seclog.txt -l security -n Security -t
```

- For even better security, use Intrusion Detection/Intrusion Prevention software

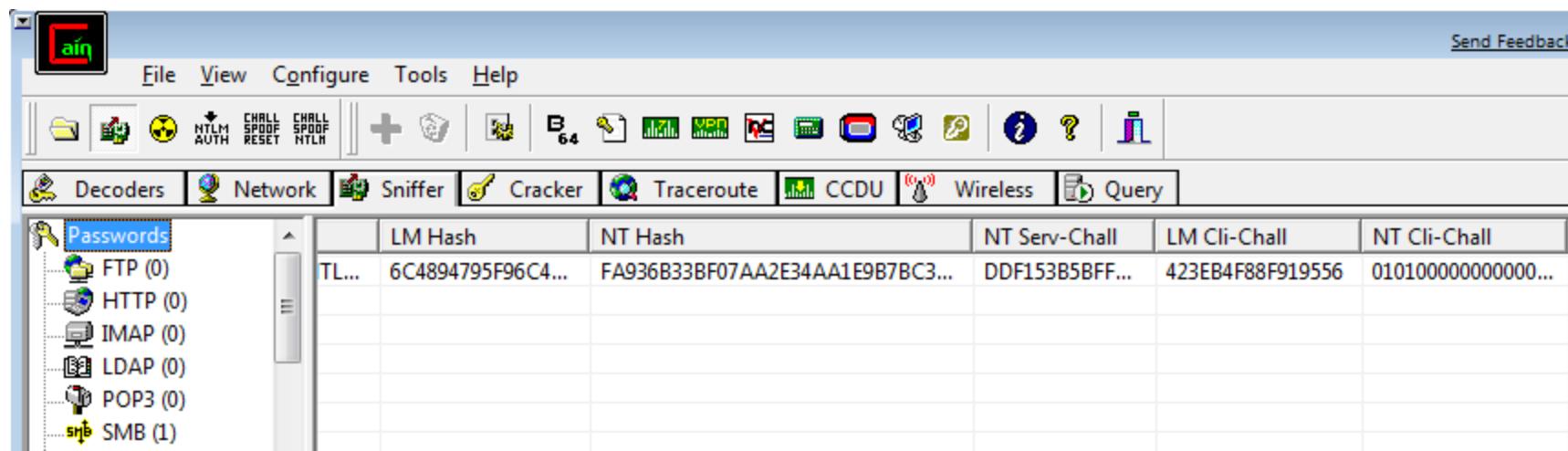
# Unauthenticated Attacks

## Authenticated Spoofing

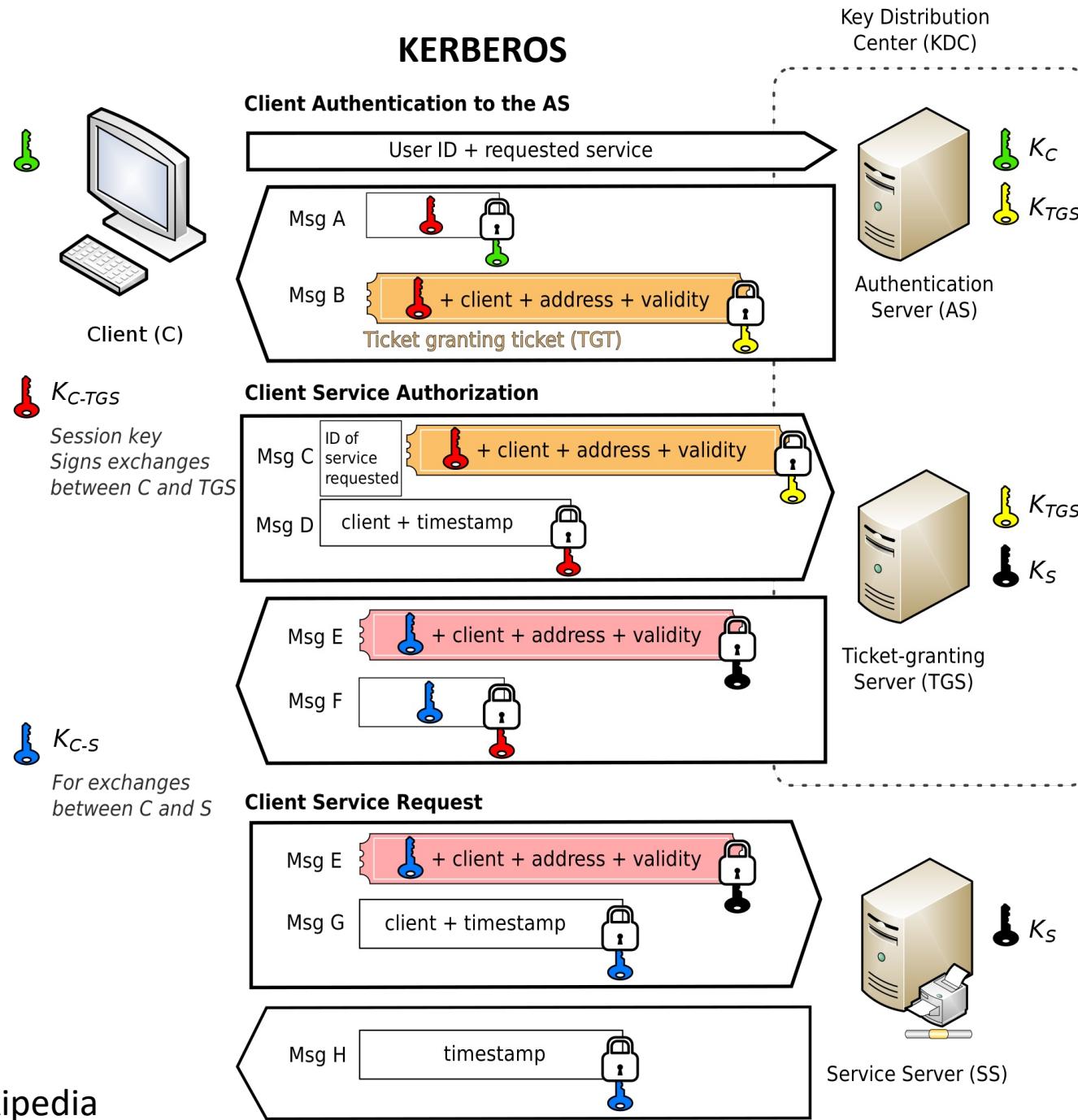
- Remote password guessing
  - Main targets: Server Message Block (SMB) on TCP 445 and 139, Microsoft Remote Procedure Call (MSRPC) on TCP 135, Terminal Services (TS) on TCP 3389, SQL on TCP 1433 and UDP 1434, SharePoint (SP) over HTTP on TCP 80 and HTTPS on TCP 443, etc.
  - Automatic guessing on CLI: **FOR** and **net use** with username/password file (see online default-password DB), **enum**, **Brutus**, **THC Hydra**, **Venom**
  - Automatic guessing on GUI of Terminal Services/Remote Desktop Services: **TSGrinder**, **Rdesktop** after **patch** with brute-force capabilities

# Eavesdropping on Network Password Exchange

- You can sniff LAN Manager (LM) password challenge-response hashes with Cain (most used)



# KERBEROS



# Kerberos Sniffing

- Kerberos 5 sends a preauthentication packet which contains a timestamp encrypted with a key derived from the user's password
  - Offline attack on that exchange can reveal a weak password
  - Cain has an MSKerb5-PreAuth packet sniffer
- There's no simple defense against this, except using long, complex, passwords

# Unauthenticated Attacks

## Windows Authentication Sniffing Countermeasures

- Disable LM authentication. NT LAN Manager (NTLM) hashes are harder to crack. Dictionary attacks
- Pick good passwords (password complexity features)
- Do not allow dictionary password
- Use public key encryption
- Use built-in Windows IPsec to authenticate and encrypt traffic

# Unauthenticated Attacks

## Eavesdropping on Network Password Exchange

- Three authentication protocols: LM (LAN Manager) (with hash), NTLM (with encryption), Kerberos (with private or optional public key encryption)
- Attack tools: Cain, LCP, L0phtcrack, KerbSniff
  - Sniffing, brute-force cracking, dictionary cracking
  - To sniff on a switched network: ARP spoofing/poisoning to redirect traffic through attackers

# Man In The Middle Attacks

- SMBRelay and SMBProxy pass authentication hashes along, to get authenticated access to the server.
- SMB Credential Reflection Attack
- SMB Credential Forwarding Attack

<https://blogs.blackberry.com/en/2015/04/redirect-to-smb>



# MITM Attack - CAIN

- Cain: ARP Poisoning, downgrade Auth versions
- Can sniff Remote Desktop sessions, breaking their encryption
  - For Windows XP and Windows Server 2003

## Security Advisory

Remote Desktop Protocol, the Good the Bad and the Ugly

Author: Massimiliano Montoro <[mao@oxid.it](mailto:mao@oxid.it)>

Issue date: May, 28, 2005

# MITM Countermeasures

- If attacker is already on your LAN, very hard
- Use authenticated and encrypted protocols
- Enforce them with Group Policy and firewall rules
- Verify identity of remote servers with strong authentication or trusted third parties

# Unauthenticated Attacks

## Man-in-the-Middle Attacks (MITM)

- Relay legitimate client authentication exchange and gain access to the server as the client
- **SMBRelay**: Harvest usernames and password hashes from SMB traffic and import into cracking tools
- ARP spoofing and DNS redirection: force victims to connect and authenticate to malicious SMB servers
- Tools: **Cain**, **Squirtle**, **SMBRelay3**
  - Cain: redirect local traffic to itself with ARP spoofing, then downgrade clients to easier authentication dialects (sniffed, unencrypted, recorded)
- MITM countermeasures
  - Authenticate and encrypt connections between clients and servers
  - Disable NetBIOS Name Services - use DNS

# Pass-the-Hash

1. Compromise a machine
2. Dump password hashes stored in RAM
3. Use them as credentials for network services without cracking them
  - Allow to compromise the Windows domain after compromising a single machine.
  - Administrator logged into the compromised machine BEFORE the compromise, also taken

# Windows Credential Editor

A screenshot of a web browser window displaying the Amplia Security website. The URL in the address bar is <https://www.ampliasecurity.com/research/wcefaq.html>. The page content is a Frequently Asked Questions (FAQ) section about the Windows Credential Editor (WCE). The questions listed are:

- What is WCE?
- What is the current version of WCE?
- Who should use WCE?
- What Operating Systems does WCE support?
- Is WCE like cachedump?
- Is WCE like pwdump?
- Is WCE like Cain & Abel?
- Where can I find more information about how WCE works?
- Where can I find information on how to use WCE on a pentest?
- What privileges do I need to run WCE?
- How do I list NTLM credentials in memory?
- How do I change my current NTLM credentials?
- How do I create a new logon session and launch a program with new NTLM credentials?
- How can I generate NTLM hashes with WCE? (for testing purposes)
- What is 'safe mode'?
- How can I write hashes obtained by WCE to a file?
- How can I dump logon cleartext passwords with WCE?

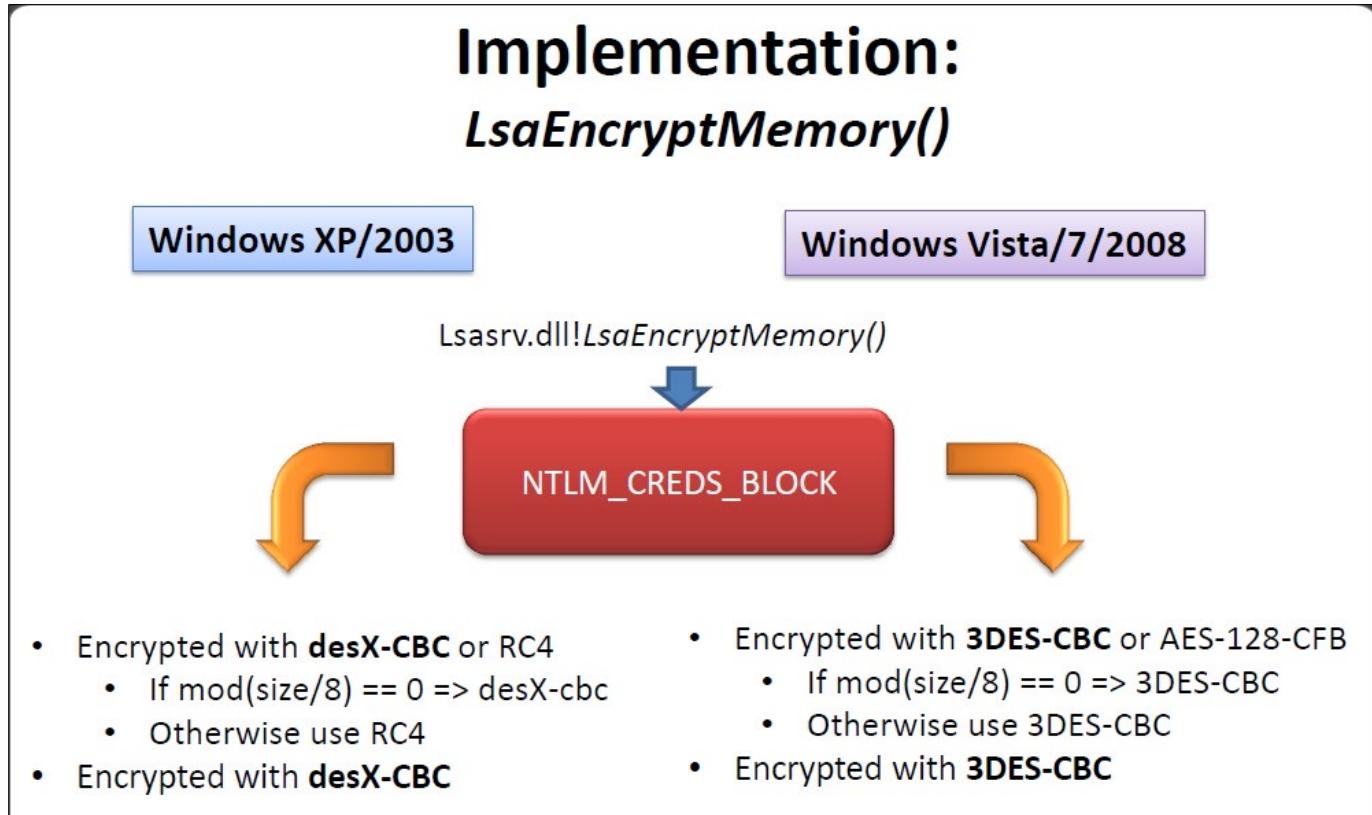
## WCE features

- Dump *in-memory* credentials of *logon sessions*
  - Lists in-memory logon sessions
    - Dumps in-memory username, domain, LM & NT hashes
      - current, future and *terminated* (...)
  - Great to ‘steal’ credentials not stored locally

## WCE features

- Single executable (*wce.exe*)
  - Easier to use, upload, etc.
- Supports
  - Windows XP
  - Windows 2003
  - **Windows Vista**
  - **Windows 7**
  - **Windows 2008**

# Passwords are Encrypted



- But the Keys are in RAM

# Pass-the-Ticket for Kerberos

- Dump existing Kerberos RAM tickets and re-use them
- WCE can replay and re-use tickets, but must compromise a host first

# Pass-the-Hash Countermeasures

- NTLM is vulnerable by design; no fix available
- Prevent intrusions in the first place, since this is a post-exploitation technique
- If possible, use two-factor authentication

# Unauthenticated Attacks

## Pass-the-Hash

- Use LM and/or NTLM hash of a user's password
  - No need to crack/brute-force the hash to cleartext password
  - Allows to gain authorized access
  - Limitations: Not all functionalities of the protocol are implemented
  - Dump/modify NTLM credentials stored in memory and replay
    - Windows Credentials Editor (WCE)
- Pass the ticket for Kerberos
  - WCE: dump Windows Kerberos tickets and reuse them

# Remote Unauthenticated Exploits

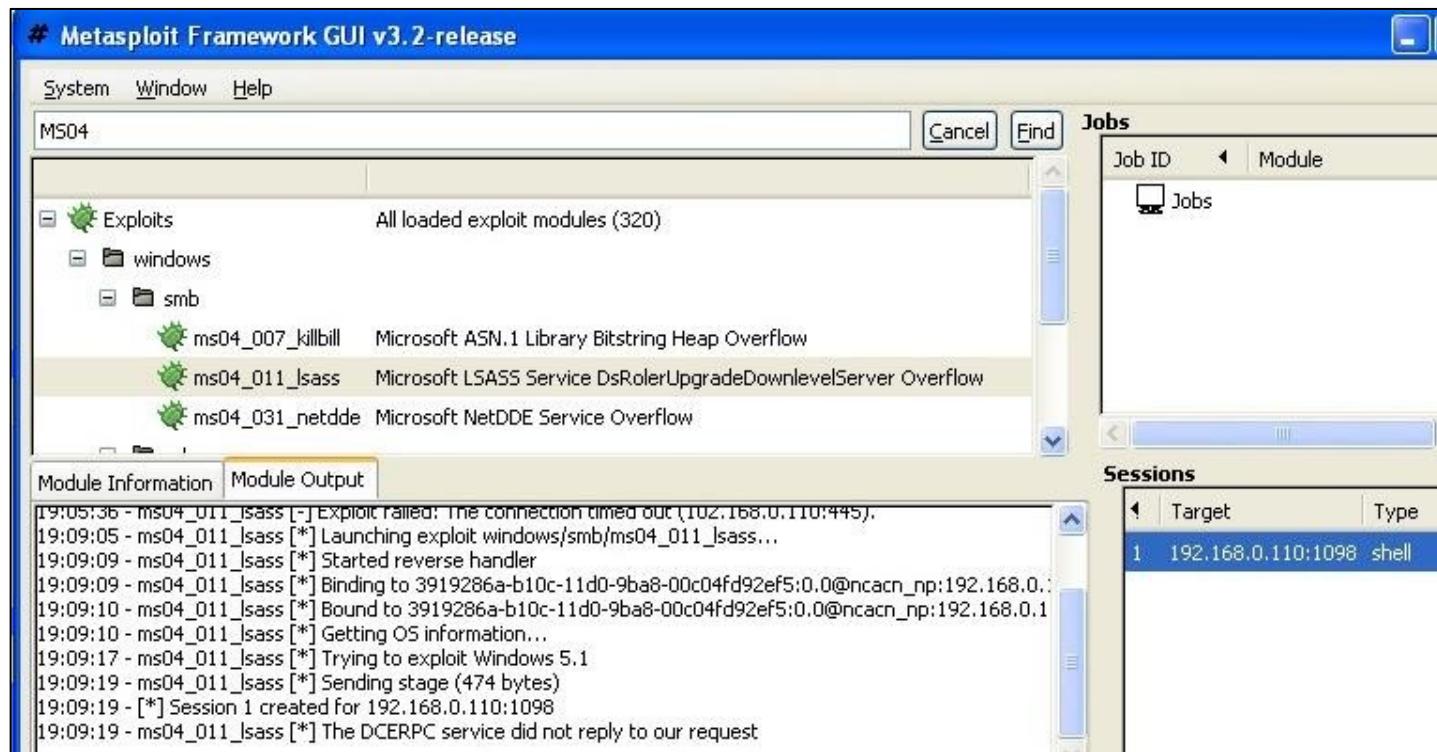
# Unauthenticated Attacks

## Remote Unauthenticated Exploits

- Flaws or misconfigurations in Windows software itself
  - TCP/UDP services → driver interface, user-mode applications (MS Office, Internet Explorer, Adobe Acrobat Reader)
- **Metaexploit**
  - Framework plus archive of exploit modules
  - Locate/search the exploit module
  - Customize exploit parameters (vendor and model of victim software), payloads (remote command shell, users, injecting prebuilt code), and options (target IP address, IDS evasion, etc.)

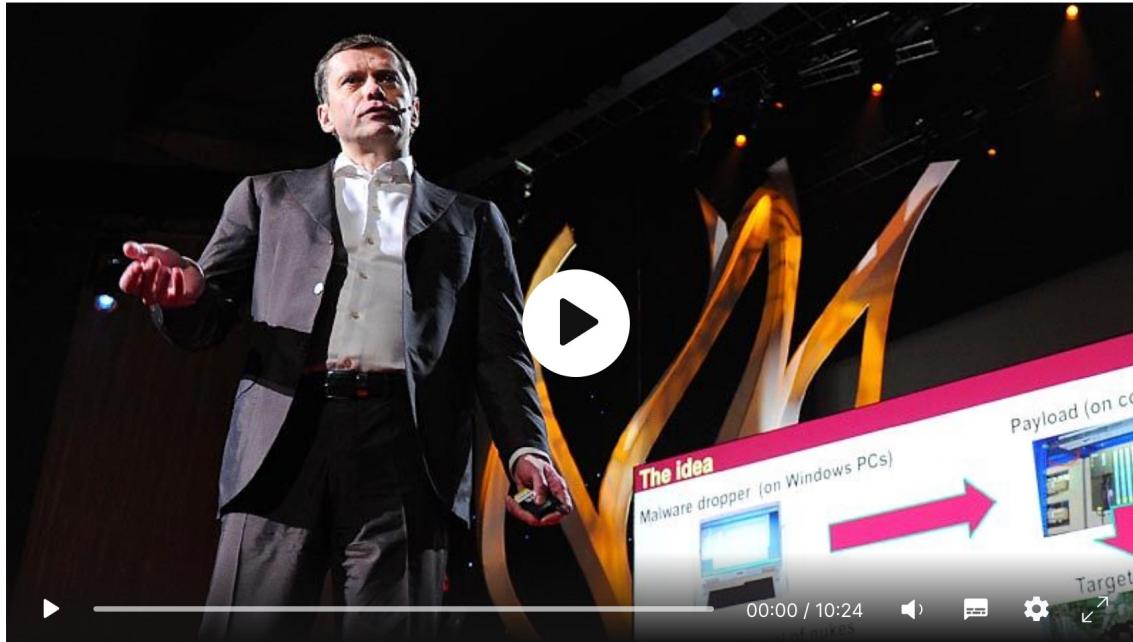
# Metasploit

- Easily exploits network services
- Typically a couple of months behind Microsoft alerts
- CORE IMPACT and Canvas are expensive, but better



# Metasploit

Metasploit includes the Print Pooler Service vulnerability exploit, used by stuxnet to attack an iranian nuclear reactor



Cracking Stuxnet, a 21st-century cyber weapon

1,717,369 views | Ralph Langner | TED2011 • March 2011

Share

Save

Like

Read transcript

When first discovered in 2010, the Stuxnet computer worm posed a baffling puzzle. Beyond its sophistication loomed a more troubling mystery: its purpose. Ralph Langner and team helped crack the code that revealed this digital warhead's final target. In a fascinating look inside cyber-forensics, he explains how -- and makes a bold (and, it turns out, correct) guess at its shocking origins.

# Network Service Exploit Countermeasures

- Apply patches quickly
- Use workarounds for unpatched vulnerabilities: disable weak services,...
- Audit, Log and monitor traffic
- Have an incident response plan: Computer Security Incident Response Team (CSIRT), a group include information security and general IT staff, representatives legal, human resources and public relations departments. Produce plan with the organization's response to a cyberattack.

# End-user Application Exploits

- End users the weakest link. Less professional on security, Poorly managed rich software ecosystem
- Worst Offenders:
  - Adobe Flash Player in browser. Display of rich media and animated content over Internet
  - Adobe PDF Reader
- Metaexploit (search /w adobe flash)

# Adobe Flash vulnerability

The screenshot shows a web browser displaying the NVD - Results page at [https://nvd.nist.gov/vuln/search/results?adv\\_search=false&form\\_type=basic&results\\_type=overview&search\\_type=last3years&query=adobe+flash](https://nvd.nist.gov/vuln/search/results?adv_search=false&form_type=basic&results_type=overview&search_type=last3years&query=adobe+flash). The page header includes the NIST logo, the Information Technology Laboratory, and the NVD logo. The main content area displays search results for 'adobe flash' with 640 matching records, showing matches 1 through 20. The results table includes columns for Vuln ID, Summary, and CVSS Severity. The first result, CVE-2018-4878, is highlighted. The bottom of the screen shows a taskbar with various icons and system status.

NVD - Results

Sicuro | https://nvd.nist.gov/vuln/search/results?adv\_search=false&form\_type=basic&results\_type=overview&search\_type=last3years&query=adobe+flash

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD MENU

VULNERABILITIES SEARCH AND STATISTICS

## Q Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

There are **640** matching records.  
Displaying matches **1** through **20**.

1	2	3	4	5	6	7	8	9	10	>	>>
---	---	---	---	---	---	---	---	---	----	---	----

**Vuln ID** **Summary** **CVSS Severity**

**CVE-2018-4878** A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

V3: **9.8 CRITICAL**  
V2: **7.5 HIGH**

Published: February 06, 2018: 04:29:00 PM -05:00

IT 08:21 26/03/2018

# End-user Application Exploits

- Countermeasures
  - Use a firewall to limit outbound connections
  - Patches
  - Antivirus, particularly on email-attach
  - Run with least privilege; if browsing Internet, never as Administrator
  - Use software security options, such as read email in plaintext
  - Configure MS Office to very high macro security

# Device Driver Exploits

- There were buffer overflows in wireless device drivers for MS
- It is possible to own every vulnerable machine in range just with a **beacon frame**
- NO connection required by the victim



Next: [Contents](#) [Contents](#)

## Exploiting 802.11 Wireless Driver Vulnerabilities on Windows

Nov, 2006

Johnny Cache [johnycsh@802.11mercenary.net](mailto:johnycsh@802.11mercenary.net)

H D Moore [hdm@metasploit.com](mailto:hdm@metasploit.com)

skape [mmiller@hick.org](mailto:mmiller@hick.org)

# Unauthenticated Attacks

## Device Driver Exploits

- Windows wireless: within physical proximity to a rogue access point beaconsing malicious packets
- MS Plug and play compatibility
  - Vast number of vendor drivers
- Execution in highly privileged kernel mode → one weak driver implies total compromise
- **Metaexploit** WIFI exploit modules: e.g. oversized wireless beacon frame → remote code execution

# Driver Exploit Countermeasures

- Apply vendor patches
- Disable wireless networking at high concentration of Aps, and other high-risk environments
- Use driver signing (trusted signatures on kernel-mode software). But does Microsoft really thoroughly test drivers? Eternal Blu?
- "Future" User-Mode Driver Framework (UMDF)
  - Now adopted (V2)

# User-Mode Driver Framework

From Wikipedia, the free encyclopedia

**User-Mode Driver Framework (UMDF)** is a device-driver development platform first introduced with Microsoft's Windows 7 system, and is also available for Windows XP. It facilitates the creation of drivers for certain classes of devices.

## Contents [hide]

- [1 Overview](#)
- [2 Version history](#)
- [3 Architecture](#)
- [4 See also](#)
- [5 References](#)
- [6 External links](#)

## Overview [edit]

Standard device drivers can be difficult to write because they must handle a very wide range of system and device state in a multithreaded software environment. Badly written device drivers can cause severe damage to a system (e.g., BSOD).

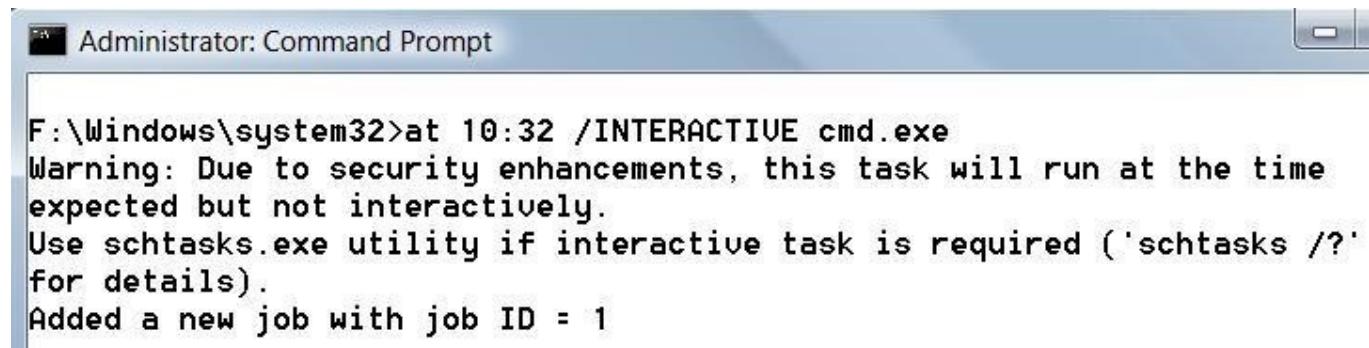
# Authenticated Attacks

# Privilege Escalation

- Once a user can log on to a Windows machine as a Guest or Limited User, the next goal is to escalate privileges to Administrator or SYSTEM
  - getadmin.exe was an early exploit
  - There have been many others, including a **buffer overrun** MS03-013

# SYSTEM status

- The SYSTEM account is more powerful than the Administrator account
- The Administrator can schedule tasks to be performed as SYSTEM
  - It's more complicated in Vista, but still possible



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered was "F:\Windows\system32>at 10:32 /INTERACTIVE cmd.exe". The output message indicates a warning about security enhancements: "Warning: Due to security enhancements, this task will run at the time expected but not interactively. Use schtasks.exe utility if interactive task is required ('schtasks /?' for details). Added a new job with job ID = 1".

```
F:\Windows\system32>at 10:32 /INTERACTIVE cmd.exe
Warning: Due to security enhancements, this task will run at the time
expected but not interactively.
Use schtasks.exe utility if interactive task is required ('schtasks /?'
for details).
Added a new job with job ID = 1
```

# Preventing Privilege Escalation

- Keep Win machines patched
- Restrict interactive logon to trusted accounts
  - Run **Security Policy** applet, secpol.msc
  - Local Policies → User Right Assignment → Deny log on locally

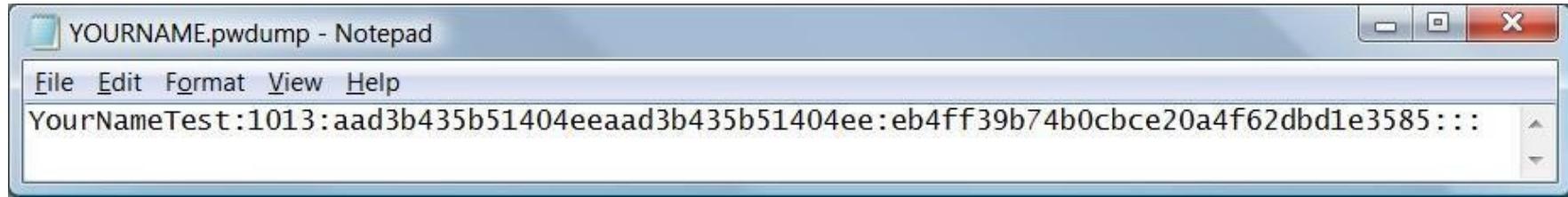


# Extracting and Cracking Passwords

- Once Administrator-equivalent status has been obtained on one machine
- Attackers often want to penetrate deeper into the network, so they want passwords
- Post-exploitation: Disable Windows firewall

# Grabbing the Password Hashes

- Local Users in the Windows Security Accounts Manager (SAM) under NT4 and earlier
- Domain in the Active Directory (Windows 2000 and greater) domain controllers (DCs)
- The SAM contains the usernames and hashed passwords of all users
  - The counterpart of the /etc/passwd file from the UNIX world



# Obtaining the Hashes

- NT4 and earlier stores password hashes in %systemroot%\system32\config\SAM
  - It's locked as long as the OS is running
  - It's also in the Registry key HKEY\_LOCAL\_MACHINE\ SAM
- On Windows 2000 and greater domain controllers, password hashes are kept in the Active Directory
  - %windir%\WindowsDS\ntds.dit

# How to Get the Hashes

- Easy way: Just use Cain
- Cracker tab, right-click, "Add to List"



# How Cain Works

- Injects a DLL into a highly privileged process in a running system
- That's how pwdump, Cain, and Ophcrack do it

# Other Ways to Get the Hashes

- Boot the target system to an alternate OS and copy the files to removable media
- Copy the backup of the SAM file created by the Repair Disk Utility
  - But this file is protected by SYSKEY encryption, which makes it harder to crack (perhaps impossible)
- Sniff Windows authentication exchanges

# pwdump2 Countermeasures

- There is no defense against pwdump2, 3, 4, Cain, Ophcrack, etc.
- But the attacker needs local Administrative rights to use them.

# Cracking Passwords

- The hash is supposed to be really difficult to reverse
  - NTLM hashes are really hard to break
  - But Windows XP and earlier still use LM Hashes for backwards compatibility, in addition to NTLM hashes
  - They are turned off by default in Vista & Win 7

# No Salt!

- To make hashing stronger, add a random "Salt" to a password before hashing it
- Windows doesn't salt its hash!
- Two accounts with the same password hash to the same result, even in Windows 7 Beta!
- This makes it possible to speed up password cracking with precomputed Rainbow Tables

# Demonstration

- Here are two accounts on a Windows 7 Beta machine with the password 'password'

User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
✗ Testuser	* empty	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C
✗ Testuser2	* empty	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C

- This hash is from a different Windows 7 Beta machine

✗ Testuser3	* empty	*	AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C
-------------	---------	---	------------	----------------------------------

# Linux Salts its Hashes

```
student@student-desktop:~$ sudo useradd -d /home/testuser1 -m testuser1
[sudo] password for student:
student@student-desktop:~$ sudo passwd testuser1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@student-desktop:~$ sudo useradd -d /home/testuser2 -m testuser2
student@student-desktop:~$ sudo passwd testuser2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
student@student-desktop:~$ sudo tail -2 /etc/shadow
testuser1:$1$zW1NMALV$kX5/VdKPX3HFUjnf2Fv301:14132:0:99999:7:::
testuser2:$1$EHNCIOxU$0nQusuZW0233b3VfHhTMS0:14132:0:99999:7:::
```

# NTLM Uses MD4 Hashing

The NTLM response is calculated as follows (see [Appendix D](#) for a sample Java implementation):

1. The MD4 message-digest algorithm (described in [RFC 1320](#)) is applied to the Unicode mixed-case password. This results in a 16-byte value - the NTLM hash.
2. The 16-byte NTLM hash is null-padded to 21 bytes.
3. This value is split into three 7-byte thirds.
4. These values are used to create three DES keys (one from each 7-byte third).
5. Each of these keys is used to DES-encrypt the challenge from the Type 2 message (resulting in three 8-byte ciphertext values).
6. These three ciphertext values are concatenated to form a 24-byte value. This is the NTLM response.

# Types of Hashes

The screenshot shows a web browser window with the URL [www.101hacker.com/2010/12/\\_hashes-and-seeds-know-basics.html](http://www.101hacker.com/2010/12/_hashes-and-seeds-know-basics.html) in the address bar. The main content is a blog post titled "Different Types of Hashes and Salts". Below the title, it says "Posted by John (Admin) on 2:21 AM | Tags : *Articles, Cryptography, How to, tutorials*".

## Different Types of Hashes and Salts

*Posted by John (Admin) on 2:21 AM | Tags : Articles, Cryptography, How to, tutorials*

- All fast hashes are **WRONG** for passwords
  - SHA, MD, CRC
- You need a **SLOW** algorithm
  - Ubuntu & Mac OS X hash thousands of times

# Brute Force v. Dictionary

- There are two techniques for cracking passwords
  - Brute Force
    - Tries all possible combinations of characters
  - Dictionary
    - Tries all the words in a word list, such as able, baker, cow...
    - May try variations such as ABLE, Able, @bl3, etc.

# Password-Cracking Countermeasures

- Strong passwords – not dictionary words, long, complex
- Add non-printable ASCII characters like (NUM LOCK) ALT255 or (NUM LOCK) ALT-129

# Ways to Speed Cracks

- Rainbow tables trade time for memory with precomputed hashes
- Elcomsoft Distributed Password Recovery
  - Uses many machines together, and their graphics cards, to make cracking 100x faster

# Authenticated Attacks

## Cracking passwords

- Hashing – one-way encipherment
- Offline password guessing
  - Hashing algorithm → hash for a list of possible values (e.g. dictionary) → compare with hashed password from pwdump → matched means cracked
  - Account lockout is not an issue
- Weak hash algorithm
  - Stronger hashing vs. salting (random value to prevent precomputed hash tables, rainbow tables, that speedup cracking)
- Smart guessing
  - Dictionary, brute-force, precomputed hash tables
  - **Project Rainbow Crack**: precomputed LM hash table for \$120 with 24GB in 6 DVDs
- Tools
  - CLI: **John The Ripper Jumbo**
  - GUI: **LCP**, **Cain** (dictionary, brute-force, LM/NTLM hashes, sniffed, rainbow tables), **Ophcrack**, **L0phtcrack**, **Elcomsoft**
- Processing time
  - Entropy ~ unpredictability

# High-entropy passwords

- Use password managers like LastPass or Built-in Google Chrome or automatic password generator (built-in in iPhones)
- Can we trust secure vaults?

## LastPass Hack Victims Lose \$4.4M in a Single Day

More than \$35 million has been stolen in total, according to recent reports.

By Oliver Knight Oct 30, 2023 at 4:04 p.m.



# Dumping Cached Passwords

- Local Security Authority (LSA) Secrets
  - Contains unencrypted logon credentials for external systems
  - Available under the Registry subkey of HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets
  - Encrypted when the machine is off, but decrypted and retained in memory after login

# Contents of LSA Secrets

- Service account passwords in *plaintext*.
  - Accounts in external domains
- Cached password hashes of the last ten users to log on to a machine
- FTP and web-user plaintext passwords
- Remote Access Services (RAS) dial-up account names and passwords
- Computer account passwords for domain access

# Win XP Password in LSA Secrets

The screenshot shows the Cain & Abel tool interface. The title bar says "Cain". The menu bar includes File, View, Configure, Tools, and Help. The toolbar contains icons for Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, and Wireless. Below the toolbar is a tab bar with Decoders selected, followed by Network, Sniffer, Cracker, Traceroute, CCDU, and Wireless. The main window displays a list of password types on the left and their corresponding hex dumps on the right. The list includes Cached Passwords, Protected Storage, LSA Secrets, Wireless Passwords, IE7 Passwords, Windows Mail Passwords, Dialup Passwords, Edit Boxes, Enterprise Manager, and Credential Manager. The LSA Secrets section shows the following output:

```
===== Cain's LSA Secrets Dumper =====
0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantAccount
55 00 31 00 2B 00 33 00 58 00 78 00 46 00 47 00 U.1.+.3.X.x.F.G.
4A 00 49 00 33 00 34 00 50 00 62 00 00 00 J.I.3.4.P.b...
0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantSID
01 05 00 00 00 00 00 05 15 00 00 00 93 E3 62 48 .....bh
93 31 DA 1C 07 E5 3B 2B E8 03 00 00 .1....;+....
20ed87e2-3b82-4114-81f9-5e219ed4c481-SALEMHELPACCOUNT
DefaultPassword
50 00 40 00 73 00 73 00 77 00 30 00 72 00 64 00 P.@.s.s.w.0.r.d.
```

# Previous Logon Cache Dump

- If a domain member cannot reach the domain controller, it performs an offline logon with cached credentials
- The last ten domain logons are stored in the cache, in an encrypted and hashes form
- The tool CacheDump can reverse the encryption and get the hashed passwords

# CacheDump Results

```
cachedump.exe
```

```
domadmin1:0E9A658F6132E709ED673458387E6892:work:work.comp.corp  
entadmin1:19E8B953689EFBC3222ABC599F835856:comp:comp.corp
```

- John the Ripper can crack these hashes with brute-force and dictionary attacks

```
> john -format:mscash hashes.txt
```

# Windows Credential Editor

- Extracts cleartext login password from RAM
- No hash-cracking required
- BUT you only get currently logged-on users
  - Or sometimes users who were logged on but have now logged off

# Previous Logon Cache Dump Countermeasures

- There's not much you can do, Microsoft offers a patch but it doesn't help much
  - Microsoft KB Article ID Q184017
- You need Administrator or SYSTEM privileges to get the hashes
- Avoid getting admin-ed in the first place

# Previous Logon Cache Dump

## Countermeasures

- Local Admin rights can lead to compromise of other accounts
- Avoid using high privileged domain accounts to log on local machines (e.g. to start services)
- Domain Admin should avoid RDP connections
- You can change the Registry value to eliminate the cached credentials
  - But then users won't be able to log in when a domain controller is not accessible

# Remote Control and Back Doors

- Back doors: services enabling remote control
- Command-line Remote Control Tools
- Netcat for Windows
  - Use this syntax to listen on port 8080, and execute cmd

```
C:\>nc -l -e cmd.exe -p 8080
```

- Add `-d` for stealth mode (no interactive console)
- Obviously this is very dangerous—remote control with no logon

# Connecting to the nc Listener

- On another machine connect with
  - TELNET /P 8080

```
L:\Documents and Settings\Sam>telnet 192.168.11.2 8080
```

- You get a shell on the other machine



A screenshot of a Microsoft Windows Telnet window. The title bar reads "Telnet 192.168.11.2". The window displays the following text:  
Microsoft Windows [Version 6.0.6000]  
Copyright (c) 2006 Microsoft Corporation. All rights reserved.  
C:\nc>dir

# PsExec et al.

- SMB on TCP 139 or 445
- From SysInternals (Microsoft.com)
- Allows remote code execution (with a username and password)

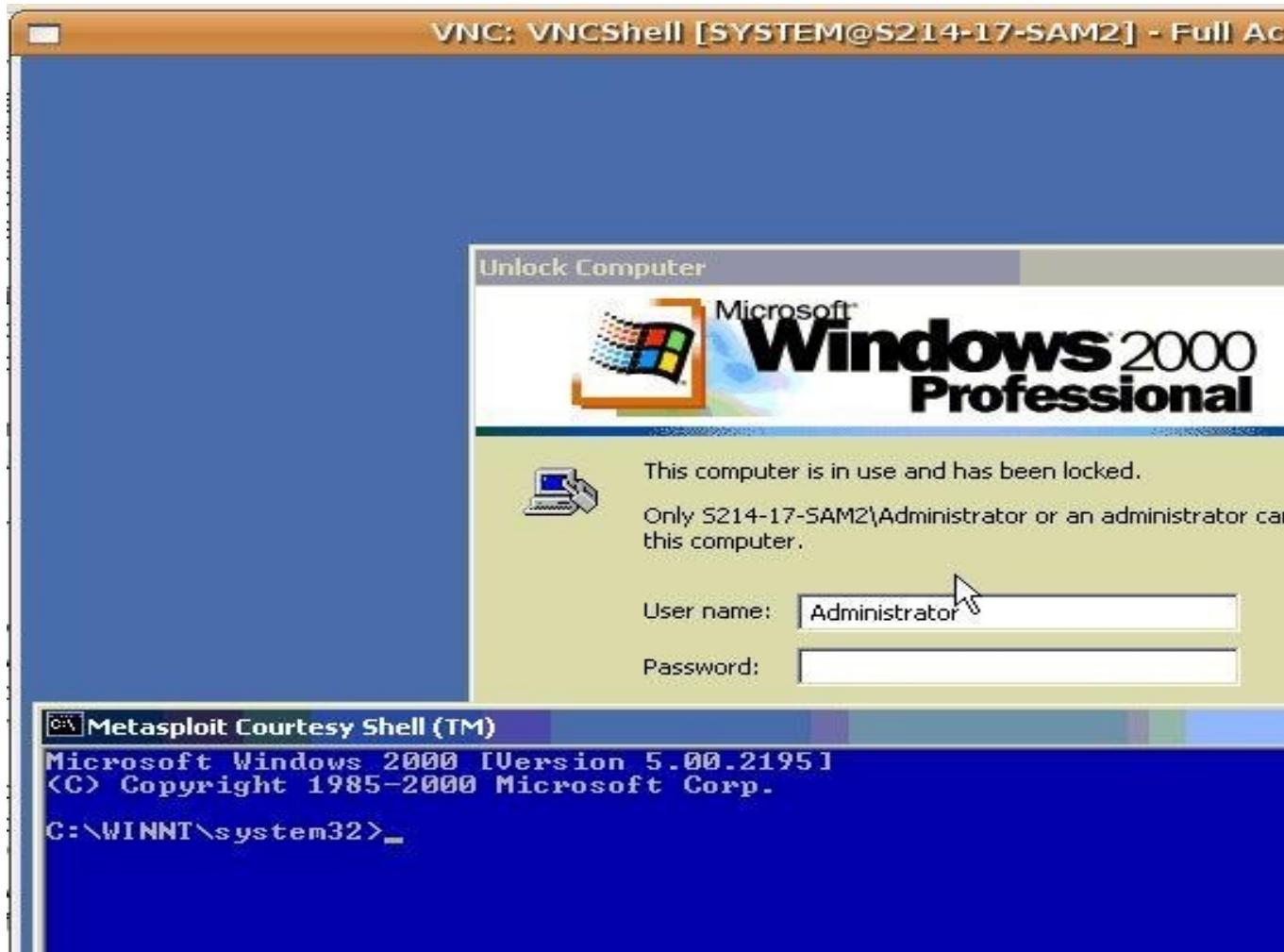
```
c:\>psexec \\10.1.1.1 -u Administrator -p password -s cmd.exe
```

- Metaexploit Framework: a large array of backdoor payloads to spawn command-line shells bound to listening ports, etc.

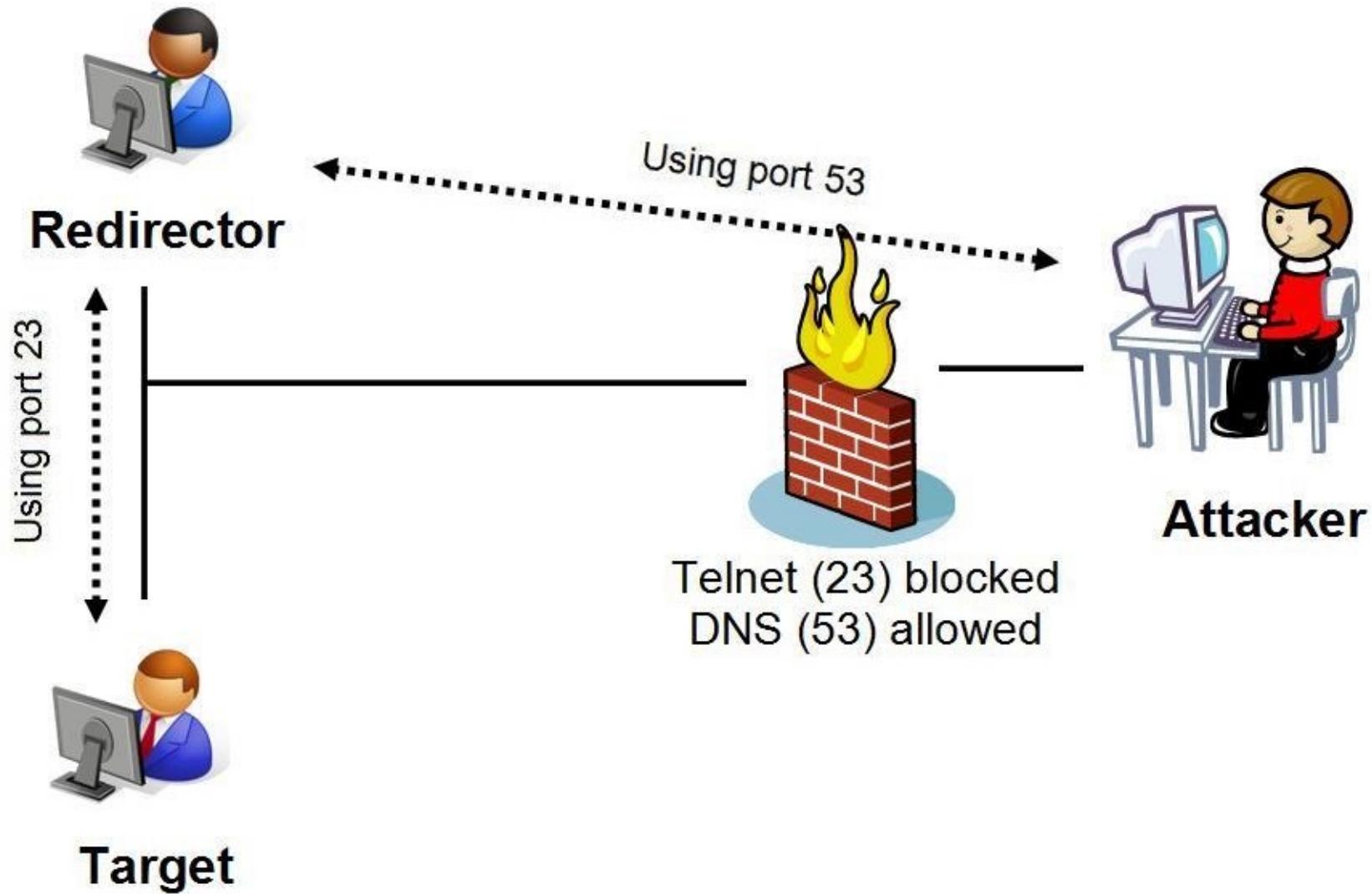
# Graphical Remote Control

- The Windows Built-in Terminal Services (aka Remote Desktop) listens on port 3389
  - It's not on by default
- Virtual Network Control (VNC) is free and very used for graphic remote control
  - Can easily be installed remotely

# VNC as used in MetaSploit

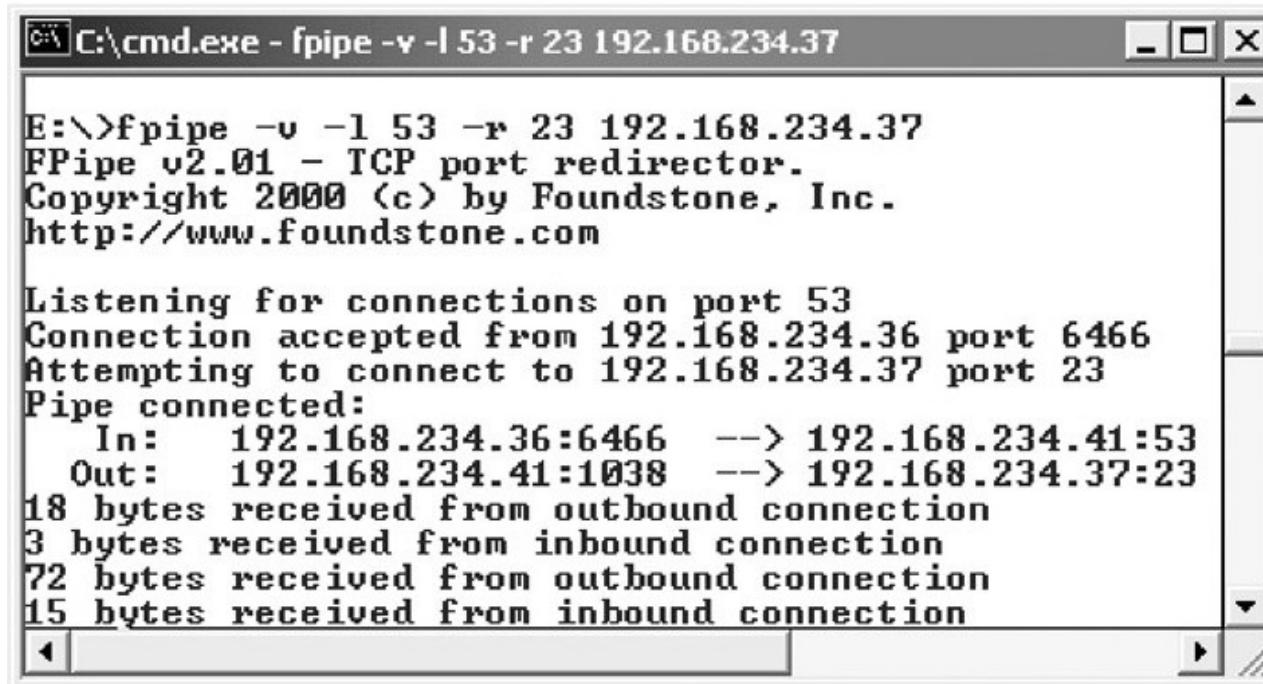


# Port Redirection



# Port Redirection

- Fpipe is a port redirection tool from McAfee



```
C:\cmd.exe - fpipe -v -l 53 -r 23 192.168.234.37
E:\>fpipe -v -l 53 -r 23 192.168.234.37
FPipe v2.01 - TCP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Listening for connections on port 53
Connection accepted from 192.168.234.36 port 6466
Attempting to connect to 192.168.234.37 port 23
Pipe connected:
  In:  192.168.234.36:6466  --> 192.168.234.41:53
  Out: 192.168.234.41:1038  --> 192.168.234.37:23
18 bytes received from outbound connection
3 bytes received from inbound connection
72 bytes received from outbound connection
15 bytes received from inbound connection
```

# Covering Tracks

- Once intruders have Administrator or SYSTEM-equivalent privileges, they will:
  - Hide evidence of intrusion
  - Install backdoors
  - Hide a toolkit to use for regaining control in the future and to use against other systems

# Disabling Auditing

- The auditpol /disable command will stop auditing
- Auditpol /enable will turn it back on again
  - Auditpol is included in Vista
  - Part of the Resource Kit for earlier versions (XP, NT, 2000 Server)

# Clearing the Event Log

- ELsave – command-line log clearing tool
  - Written for Windows NT

# Hiding Files

- Attrib +h filename
  - Sets the Hidden bit, which hides files somewhat
- Alternate Data Streams
  - Hide a file within a file
  - A NT feature designed for compatibility with Macintosh

# Demonstration of ADS

```
Command Prompt

F:\Users\Sam>echo "haha" > original.txt

F:\Users\Sam>echo "12345678901234567890" > original.txt:more.txt

F:\Users\Sam>type original.txt
"haha"

F:\Users\Sam>type original.txt:more.txt
The filename, directory name, or volume label syntax is incorrect.

F:\Users\Sam>notepad original.txt:more.txt
```

# ADS With Binary Files

- You need the POSIX *cp* utility (in the Resource Kit)
- To detect alternate data streams, use LADS or Foundstone's SFIND
- To delete an ADS, copy the file to a FAT partition and then back to NTFS

# Cp example

- The intruder wants to hide netcat

```
C: \>cp nc.exe oso001.009:nc.exe
```

- An intruder wants to get netcat

```
C: \>cp oso001.009:nc.exe nc.exe
```

- To execute a hidden file

```
start oso001.009:nc.exe
```

# Rootkits

- Rootkits are the best way to hide files, accounts, backdoors, network connections, etc. on a machine
- More on rootkits in a dedicated chapter

WHIPS (Windows Host IPS) X

Sicuro | https://sourceforge.net/projects/whips/

SOURCEFORGE

Browse Blog Deals Help Create Join Login

Articles Cloud Storage Business VoIP Internet Speed Test

Search for software or solutions

 Singularity UNIVERSITY

Disruption Workshop.

20-21 GIUGNO 2016 Milano

Un corso pratico per generare idee, innovare processi, prodotti o servizi: non mancare!

• • • Registrati

Advertisement - Report

Home / Browse / Security & Utilities / Security / WHIPS (Windows Host IPS)

# WHIPS (Windows Host IPS)

Status: Beta Brought to you by: rbattistoni

★★★★★ 1 Reviews

Downloads: 0 This Week

Last Update: 2015-08-06

Download Get Updates Share This

Windows

Summary Files Reviews Support Wiki Discussion Code Cvs

WHIPS (Windows Host Intrusion Prevention System) is a Host Intrusion Prevention System for Windows NT/XP/2003. WHIPS uses the system call interposition technics and it is developed as a kernel module.

GFI OneGuard™

Antivirus, Patch Management and Asset Tracking in one solution

Get latest updates about Open Source Projects, Conferences and News.

Sign Up

No, Thank you

IT 05/04/2020 07:27



European Symposium on Research in Computer Security

ESORICS 2004: Computer Security – ESORICS 2004 pp 352–368 | Cite as

Log in

# A Host Intrusion Prevention System for Windows Operating Systems

Authors

Authors and affiliations

Roberto Battistoni, Emanuele Gabrielli, Luigi V. Mancini

Conference paper



Part of the [Lecture Notes in Computer Science](#) book series (LNCS, volume 3193)

- Inst
- Rea
- Ow
- Loc

Learn  
subscr

Cite p

## Abstract

We propose an intrusion prevention system called WHIPS that controls, entirely in kernel mode, the invocation of the critical system calls for the Windows OS security. WHIPS is implemented as a kernel driver, also called kernel module, by using kernel structures of the Windows OS. It is able to intercept all the system calls and to verify if they are valid or not according to the kernel algorithm. If the answer is negative, it will prevent the system call from being executed. This way, it is possible to prevent attacks without source code changes or recompilation. A working prototype has been developed and tested on a Windows XP system.

We use cookies to improve your experience with our site. [More information](#)

[Accept](#)

# General Countermeasures to Authenticated Compromise

- Once a system has been compromised with administrator privileges, you should just reinstall it completely
  - You can never be sure you really found and removed all the backdoors
- But if you want to clean it, cover four areas: Files, Registry keys, Processes and Network ports.

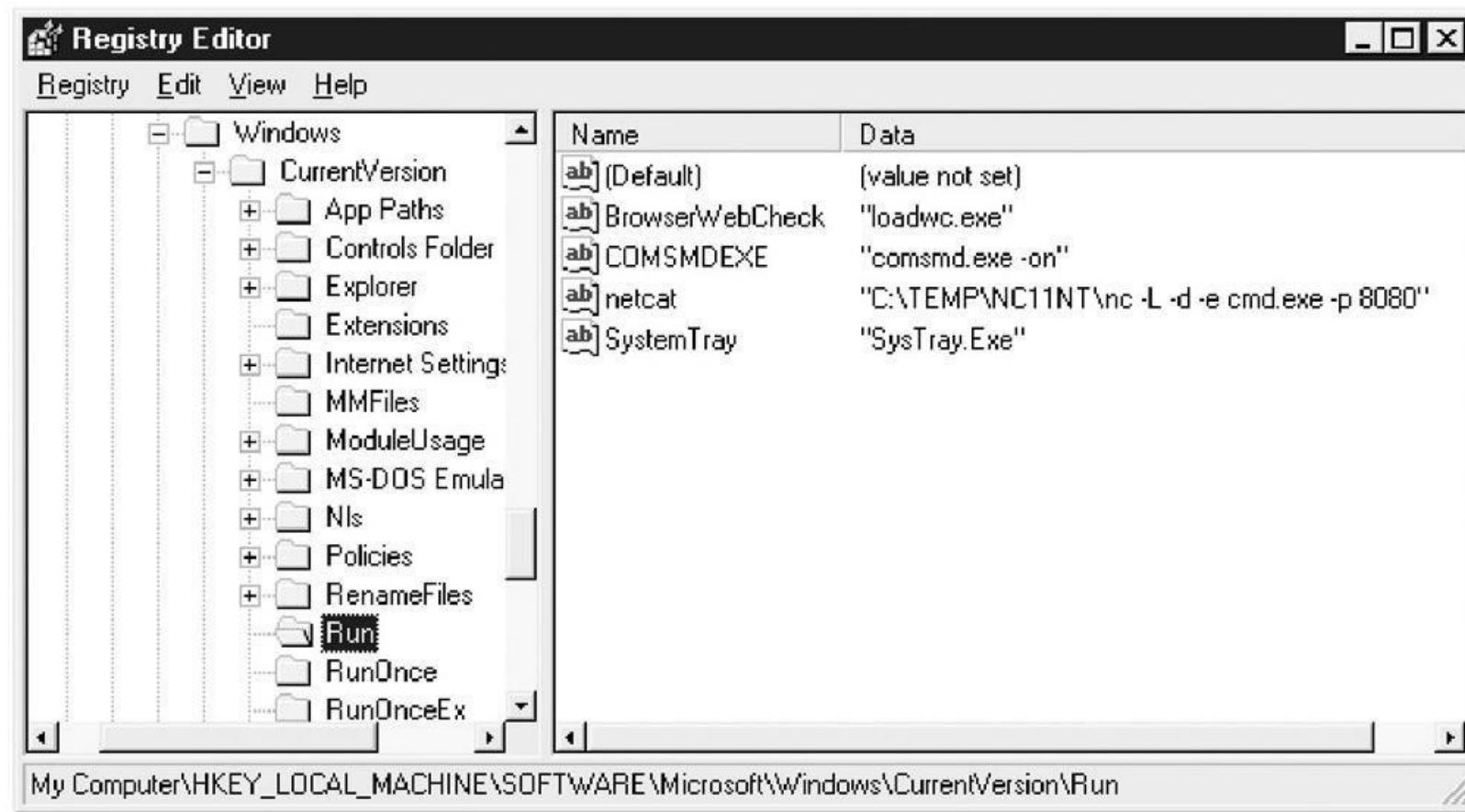
# Suspicious Files

- Known dangerous filenames like nc.exe
- Run antivirus software
- Use Tripwire or other tools that identify changes to system files

# Suspicious Registry Entries

- Look for registry keys that start known backdoors like"
  - HKEY\_USERS\.DEFAULT\Software\ORL\WINVNC3
  - HKEY\_LOCAL\_MACHINE\SOFTWARE\Net Solutions\NetBus Server
- Use *reg delete* to remove them

# A Back-Door Favorite: Autostart Extensibility Points (ASEPs)



# Suspicious Processes

- Malicious process with CPU utilization
- End process or kill to stop
- Check scheduler queue: schtasks, task scheduler

# Suspicious Ports

- Use **netstat -aon** to view network connections

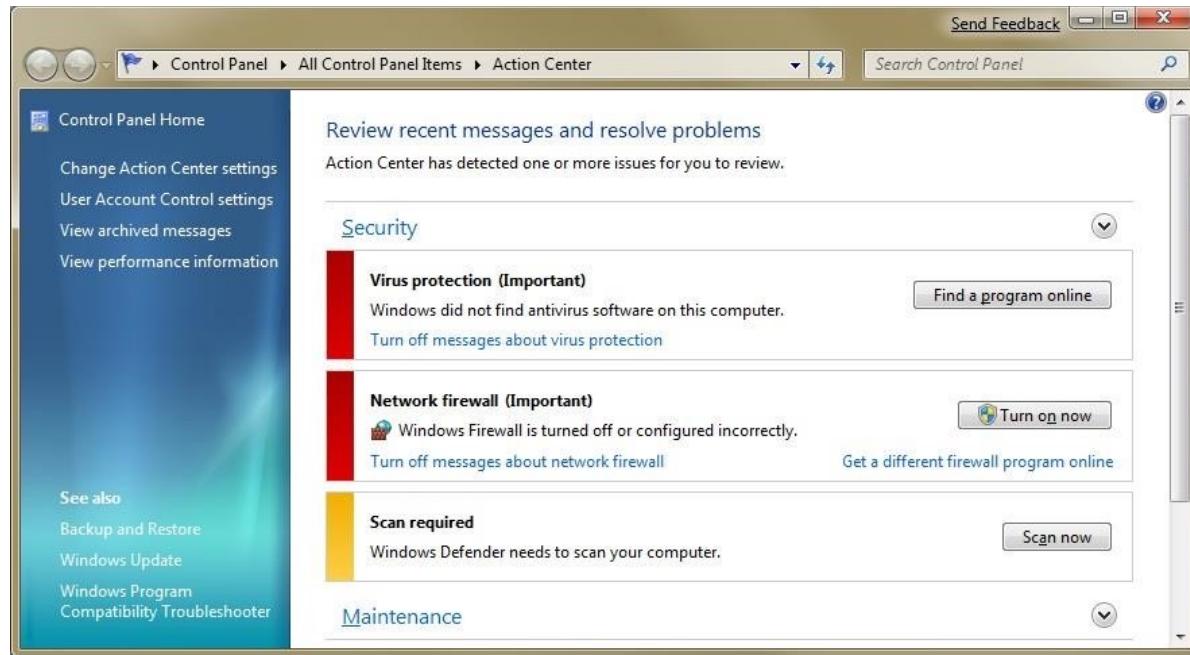
```
F:\Users\Sam>netstat -aon
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	816
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	1160
TCP	0.0.0.0:12121	0.0.0.0:0	LISTENING	3840
TCP	0.0.0.0:12122	0.0.0.0:0	LISTENING	3840
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	504

# Windows Security Features

- Windows Firewall
- Automated Updates
- Security Center: for consumers, not IT pros



# Windows Security Features

- Group Policy tool
  - Allows security policy settings in domains
- Microsoft Security Essentials
  - Free antivirus, included in Win 8 by default
- EMET (Enhanced Mitigation Experience Toolkit)
  - Allows the user to configure DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization)

# Data Execution Prevention

Data Execution Prevention (DEP) is a system-level memory protection feature that is built into the operating system starting with Windows XP and Windows Server 2003. DEP enables the system to mark one or more pages of memory as non-executable. Marking memory regions as non-executable means that code cannot be run from that region of memory, which makes it harder for the exploitation of buffer overruns.

DEP prevents code from being run from data pages such as the default heap, stacks, and memory pools. If an application attempts to run code from a data page that is protected, a memory access violation exception occurs, and if the exception is not handled, the calling process is terminated.

DEP is not intended to be a comprehensive defense against all exploits; it is intended to be another tool that you can use to secure your application.

## How Data Execution Prevention Works

If an application attempts to run code from a protected page, the application receives an exception with the status code **STATUS\_ACCESS\_VIOLATION**. If your application must run code from a memory page, it must allocate and set the proper virtual [memory protection](#) attributes. The allocated memory must be marked **PAGE\_EXECUTE**, **PAGE\_EXECUTE\_READ**, **PAGE\_EXECUTE\_READWRITE**, or **PAGE\_EXECUTE\_WRITECOPY** when allocating memory. Heap allocations made by calling the **malloc** and **HeapAlloc** functions are non-executable.

Applications cannot run code from the default process heap or the stack.

DEP is configured at system boot according to the no-execute page protection policy setting in the boot configuration data. An application can get the current policy setting by calling the [GetSystemDEPPolicy](#) function. Depending on the policy setting, an application can change the DEP setting for the current process by calling the [SetProcessDEPPolicy](#) function.

# When ASLR makes the difference

Rate this article ★★★★☆



swiat March 12, 2014

[Share 0](#)[0](#)[in 0](#)[0](#)

We wrote several times in this blog about the importance of enabling *Address Space Layout Randomization* mitigation (ASLR) in modern software because it's a very important defense mechanism that can increase the cost of writing exploits for attackers and in some cases prevent reliable exploitation. In today's blog, we'll go through ASLR one more time to show in practice how it can be valuable to mitigate two real exploits seen in the wild and to suggest solutions for programs not equipped with ASLR yet.

## Born with ASLR

ASLR mitigation adds a significant component in exploit development, but we realized that sometimes a single module without ASLR loaded in a program can be enough to compromise all the benefits at once. For this reason recent versions of most popular Microsoft programs were natively developed to enforce ASLR automatically for every module loaded into the process space. In fact [Internet Explorer 10/11 and Microsoft Office 2013](#) are designed to run with full benefits of this mitigation and they [enforce ASLR randomization natively without any additional setting on Win7 and above](#), even for those DLLs not originally compiled with /DYNAMICBASE flag. So, customers using these programs have already a good native protection and they need to take care only of other programs potentially targeted by exploits not using ASLR.

## ASLR effectiveness in action

Given the importance of ASLR, we are taking additional efforts to close gaps when ASLR bypasses arise in security conferences from time to time or when they are found in-the-wild used in targeted attacks. The outcome of this effort is to strengthen protection also for previous versions of Microsoft OS and browser not able to enforce ASLR natively as IE 10/11 and Office 2013 can do. Some examples of recent updates designed to break well-known ASLR bypasses are shown in the following table.

# Windows Security Features

- Encryption: BitLocker and Encrypting File System
- EFS: Symmetric key itself encrypted by public key of a user and stored as an attribute of the file; symmetric key decrypted by a private key first before decrypting the file
- Protection from booting alternative OS, files in remote server.
- Recovery Agent
- Employees leave the organization - privacy issues
- Primary vulnerability: Recovery Agent account

# Windows Security Features

- EFS encrypts folders
  - Win 2000 and Server 2003 also set the Local administrator account as the Default Recovery Agent, which was a serious security hole; but this was fixed since Win XP
- BitLocker encrypts the whole hard drive
- In Windows 7, BitLocker To Go can encrypt removable USB devices

# Video: Hacking BitLocker

## Lest We Remember: Cold Boot Attacks on Encryption Keys

J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten



# Key Management

- [https://www.youtube.com/watch?v=JDaicPlgn9U&ab\\_channel=pucitp](https://www.youtube.com/watch?v=JDaicPlgn9U&ab_channel=pucitp)
- Cold Boot Countermeasures: separate the key physically, removable external module

# Least Privilege

- Most Windows users use an Administrative account all the time
- Many Win Services run under Administrative privileges
  - Very poor for security, but convenient
  - For XP, 2003, and earlier: log on as a limited user, use run as to elevate privileges as needed

# Windows Security Features (1/3)

- Windows Firewall
  - “Exception” metaphor for permitted applications
  - All inbound connections are blocked by default
- Automated Updates
- Security Center
  - For consumers, not IT pros
- Security Policy and Group Policy
  - For stand-alone computer and large number of systems
- Microsoft Security Essentials
  - Antimalware: real-time protection, system scanning and cleaning, rootkit protection, network inspection, automatic updates
- The Enhanced Mitigation Experience Toolkit
  - Managing mitigation technologies in Windows: DEP (Data Execution Prevention), ASLR (Address Space Layout Randomization)

# Windows Security Features (2/3)

- Bitlocker and encryption file system
  - EFS (Encryption File System)
    - Symmetric key itself encrypted by public key of a user and stored as an attribute of the file; symmetric key decrypted by a private key first before decrypting the file
  - BDE (Bitlock Drive Encryption)
    - Encrypt the entire volumes and store the key securely
    - Cold boot attack: cool DRAM chips to increase the time before the key is flushed from volatile memory
    - Countermeasures: separate the key physically, removable external module
- Windows Resource Protection (WRP)
  - Protect files and registry values from modifications by ACL
- Integrity levels
  - Mandatory Integrity Control (MIC): actions - privileges 105

# Windows Security Features (3/3)

- Data Execution Protection (DEP)
  - Mark portions of memory nonexecutable to prevent buffer overflow attacks
- Windows service hardening
  - Service resource isolation, least privilege services, service refactoring, restricted network access, session 0 isolation
- Compiler-based enhancements
  - Compile-time under-the-hood features, not configurable by admins or users: buffer security check (GS), ASLR, SafeSEH

# Center for Internet Security - nonprofit

The screenshot shows the homepage of the CIS Center for Internet Security. At the top, there's a navigation bar with links for "Cybersecurity Best Practices", "Cybersecurity Tools", "Cybersecurity Threats", and "Membership". Below the navigation, a banner features a blog post about identifying email hoaxes. A color-coded alert level scale from "Low" (green) to "Severe" (red) is displayed, with "GUARDED" highlighted in blue. Three main service boxes are shown: "CIS SecureSuite®", "CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.", and "MS-ISAC®". The bottom section contains links for "CIS-CAT Pro", "CIS SecureSuite® Membership", and "CIS Benchmarks". A testimonial quote from a Senior Manager at the International Public Communications Agency is also present.

CIS Center for Internet S X

Sicuro | https://www.cisecurity.org

Membership

Cybersecurity Best Practices

Cybersecurity Tools

Cybersecurity Threats

Blog Post: How to Identify an Email Hoax & What to do if You Fall Victim → See all the latest →

Alert Level: GUARDED

Low Guarded Elevated High Severe

**CIS SecureSuite®**

*Start Secure. Stay Secure.™*

A CIS SecureSuite Membership combines the CIS Benchmarks, CIS Controls, and CIS-CAT Pro into one powerful cybersecurity resource. New members save 10% with promo code CIS-April2018.

New Members Save 10% Learn more→

**CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.**

**MS-ISAC®**

The Multi-State Information Sharing Center (MS-ISAC) is the focal point for prevention, protection, response and recovery for U.S. State, Local, Tribal and Territorial entities. CIS is home to the MS-ISAC.

**CIS-CAT Pro**

Robust automated configuration assessment tool rapidly identifies vulnerabilities with coverage for 80+ CIS Benchmarks.

Learn More →

**CIS SecureSuite® Membership**

**Start Secure, Stay Secure**

A CIS SecureSuite Membership combines and automates the CIS Benchmarks, CIS Controls, and CIS-CAT Pro into one powerful, time-saving cybersecurity resource for businesses, nonprofits, and governmental entities.

*"It is the most important membership compliance review of information security in the market today."*

— Senior Manager, Information Security  
Compliance International Public Communications Agency

**CIS Benchmarks**

Proven CIS Benchmarks guidelines to protect over 100 different systems

Download →

# Center for Internet Security

From Wikipedia, the free encyclopedia

The **Center for Internet Security (CIS)** is a 501(c)(3) nonprofit organization,<sup>[2][3]</sup> formed in October, 2000.<sup>[1]</sup> Its mission is to "identify, develop, validate, promote, and sustain best practice solutions for [cyber defense](#) and build and lead communities to enable an environment of trust in [cyberspace](#)".<sup>[8]</sup> The organization is headquartered in [East Greenbush](#), New York, with members including large corporations, government agencies, and academic institutions.<sup>[1]</sup>

CIS employs a closed [crowdsourcing](#) model to identify and refine effective security measures, with individuals developing recommendations that are shared with the community for evaluation through a [consensus decision-making](#) process. At the national and international level, CIS plays an important role in forming security policies and decisions by maintaining the CIS Controls and CIS Benchmarks, and hosting the Multi-State Information Sharing and Analysis Center (MS-ISAC).<sup>[9]</sup>

## Contents [hide]

### 1 Program areas

## Center for Intern



Founded	October, 2000
Type	501(c)(3) nonprofit organization
Legal status	Active
Location	East Greenbush, New York
Coordinates	42°36'44"N 73°53'45"W
Chairman and interim CEO	John C. Gilligan
Key people	Steven J. Silliman, COO; Curtis W. Morgan, Executive Director

# Summary

1. Center for Internet Security (CIS): free Microsoft security configuration benchmarks and scoring tools at [www.cisecurity.org](http://www.cisecurity.org)
2. Another book – Hacking Exposed Windows
3. New Microsoft security tools and best practices at [microsoft.com/security](http://microsoft.com/security)
4. Don't forget exposures from other Microsoft products, e.g. SQL vulnerabilities
5. Applications are far more vulnerable than OS
  - Hacking Exposed Web Applications
6. Minimization of services equals higher security
7. Disable print, and other unnecessary services (e.g. SMB)
8. Use Windows Firewall
9. Protect Internet-facing servers
10. Keep up to date service packs and security patches
11. Limit interactive logon privileges and escalation
12. Use Group Policy to create and distribute configurations
13. Enforce physical security against offline attacks
14. Subscribe to security publications and online resources