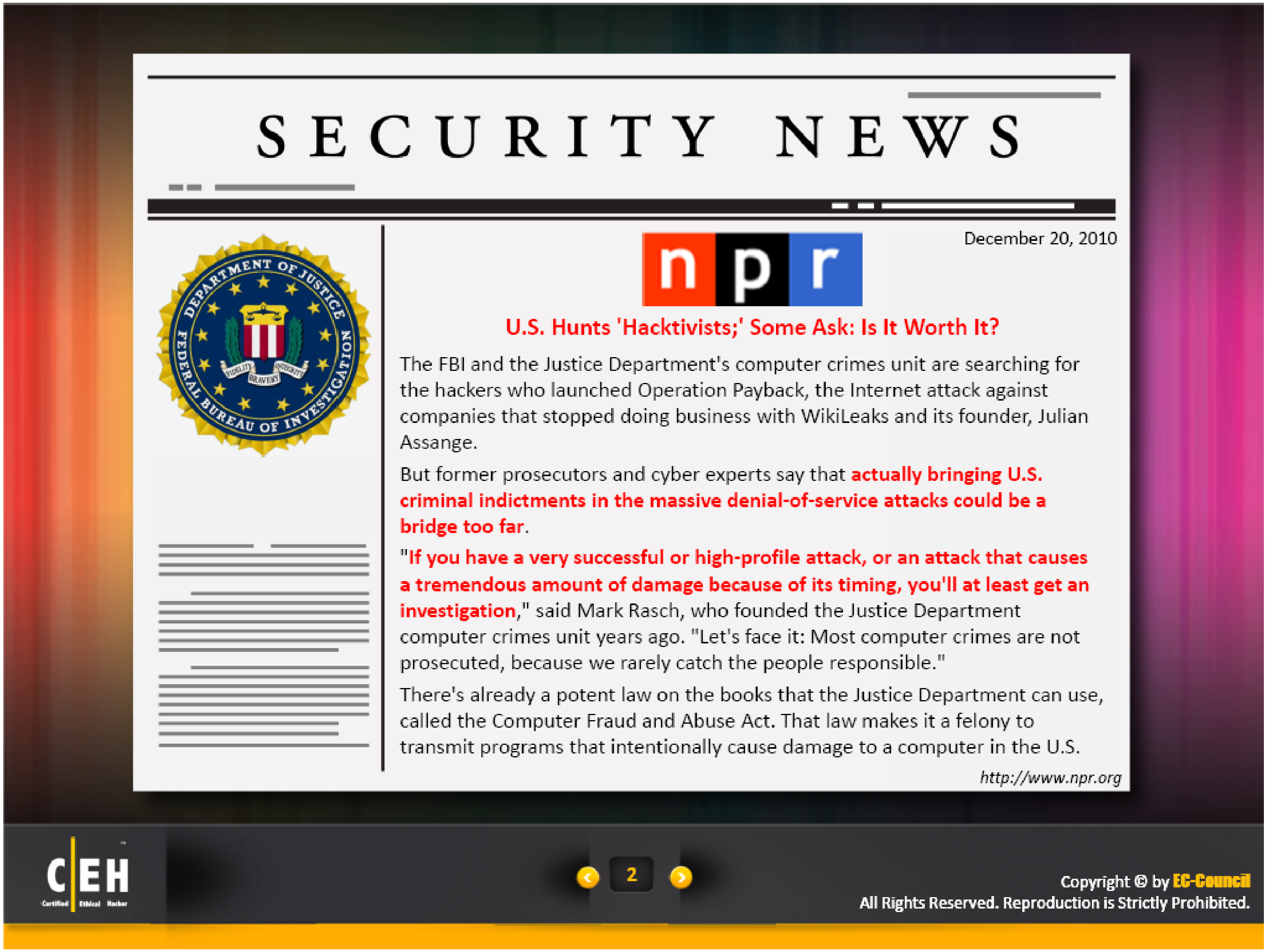
System Hacking

Module 5

Engineered by Hackers. Presented by Professionals.

C|EH™

Certified Ethical Hacker



SECURITY NEWS

December 20, 2010

npr

U.S. Hunts 'Hacktivists;' Some Ask: Is It Worth It?

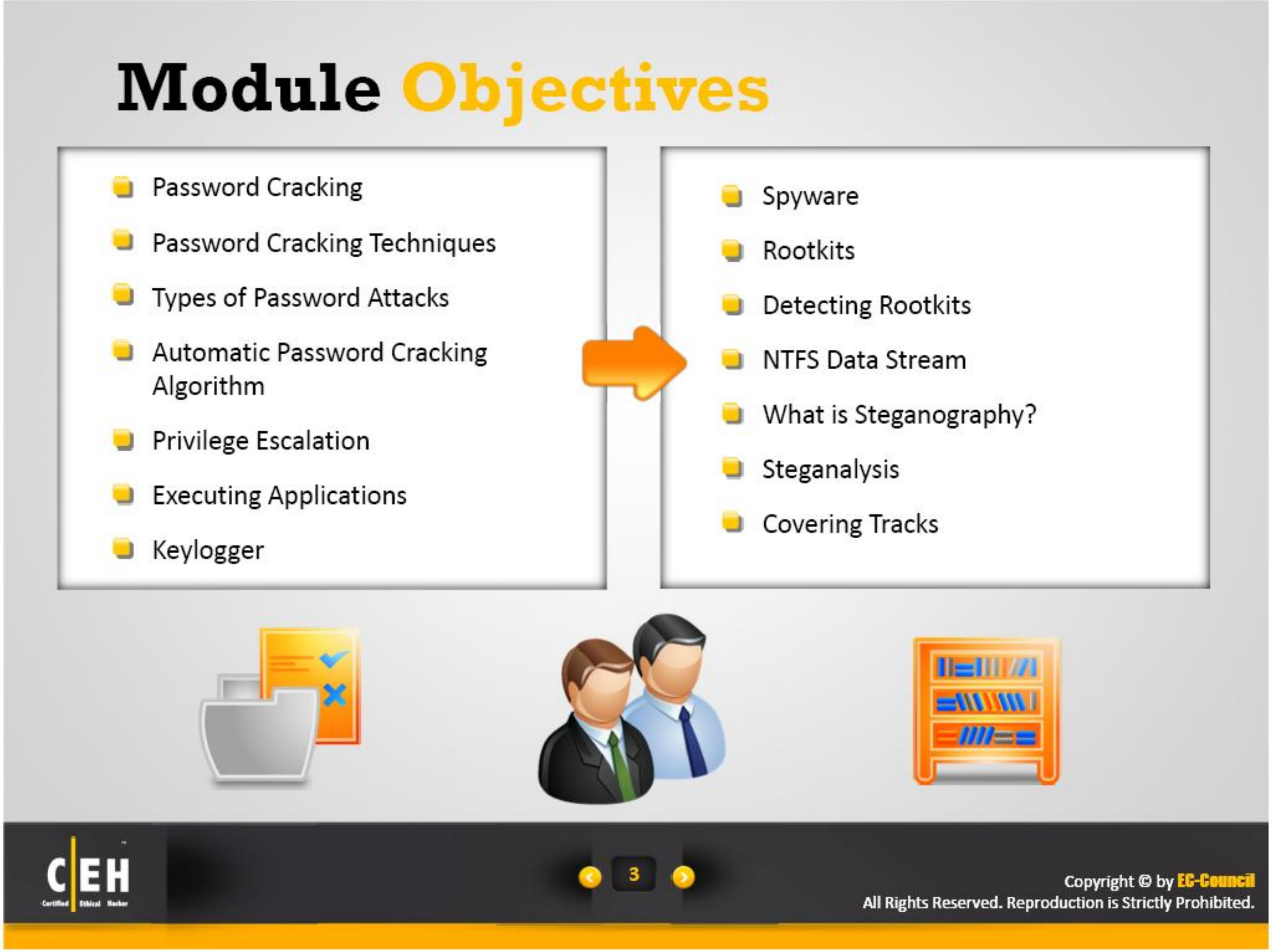
The FBI and the Justice Department's computer crimes unit are searching for the hackers who launched Operation Payback, the Internet attack against companies that stopped doing business with WikiLeaks and its founder, Julian Assange.

But former prosecutors and cyber experts say that **actually bringing U.S. criminal indictments in the massive denial-of-service attacks could be a bridge too far**.

"**If you have a very successful or high-profile attack, or an attack that causes a tremendous amount of damage because of its timing, you'll at least get an investigation**," said Mark Rasch, who founded the Justice Department computer crimes unit years ago. "Let's face it: Most computer crimes are not prosecuted, because we rarely catch the people responsible."

There's already a potent law on the books that the Justice Department can use, called the Computer Fraud and Abuse Act. That law makes it a felony to transmit programs that intentionally cause damage to a computer in the U.S.

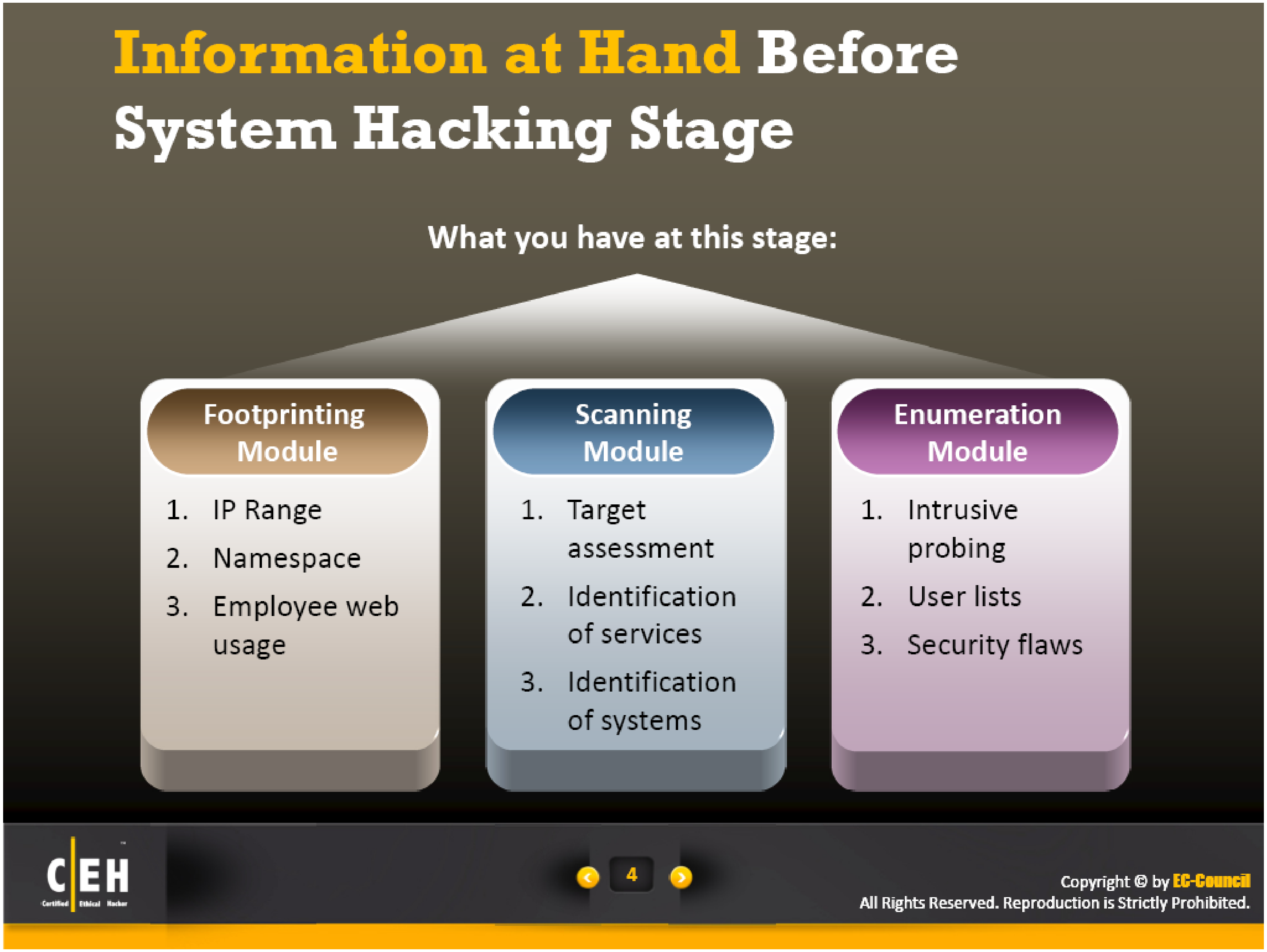
http://www.npr.org



Module Objectives

- Password Cracking
- Password Cracking Techniques
- Types of Password Attacks
- Automatic Password Cracking Algorithm
- Privilege Escalation
- Executing Applications
- Keylogger

- Spyware
- Rootkits
- Detecting Rootkits
- NTFS Data Stream
- What is Steganography?
- Steganalysis
- Covering Tracks



Information at Hand Before System Hacking Stage

What you have at this stage:

Footprinting Module

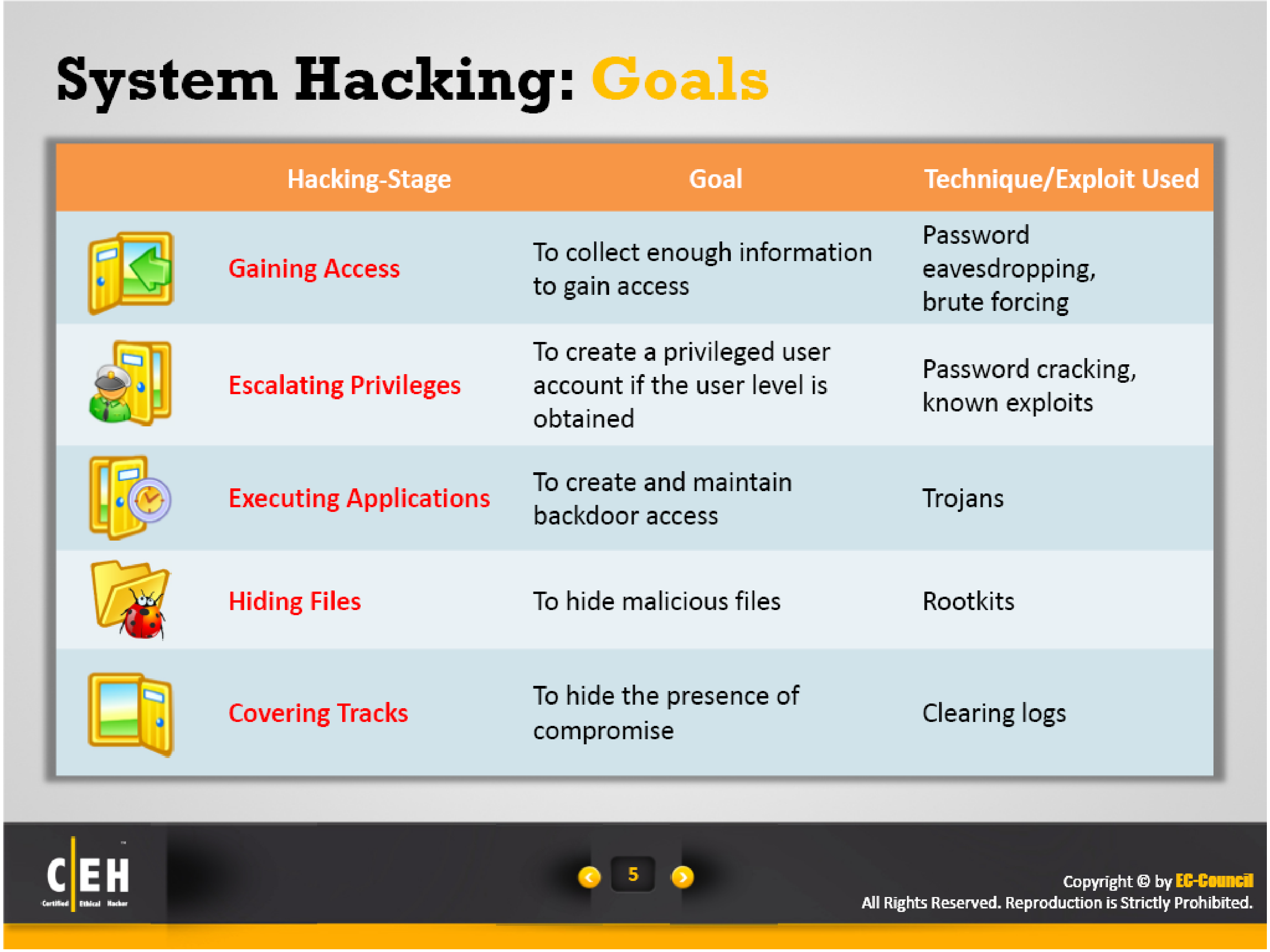
1. IP Range
2. Namespace
3. Employee web usage

Scanning Module

1. Target assessment
2. Identification of services
3. Identification of systems

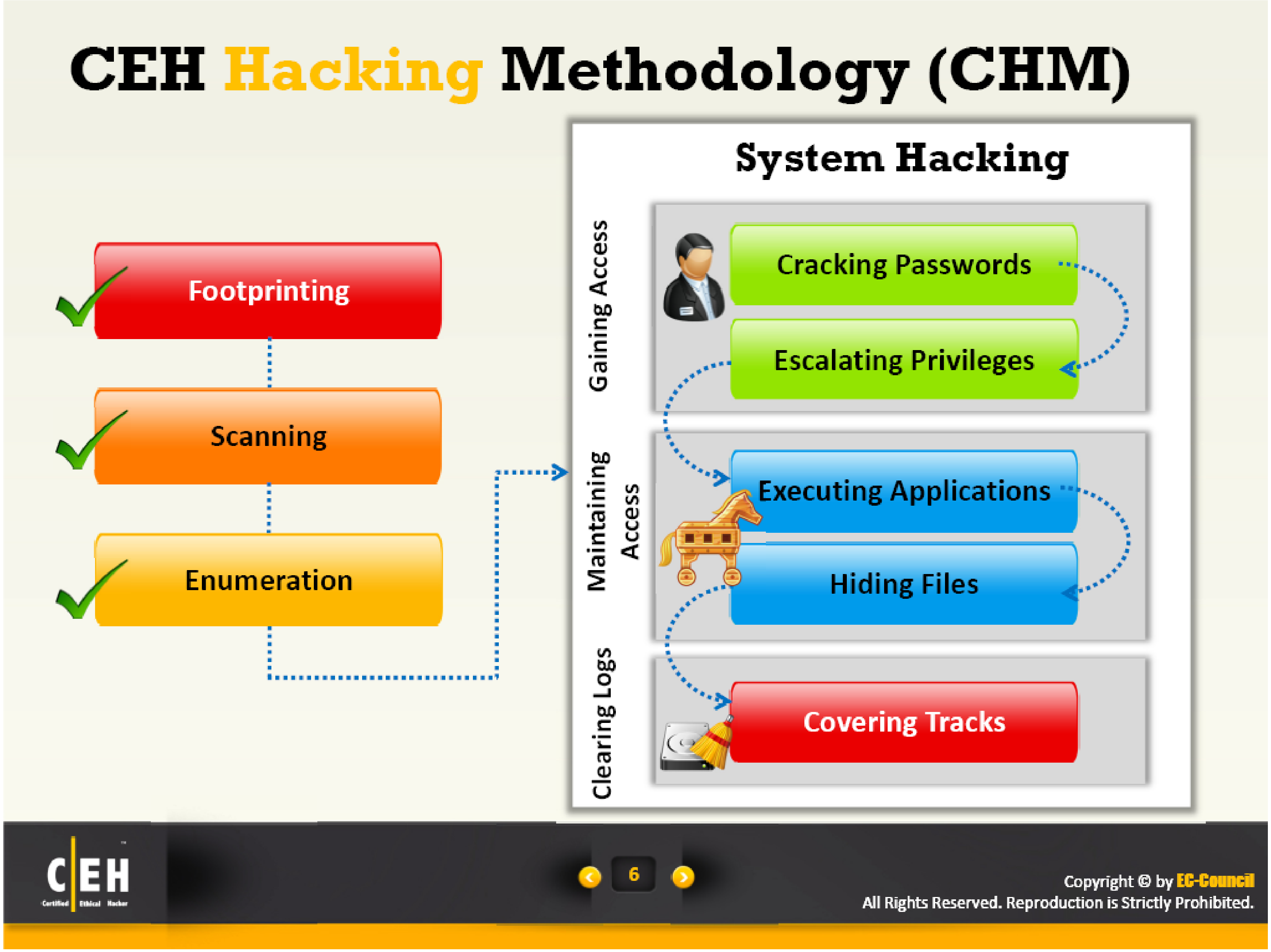
Enumeration Module

1. Intrusive probing
2. User lists
3. Security flaws



System Hacking: Goals

Hacking-Stage	Goal	Technique/Exploit Used
Gaining Access	To collect enough information to gain access	Password eavesdropping, brute forcing
Escalating Privileges	To create a privileged user account if the user level is obtained	Password cracking, known exploits
Executing Applications	To create and maintain backdoor access	Trojans
Hiding Files	To hide malicious files	Rootkits
Covering Tracks	To hide the presence of compromise	Clearing logs



CEH Hacking Methodology (CHM)

✓ Footprinting

✓ Scanning

✓ Enumeration

System Hacking

Gaining Access

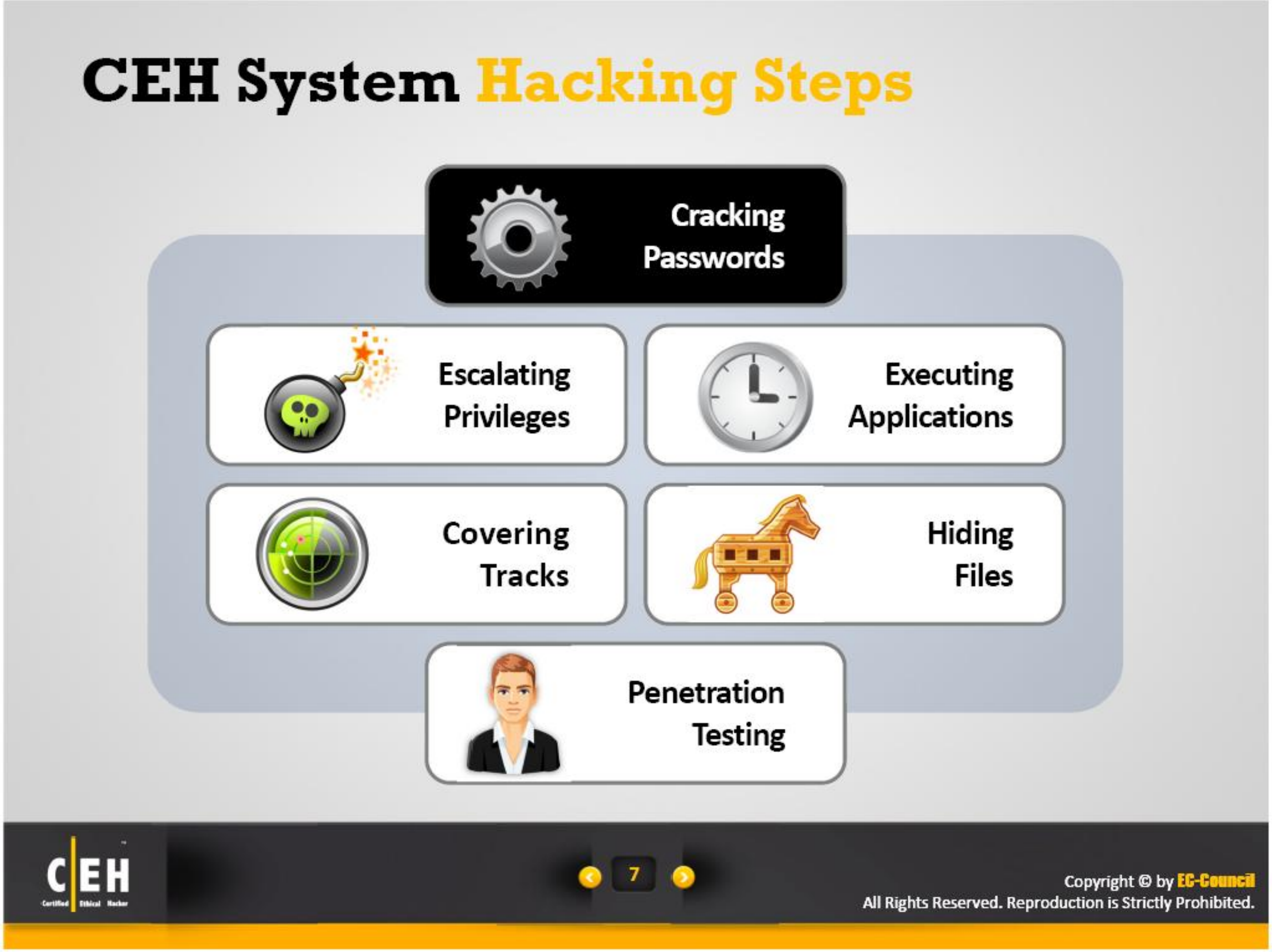
- Cracking Passwords
- Escalating Privileges

Maintaining Access

- Executing Applications
- Hiding Files

Clearing Logs

- Covering Tracks



CEH System Hacking Steps

Cracking Passwords

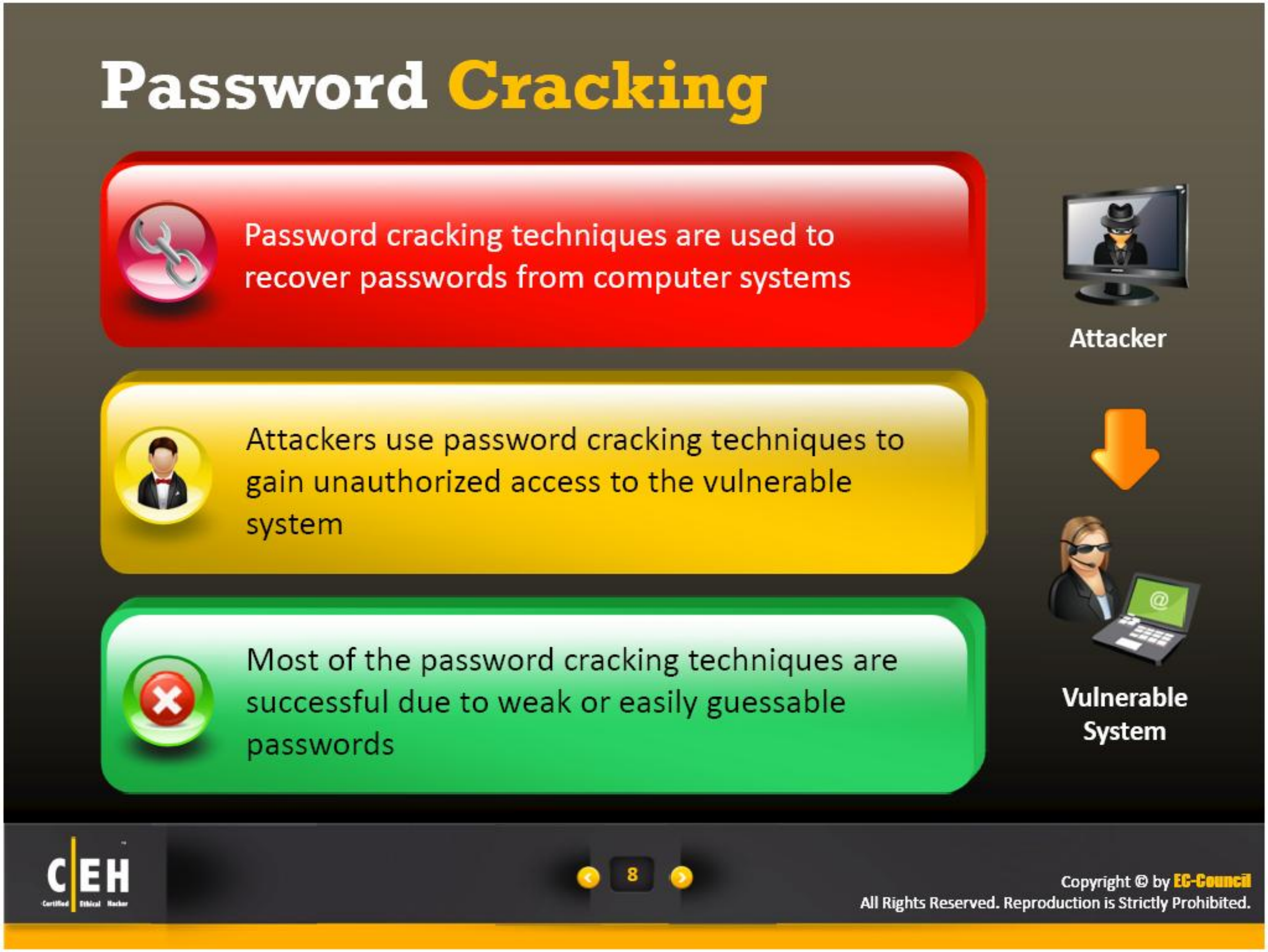
Escalating Privileges

Executing Applications

Covering Tracks

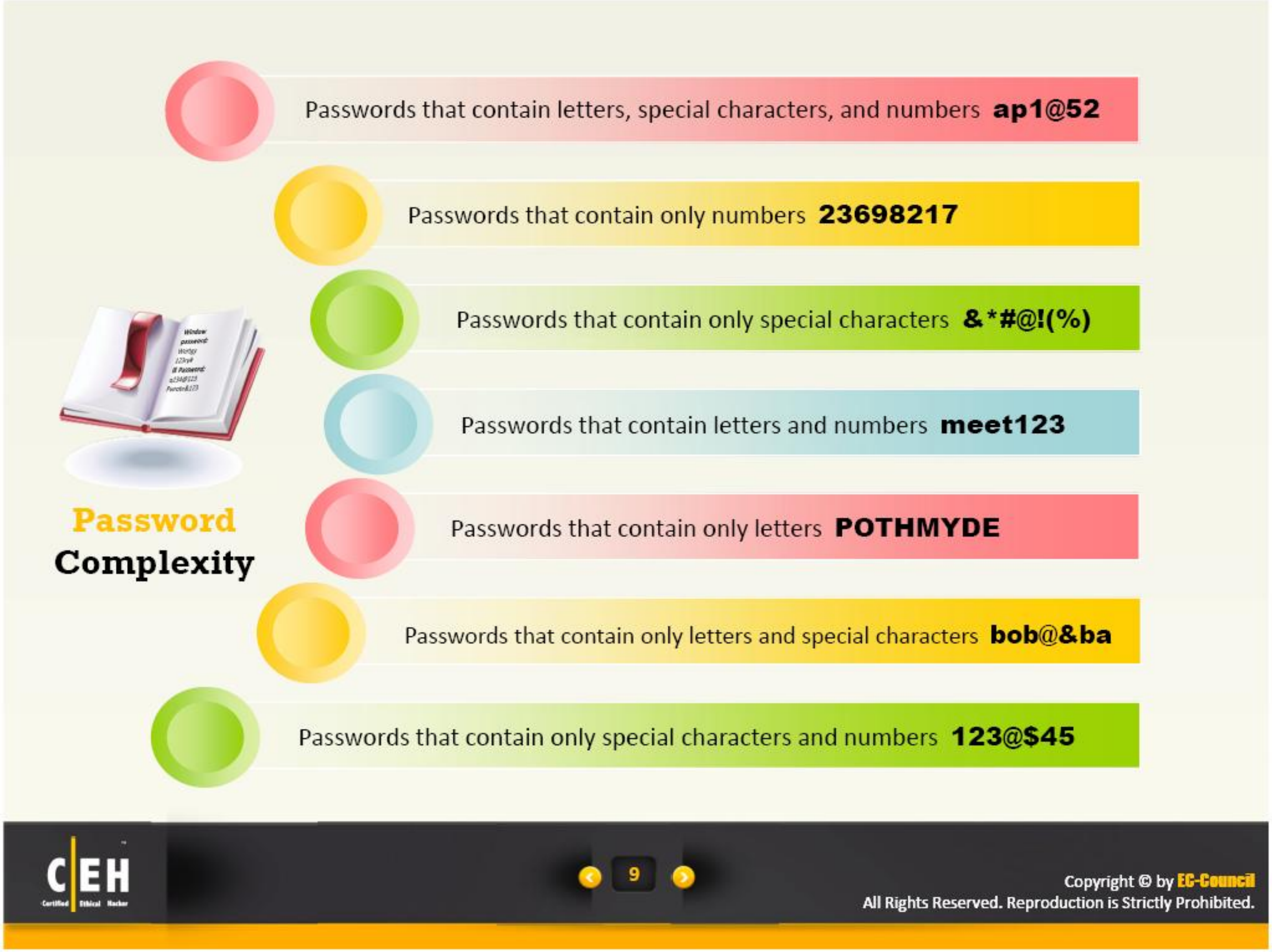
Hiding Files

Penetration Testing



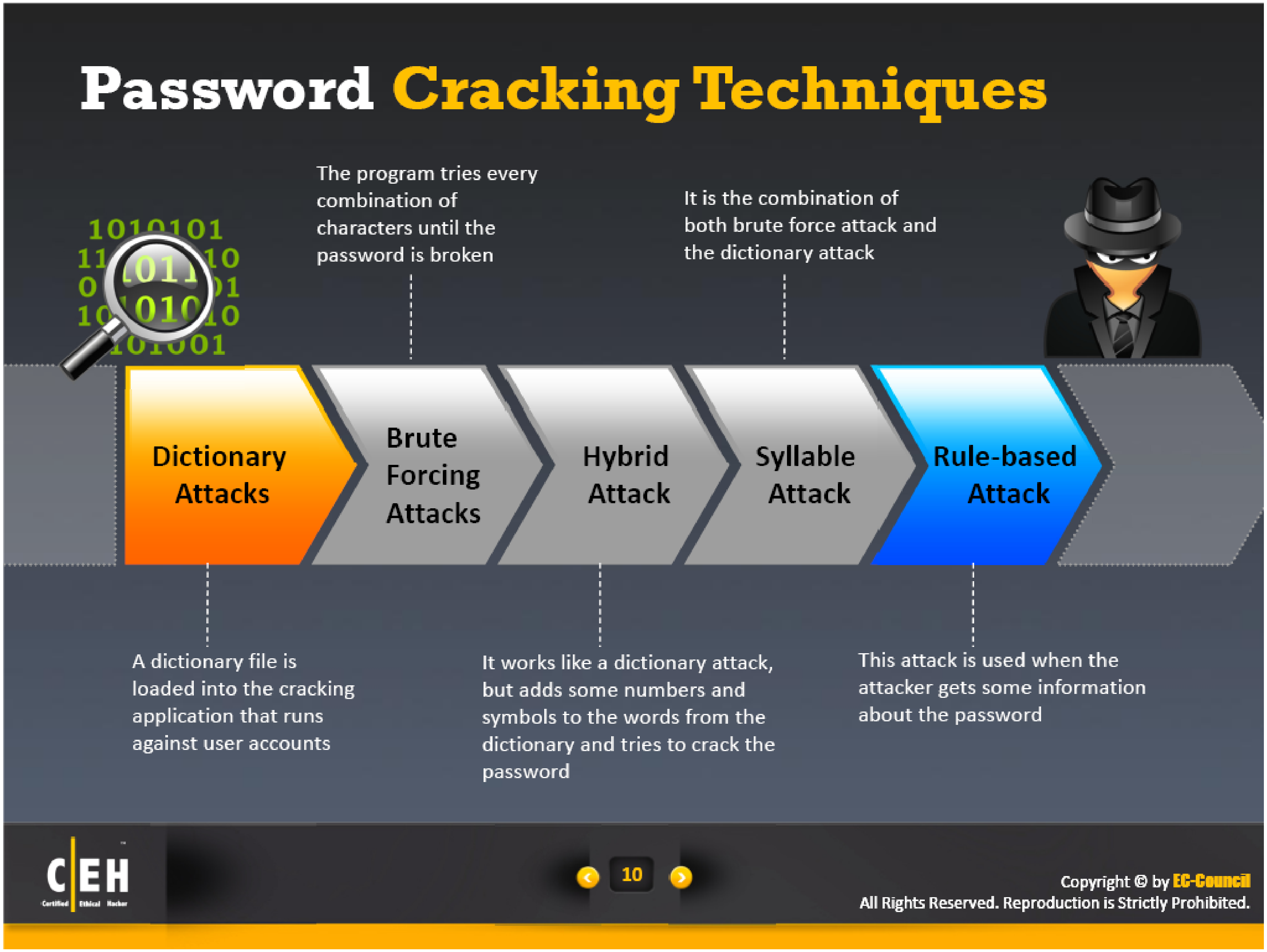
Password Cracking

- Password cracking techniques are used to recover passwords from computer systems
- Attackers use password cracking techniques to gain unauthorized access to the vulnerable system
- Most of the password cracking techniques are successful due to weak or easily guessable passwords



Password Complexity

- Passwords that contain letters, special characters, and numbers **ap1@52**
- Passwords that contain only numbers **23698217**
- Passwords that contain only special characters **&*#@!(%)**
- Passwords that contain letters and numbers **meet123**
- Passwords that contain only letters **POTHMYDE**
- Passwords that contain only letters and special characters **bob@&ba**
- Passwords that contain only special characters and numbers **123@$45**



Password Cracking Techniques

Dictionary Attacks

A dictionary file is loaded into the cracking application that runs against user accounts

Brute Forcing Attacks

The program tries every combination of characters until the password is broken

Hybrid Attack

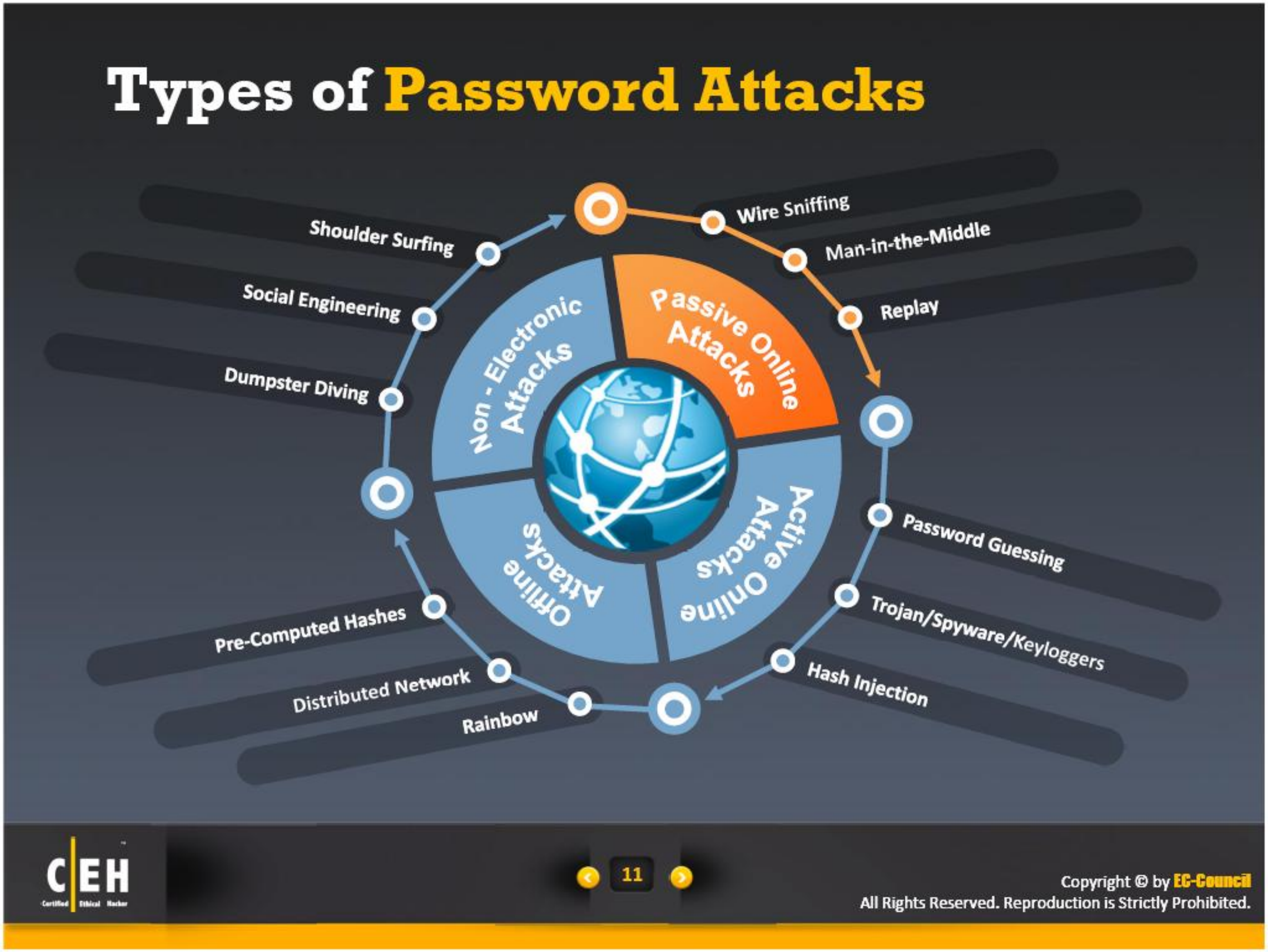
It works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password

Syllable Attack

It is the combination of both brute force attack and the dictionary attack

Rule-based Attack

This attack is used when the attacker gets some information about the password



Types of Password Attacks

Non - Electronic Attacks

- Shoulder Surfing
- Social Engineering
- Dumpster Diving

Passive Online Attacks

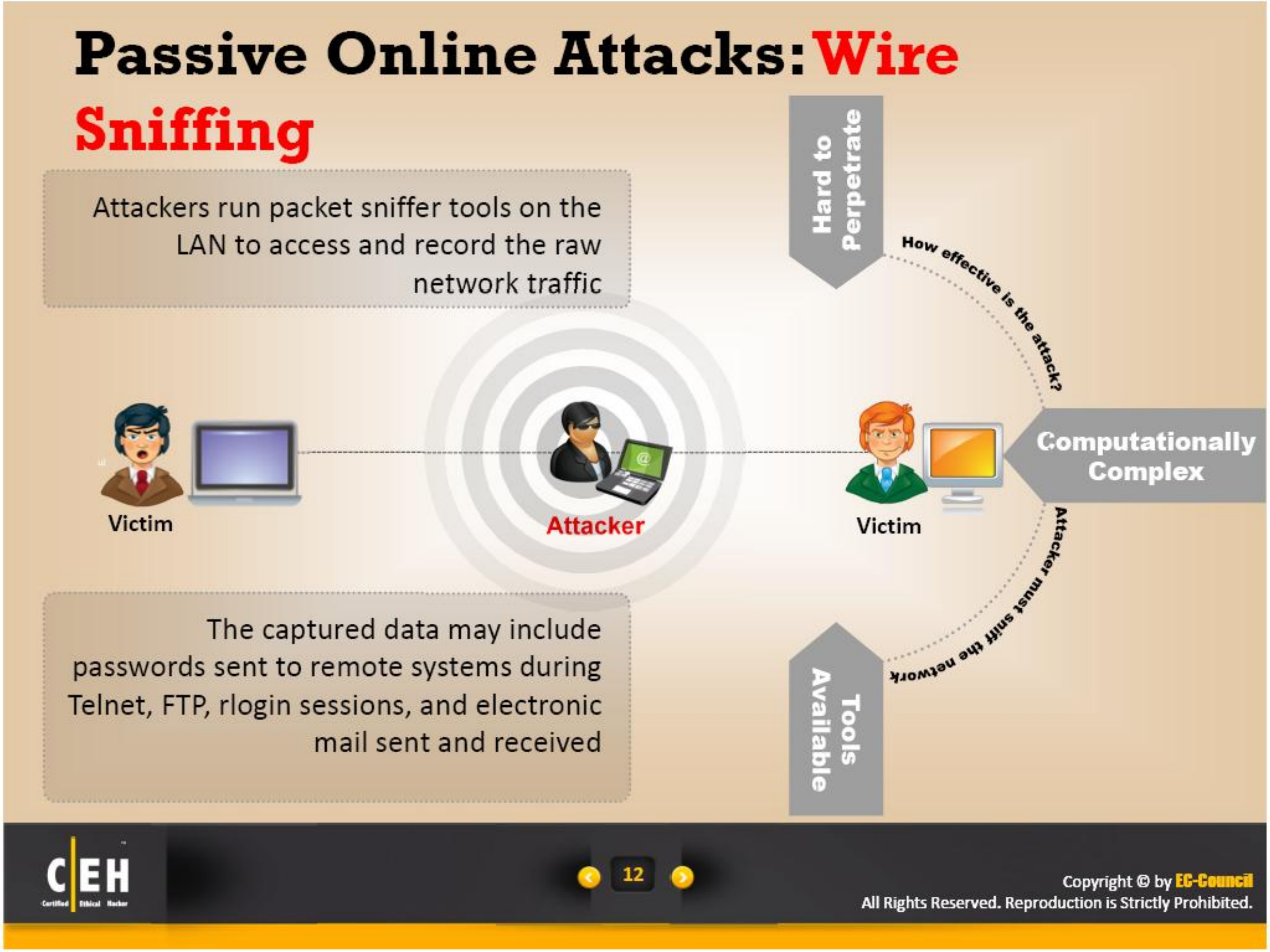
- Wire Sniffing
- Man-in-the-Middle
- Replay

Active Online Attacks

- Password Guessing
- Trojan/Spyware/Keyloggers
- Hash Injection

Offline Attacks

- Rainbow
- Distributed Network
- Pre-Computed Hashes



Passive Online Attacks: Wire Sniffing

Attackers run packet sniffer tools on the LAN to access and record the raw network traffic

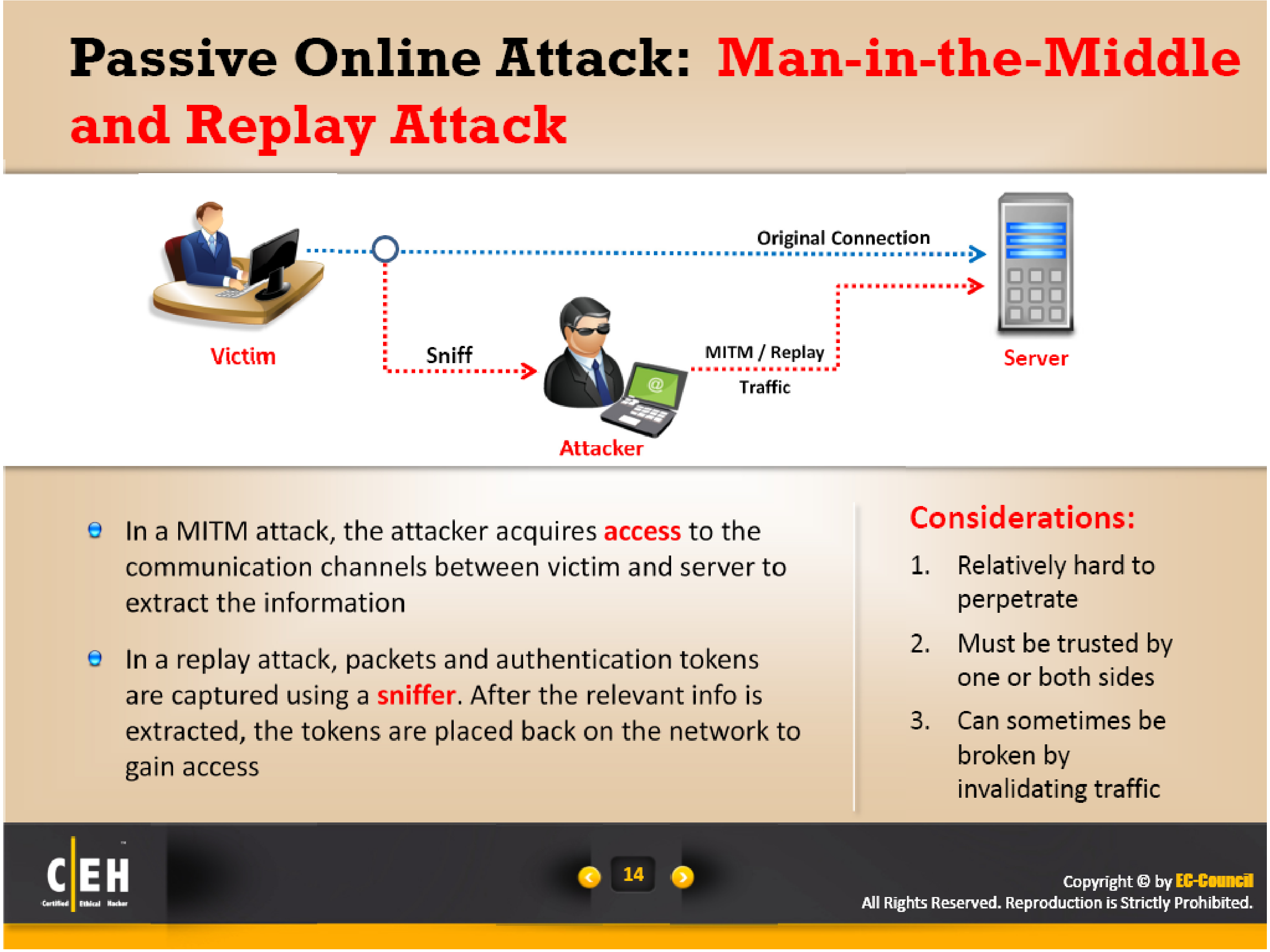
The captured data may include passwords sent to remote systems during Telnet, FTP, rlogin sessions, and electronic mail sent and received

Password Sniffing

If an attacker is able to eavesdrop on Windows logins, then this approach can spare random guesswork

Sniff credentials off the wire while logging in to a server and then replay them to gain access

Password guessing is a tough task

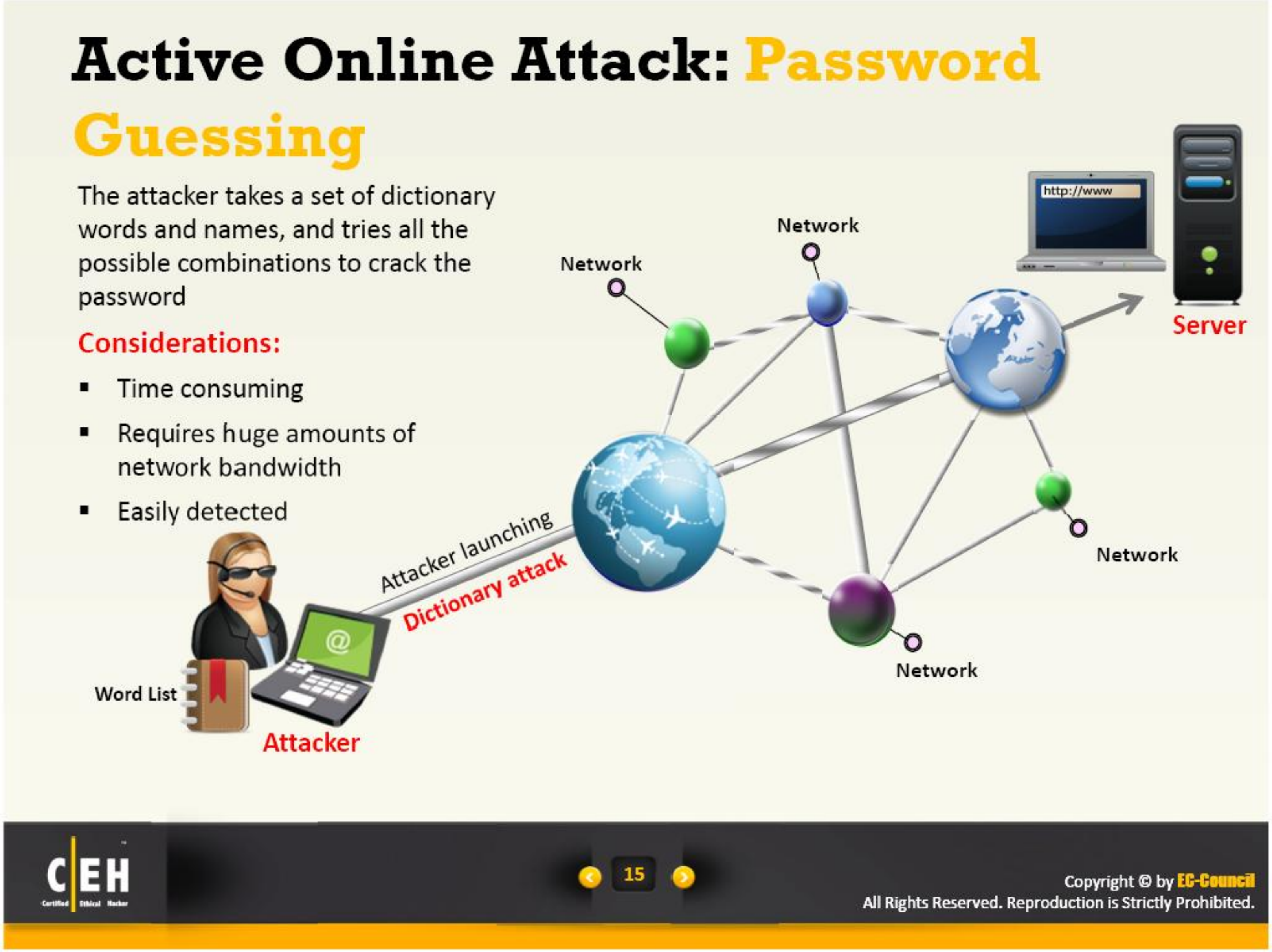


Passive Online Attack: Man-in-the-Middle and Replay Attack

- In a MITM attack, the attacker acquires **access** to the communication channels between victim and server to extract the information
- In a replay attack, packets and authentication tokens are captured using a **sniffer**. After the relevant info is extracted, the tokens are placed back on the network to gain access

Considerations:

1. Relatively hard to perpetrate
2. Must be trusted by one or both sides
3. Can sometimes be broken by invalidating traffic

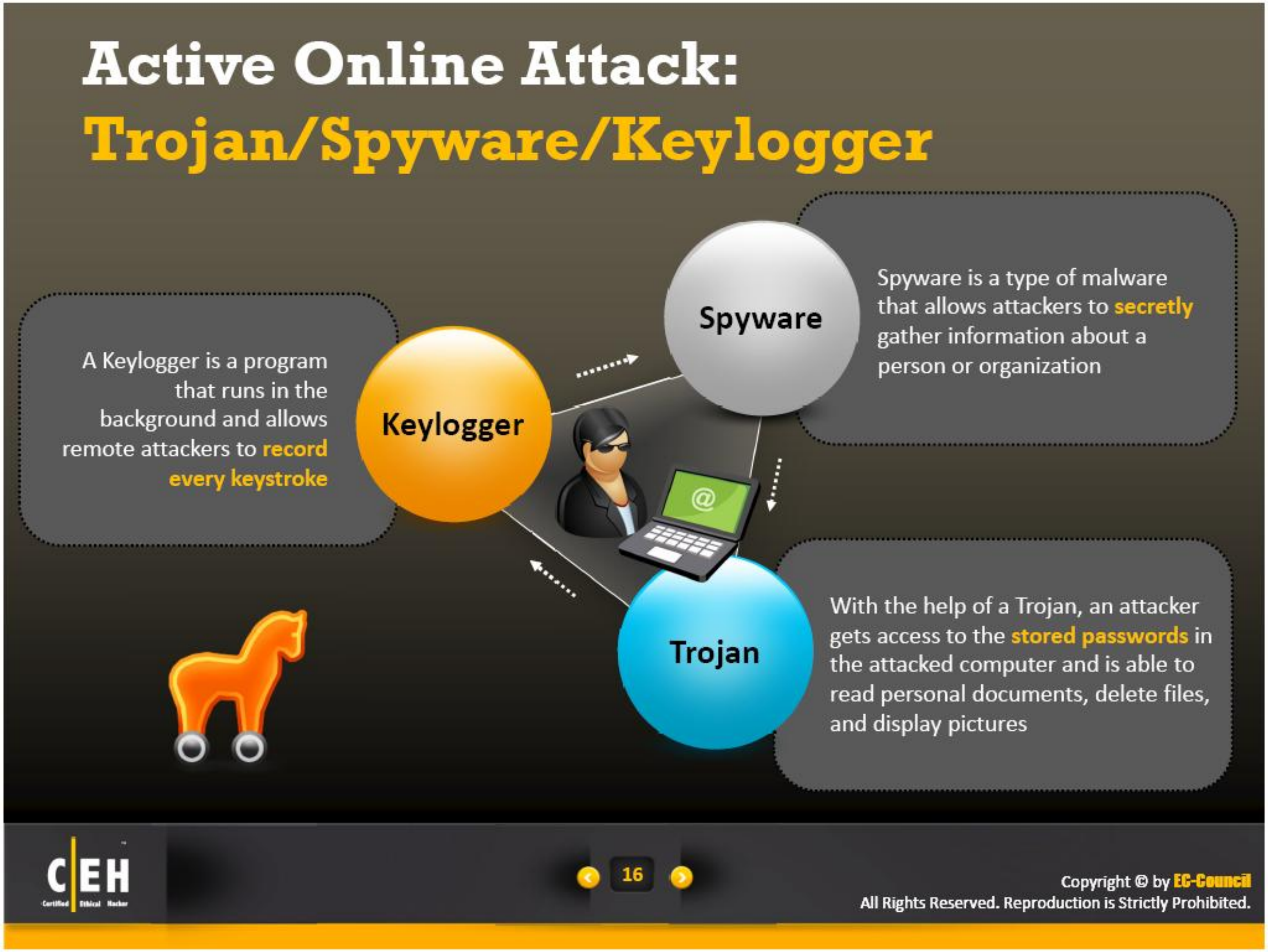


Active Online Attack: Password Guessing

The attacker takes a set of dictionary words and names, and tries all the possible combinations to crack the password

Considerations:

- Time consuming
- Requires huge amounts of network bandwidth
- Easily detected



Active Online Attack: Trojan/Spyware/Keylogger

Keylogger

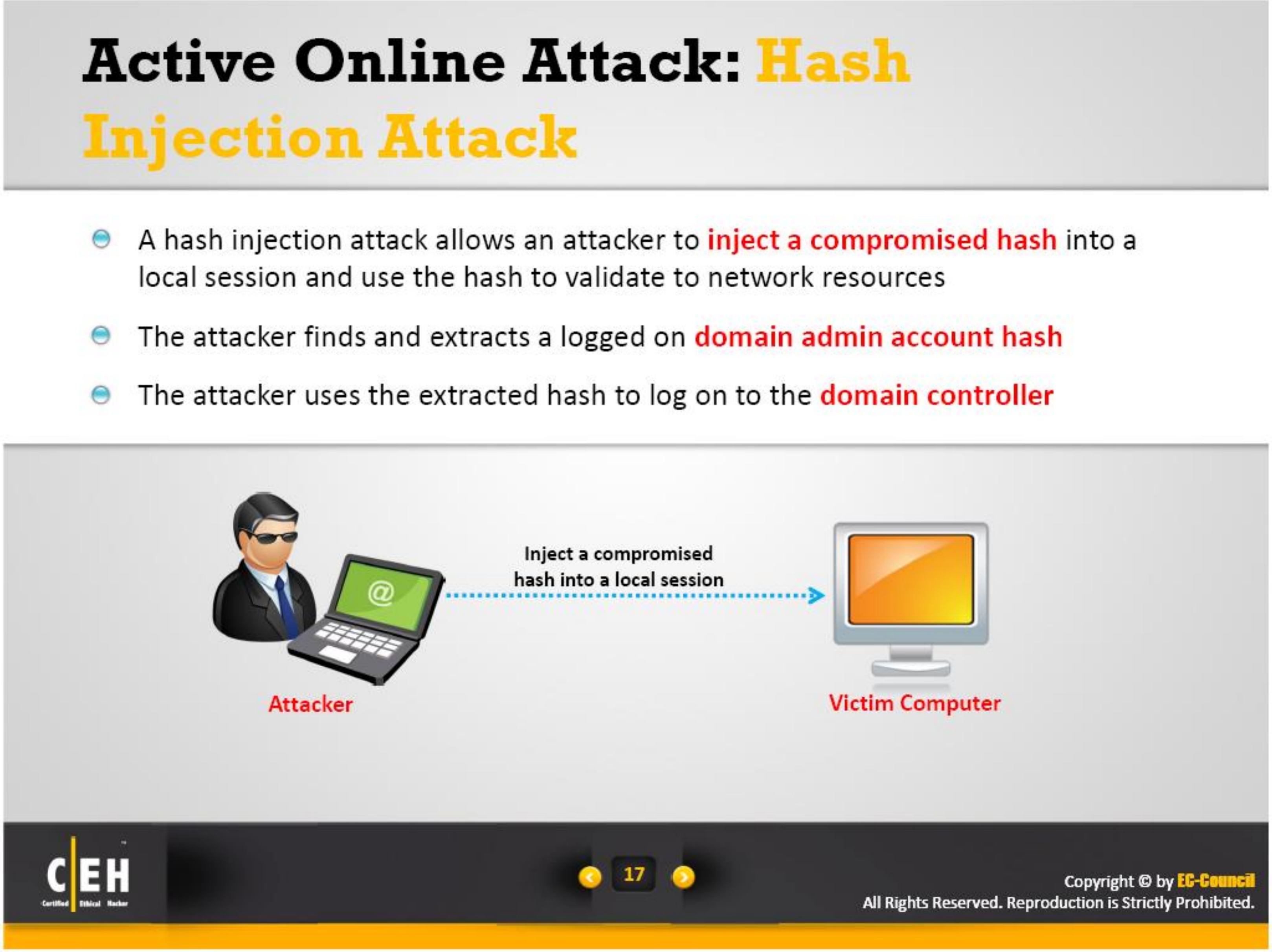
A Keylogger is a program that runs in the background and allows remote attackers to **record every keystroke**

Spyware

Spyware is a type of malware that allows attackers to **secretly** gather information about a person or organization

Trojan

With the help of a Trojan, an attacker gets access to the **stored passwords** in the attacked computer and is able to read personal documents, delete files, and display pictures



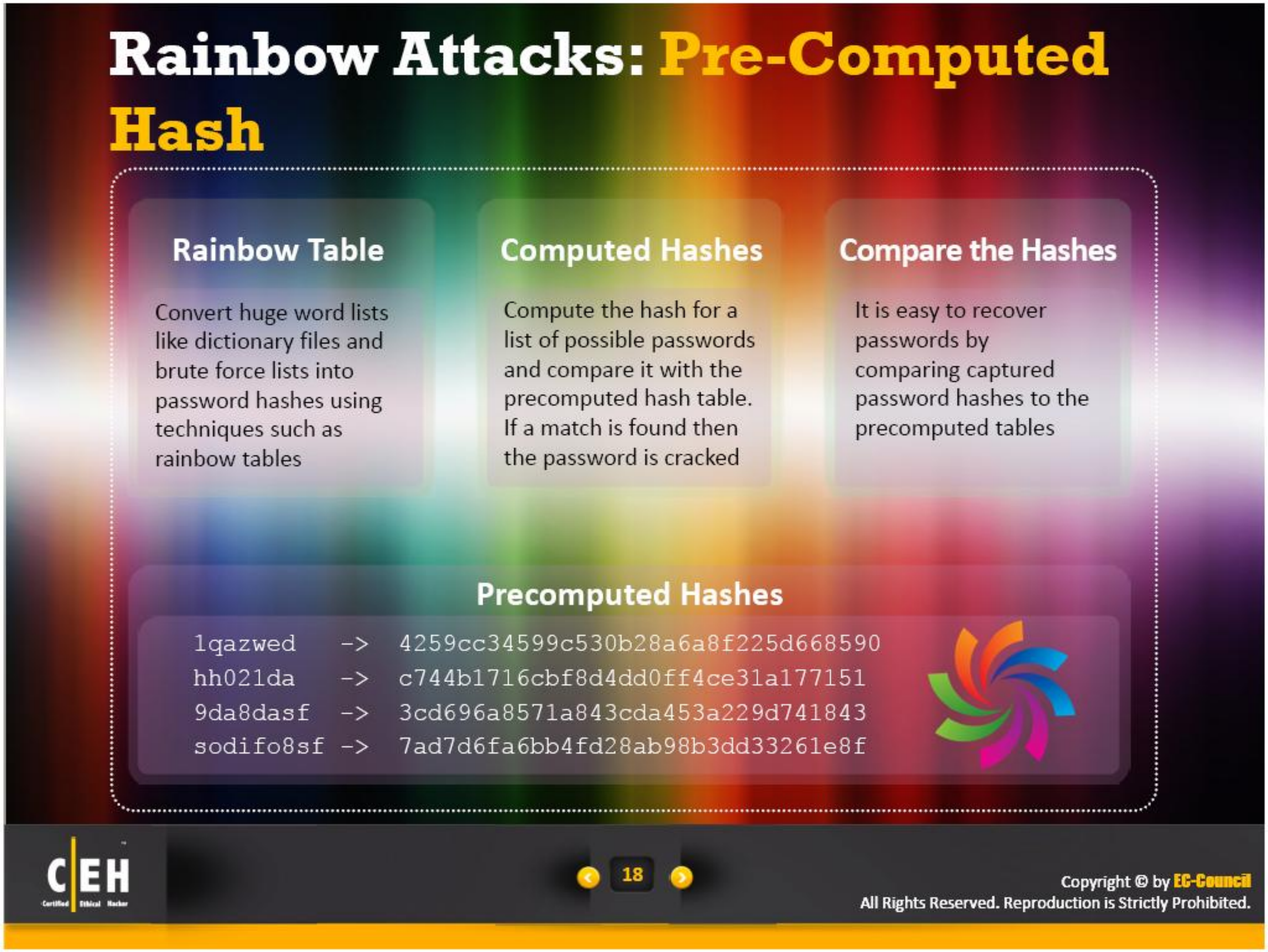
Active Online Attack: Hash Injection Attack

- A hash injection attack allows an attacker to **inject a compromised hash** into a local session and use the hash to validate to network resources
- The attacker finds and extracts a logged on **domain admin account hash**
- The attacker uses the extracted hash to log on to the **domain controller**

Attacker

Inject a compromised hash into a local session

Victim Computer



Rainbow Attacks: Pre-Computed Hash

Rainbow Table

Convert huge word lists like dictionary files and brute force lists into password hashes using techniques such as rainbow tables

Computed Hashes

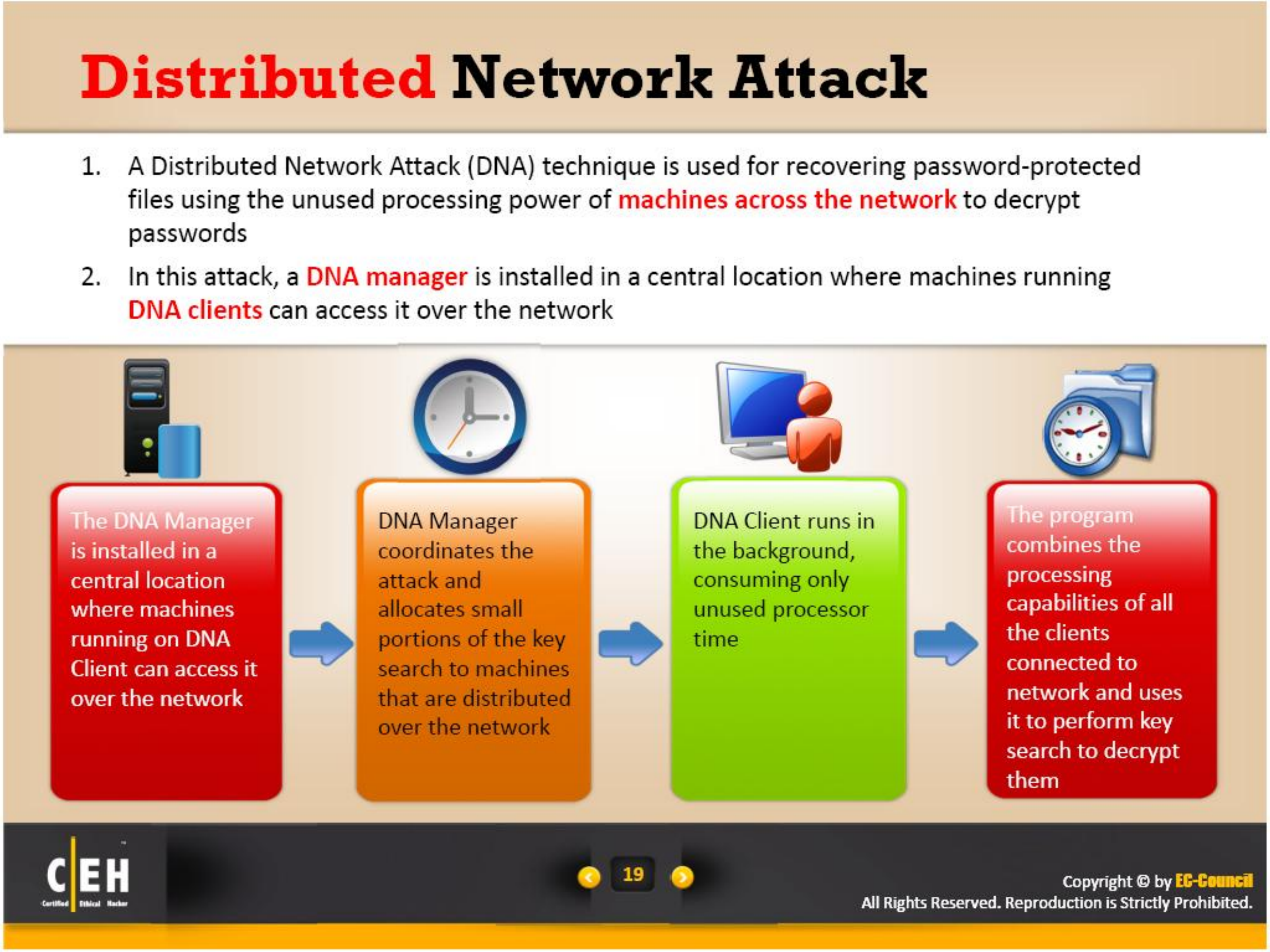
Compute the hash for a list of possible passwords and compare it with the precomputed hash table. If a match is found then the password is cracked

Compare the Hashes

It is easy to recover passwords by comparing captured password hashes to the precomputed tables

Precomputed Hashes

```
1qazwed   -> 4259cc34599c530b28a6a8f225d668590
hh021da   -> c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf  -> 3cd696a8571a843cda453a229d741843
sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
```



Distributed Network Attack

1. A Distributed Network Attack (DNA) technique is used for recovering password-protected files using the unused processing power of **machines across the network** to decrypt passwords

2. In this attack, a **DNA manager** is installed in a central location where machines running **DNA clients** can access it over the network

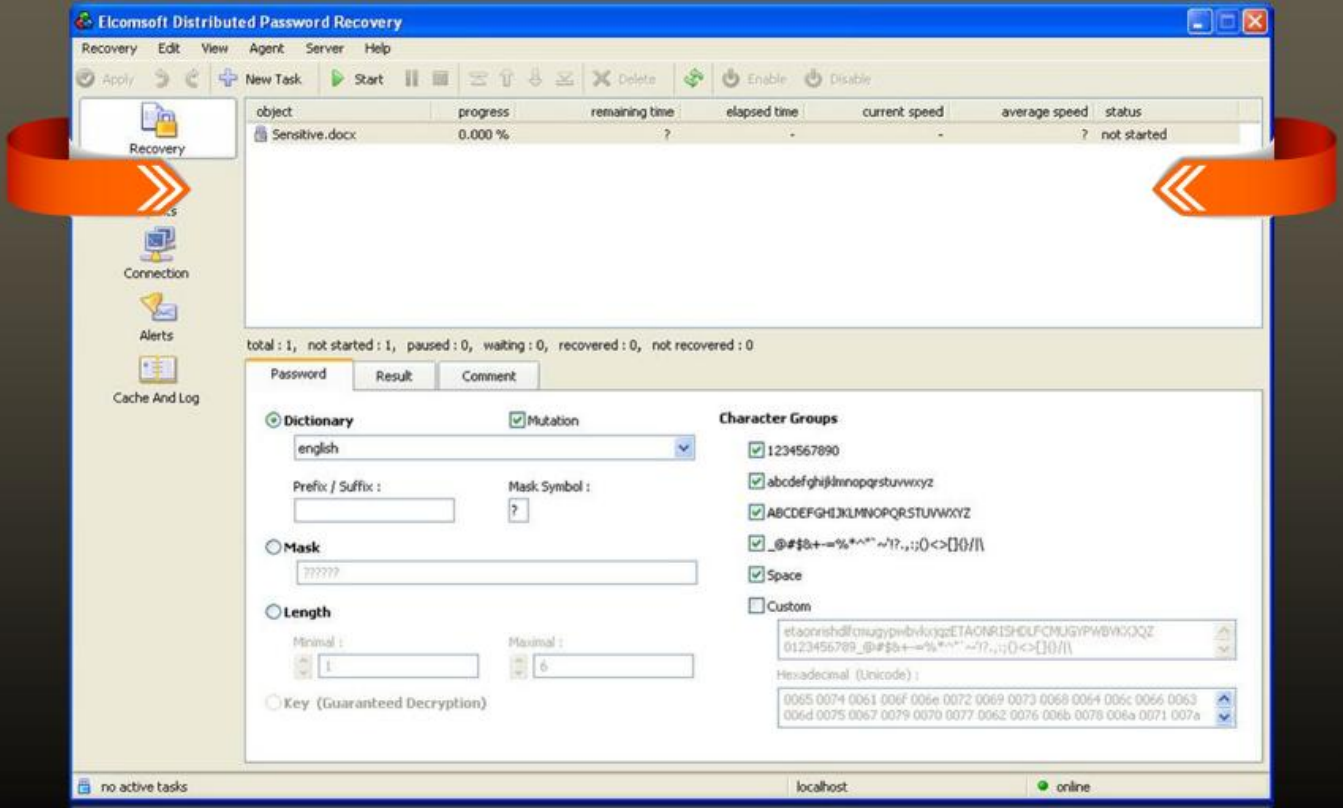
The DNA Manager is installed in a central location where machines running on DNA Client can access it over the network

DNA Manager coordinates the attack and allocates small portions of the key search to machines that are distributed over the network

DNA Client runs in the background, consuming only unused processor time

The program combines the processing capabilities of all the clients connected to network and uses it to perform key search to decrypt them

Elcomsoft Distributed Password Recovery



object	progress	remaining time	elapsed time	current speed	average speed	status
Sensitive.docx	0.000 %	?	-	-	?	not started

total : 1, not started : 1, paused : 0, waiting : 0, recovered : 0, not recovered : 0

● Dictionary ☑ Mutation

english

Prefix / Suffix :

Mask Symbol : ?

○ Mask

??????

○ Length

Minimal : 1

Maximal : 6

○ Key (Guaranteed Decryption)

Character Groups

☑ 1234567890

☑ abcdefghijklmnopqrstuvwxyz

☑ ABCDEFGHIJKLMNOPQRSTUVWXYZ

☑ _@#$&+-=%*^"`~'!?.,:;()<>[]{}/|\

☑ Space

□ Custom

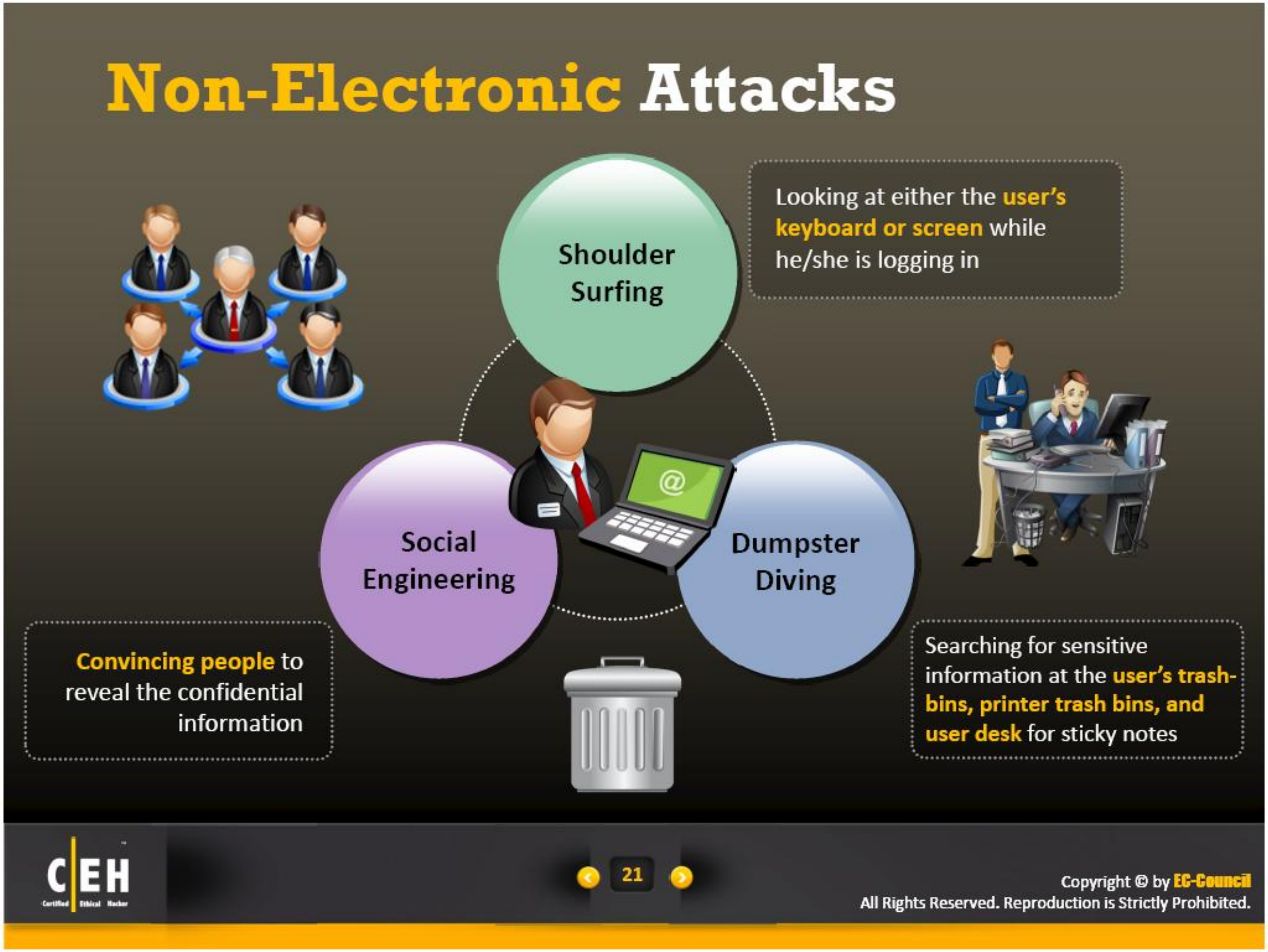
etaonrishdlfcmugypwbvkxjqzETAONRISHDLFCMUGYPWBVKXJQZ
0123456789_@#$&+-=%*^"`~'!?.,:;()<>[]{}/|\

Hexadecimal (Unicode) :

0065 0074 0061 006f 006e 0072 0069 0073 0068 0064 006c 0066 0063
006d 0075 0067 0079 0070 0077 0062 0076 006b 0078 006a 0071 007a

no active tasks localhost online

http://www.elcomsoft.com



Non-Electronic Attacks

Shoulder Surfing

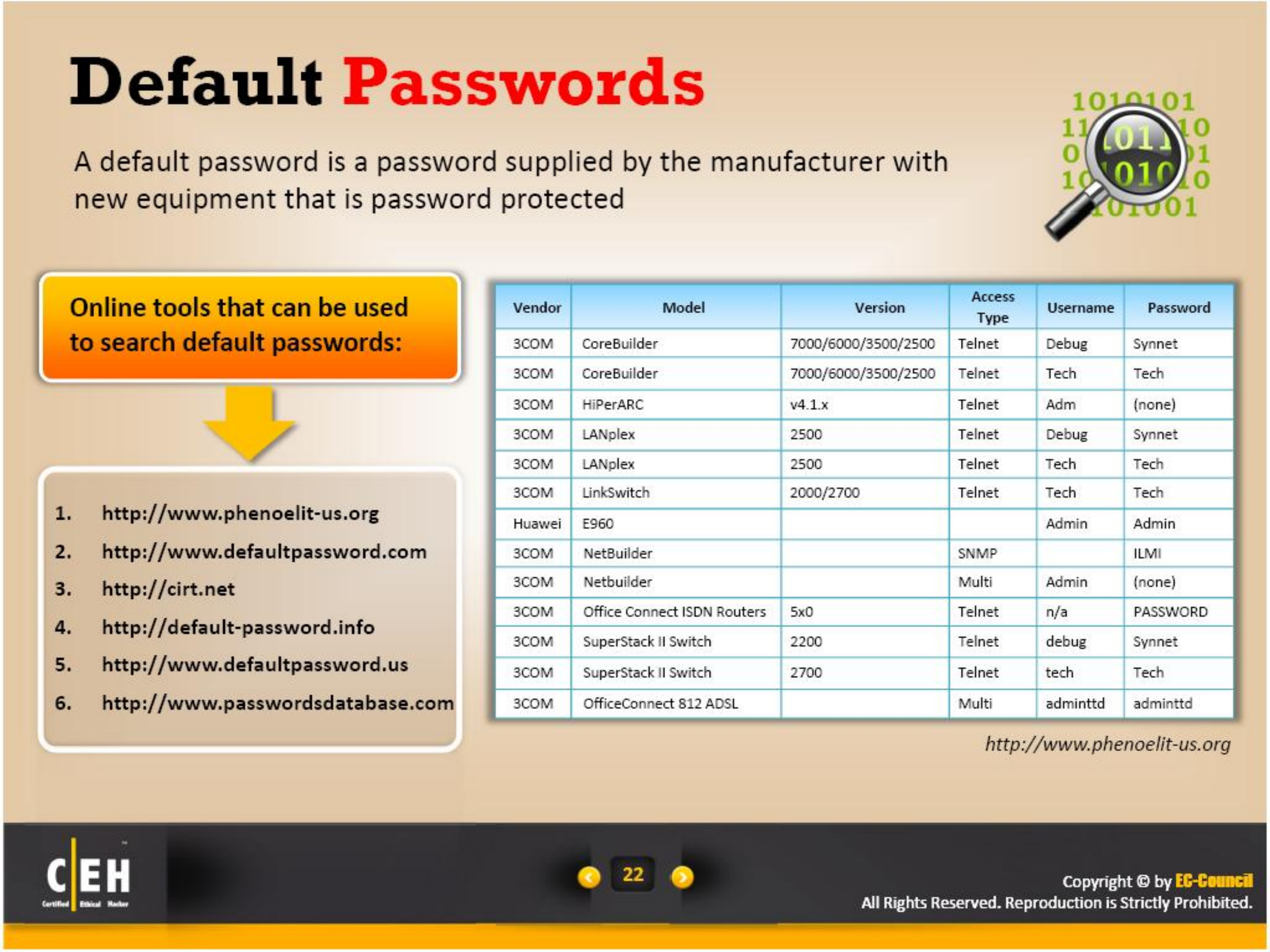
Looking at either the **user's keyboard or screen** while he/she is logging in

Social Engineering

Convincing people to reveal the confidential information

Dumpster Diving

Searching for sensitive information at the **user's trash-bins, printer trash bins, and user desk** for sticky notes



Default Passwords

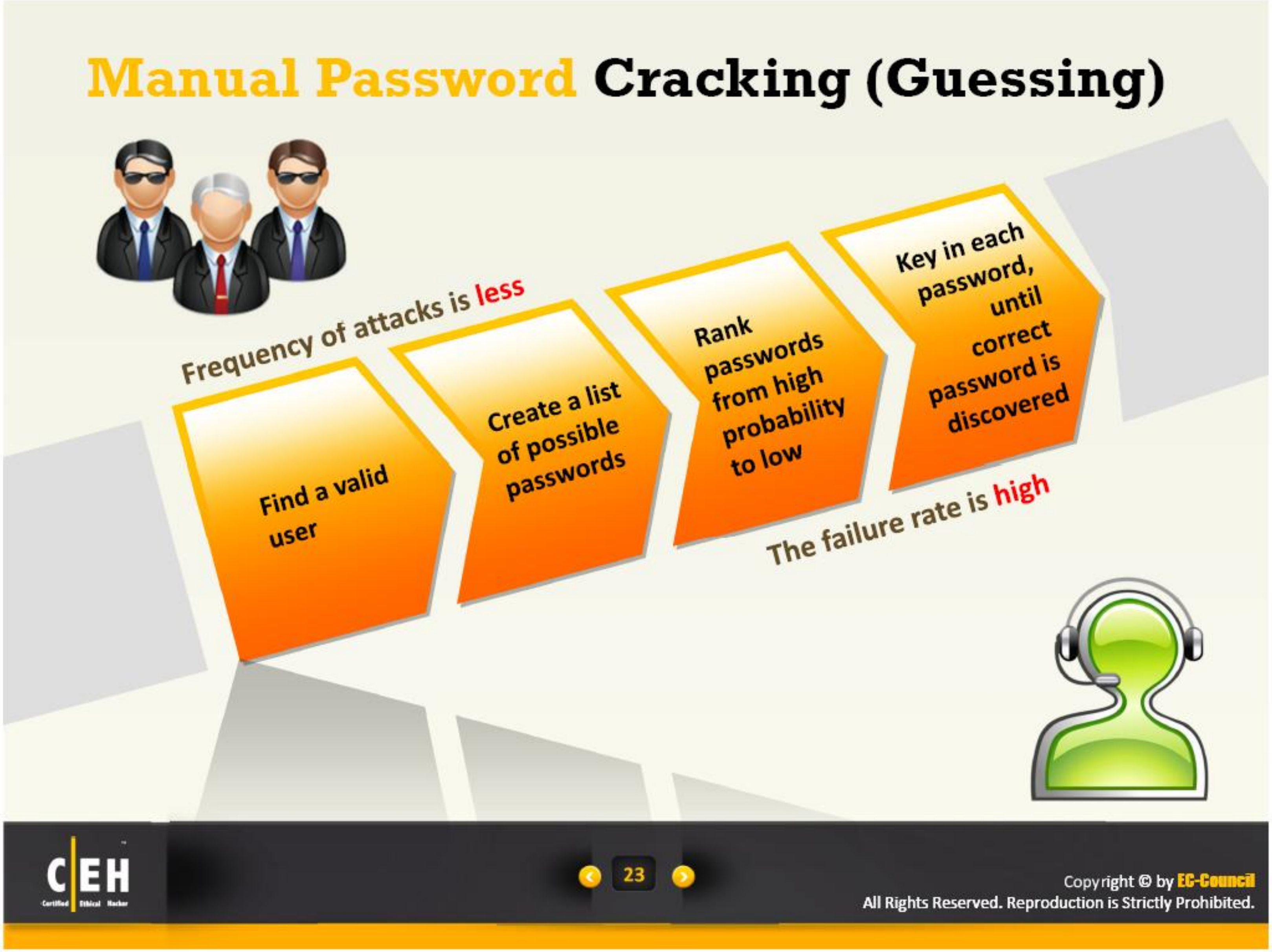
A default password is a password supplied by the manufacturer with new equipment that is password protected

Online tools that can be used to search default passwords:

1. http://www.phenoelit-us.org
2. http://www.defaultpassword.com
3. http://cirt.net
4. http://default-password.info
5. http://www.defaultpassword.us
6. http://www.passwordsdatabase.com

Vendor	Model	Version	Access Type	Username	Password
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Debug	Synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	Tech	Tech
3COM	HiPerARC	v4.1.x	Telnet	Adm	(none)
3COM	LANplex	2500	Telnet	Debug	Synnet
3COM	LANplex	2500	Telnet	Tech	Tech
3COM	LinkSwitch	2000/2700	Telnet	Tech	Tech
Huawei	E960			Admin	Admin
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	Admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	Synnet
3COM	SuperStack II Switch	2700	Telnet	tech	Tech
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd

http://www.phenoelit-us.org

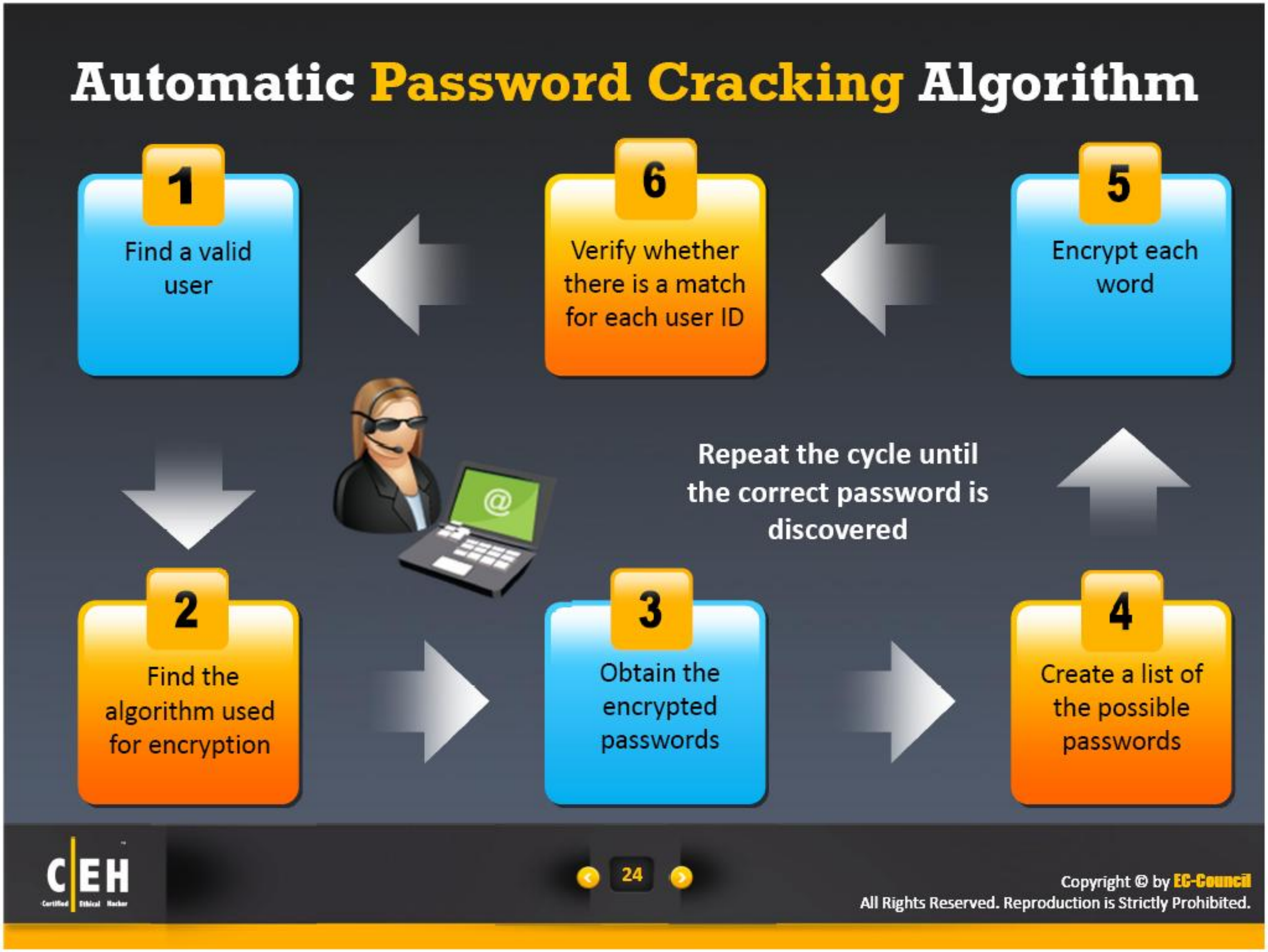


Manual Password Cracking (Guessing)

Frequency of attacks is less

1. Find a valid user
2. Create a list of possible passwords
3. Rank passwords from high probability to low
4. Key in each password, until correct password is discovered

The failure rate is high



Automatic Password Cracking Algorithm

1 Find a valid user

2 Find the algorithm used for encryption

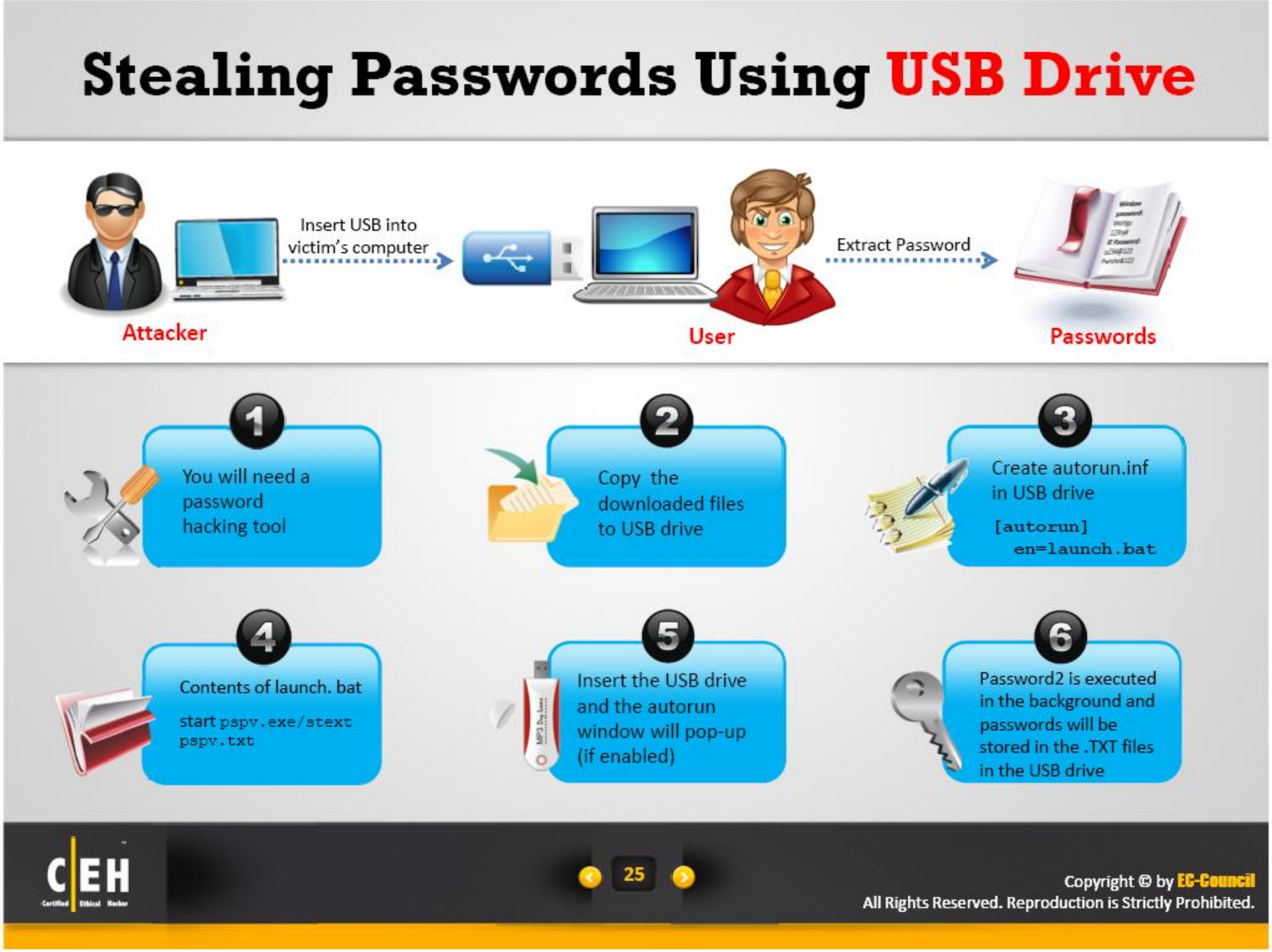
3 Obtain the encrypted passwords

4 Create a list of the possible passwords

5 Encrypt each word

6 Verify whether there is a match for each user ID

Repeat the cycle until the correct password is discovered



Stealing Passwords Using USB Drive

Attacker

Insert USB into victim's computer

User

Extract Password

Passwords

1. You will need a password hacking tool

2. Copy the downloaded files to USB drive

3. Create autorun.inf in USB drive

```
[autorun]
  en=launch.bat
```

4. Contents of launch. bat

start `pspv.exe/stext pspv.txt`

5. Insert the USB drive and the autorun window will pop-up (if enabled)

6. Password2 is executed in the background and passwords will be stored in the .TXT files in the USB drive

Microsoft Authentication

SAM Database

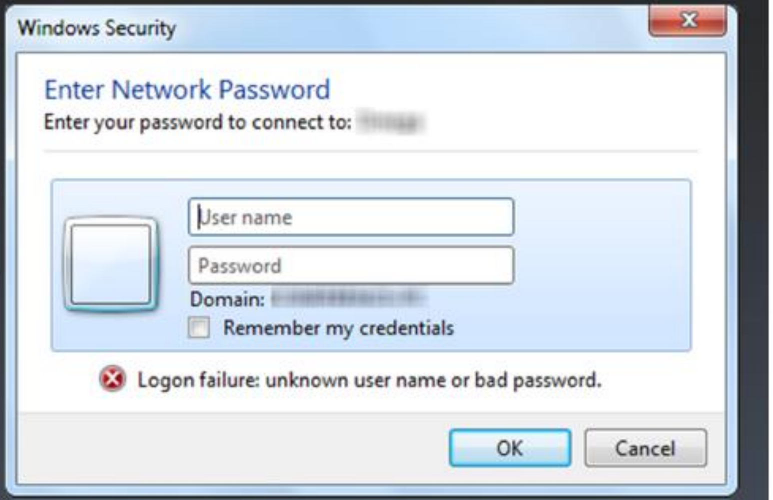
Windows stores user passwords in the Security Accounts Manager database (SAM), or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed and the results are stored in the SAM

NTLM Authentication

The NTLM authentication protocol consists of two authentication protocols: the NTLM and the LM authentication protocol. These protocols use different hashing methods to securely store a user's password in the SAM database

Kerberos

Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM



Windows Security

Enter Network Password

Enter your password to connect to: [redacted]

User name

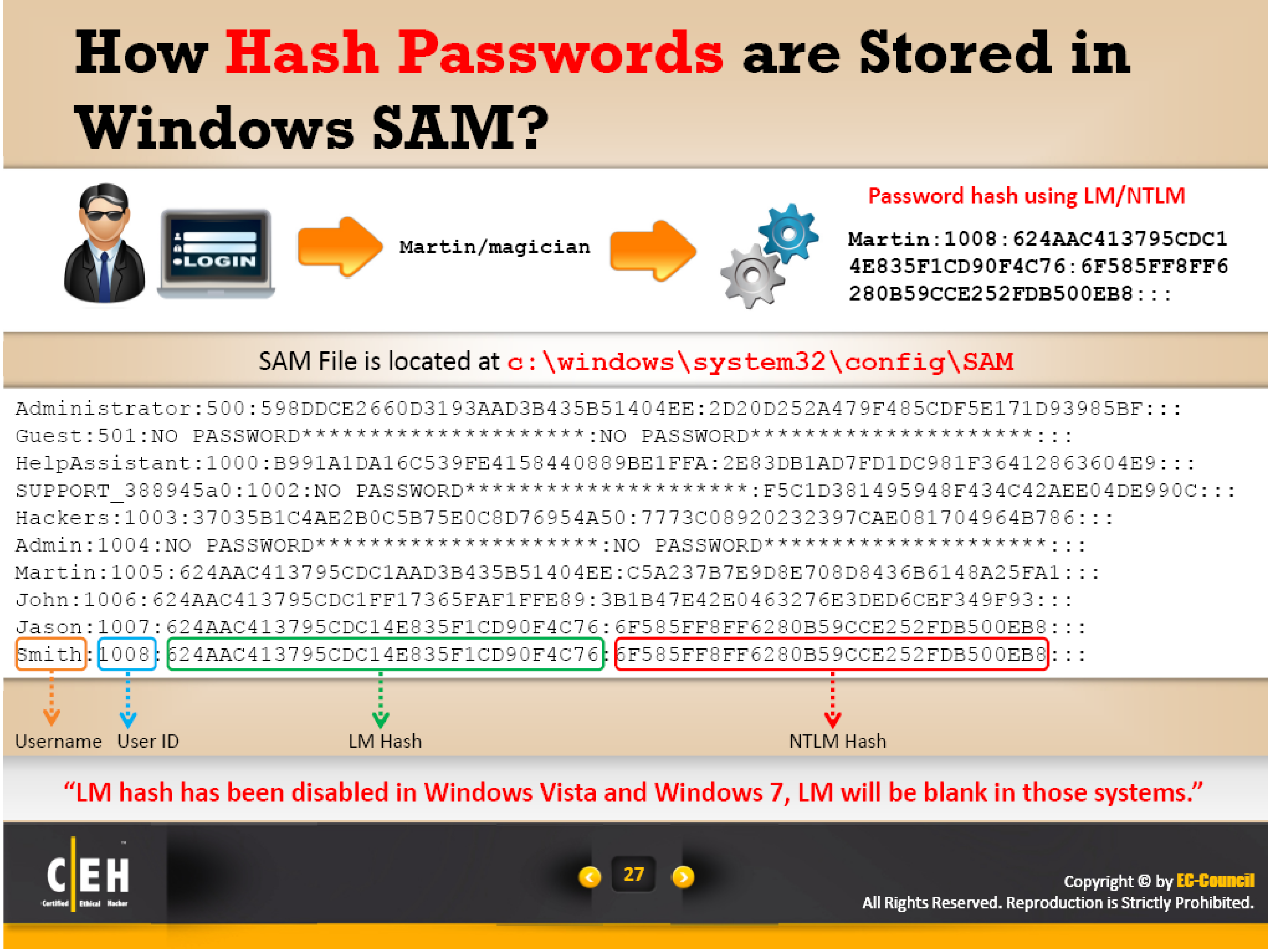
Password

Domain: [redacted]

□ Remember my credentials

Logon failure: unknown user name or bad password.

Windows 7



How Hash Passwords are Stored in Windows SAM?

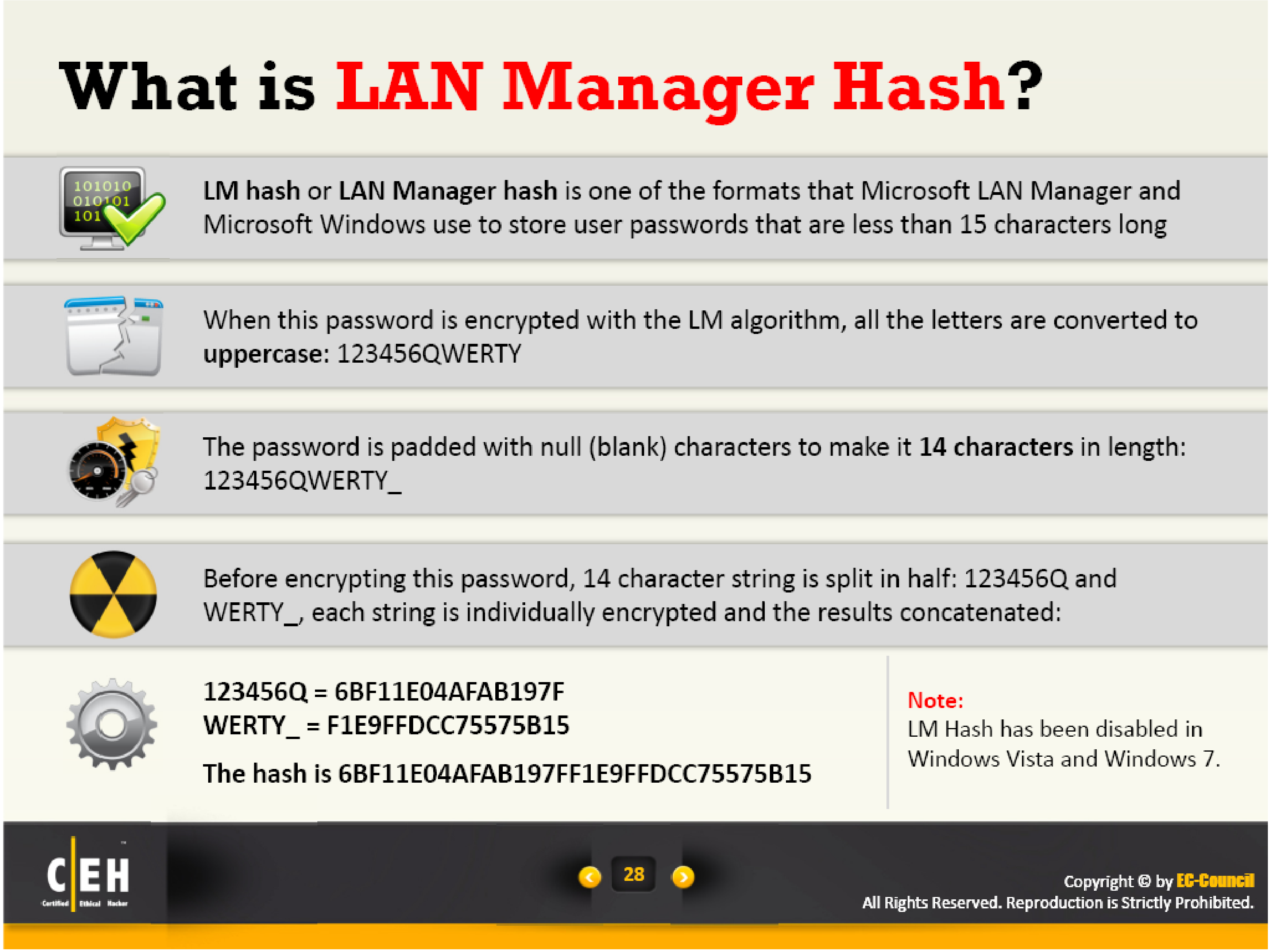
Password hash using LM/NTLM

```
Martin:1008:624AAC413795CDC1
4E835F1CD90F4C76:6F585FF8FF6
280B59CCE252FDB500EB8:::
```

SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:B991A1DA16C539FE4158440889BE1FFA:2E83DB1AD7FD1DC981F36412863604E9:::
SUPPORT_388945a0:1002:NO PASSWORD*********************:F5C1D381495948F434C42AEE04DE990C:::
Hackers:1003:37035B1C4AE2B0C5B75E0C8D76954A50:7773C08920232397CAE081704964B786:::
Admin:1004:NO PASSWORD*********************:NO PASSWORD*********************:::
Martin:1005:624AAC413795CDC1AAD3B435B51404EE:C5A237B7E9D8E708D8436B6148A25FA1:::
John:1006:624AAC413795CDC1FF17365FAF1FFE89:3B1B47E42E0463276E3DED6CEF349F93:::
Jason:1007:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
Smith:1008:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8:::
```

"LM hash has been disabled in Windows Vista and Windows 7, LM will be blank in those systems."



What is LAN Manager Hash?

LM hash or **LAN Manager hash** is one of the formats that Microsoft LAN Manager and Microsoft Windows use to store user passwords that are less than 15 characters long

When this password is encrypted with the LM algorithm, all the letters are converted to **uppercase:** 123456QWERTY

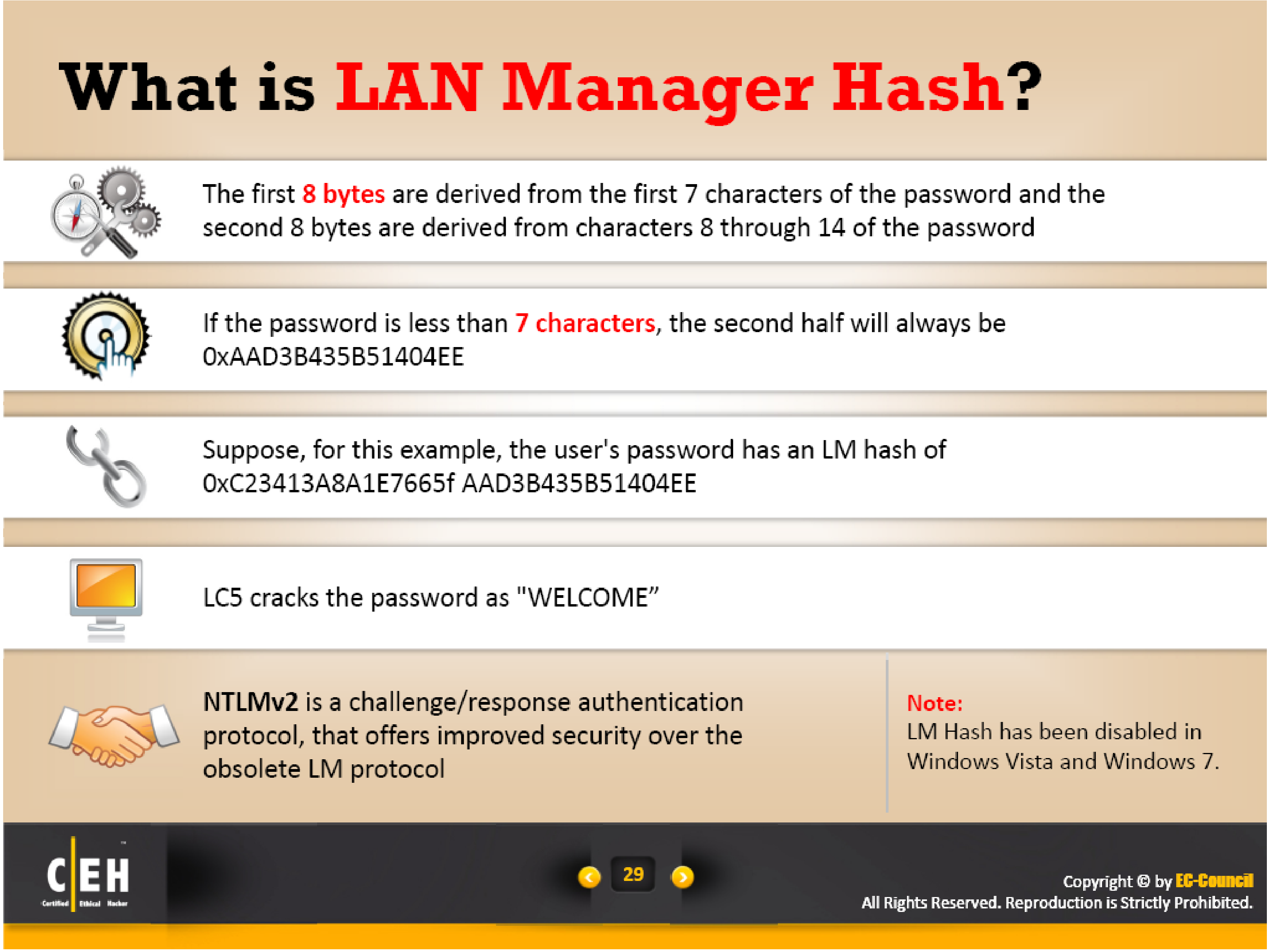
The password is padded with null (blank) characters to make it **14 characters** in length: 123456QWERTY_

Before encrypting this password, 14 character string is split in half: 123456Q and WERTY_, each string is individually encrypted and the results concatenated:

123456Q = 6BF11E04AFAB197F
WERTY_ = F1E9FFDCC75575B15

The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15

Note:
LM Hash has been disabled in Windows Vista and Windows 7.



What is LAN Manager Hash?

The first 8 bytes are derived from the first 7 characters of the password and the second 8 bytes are derived from characters 8 through 14 of the password

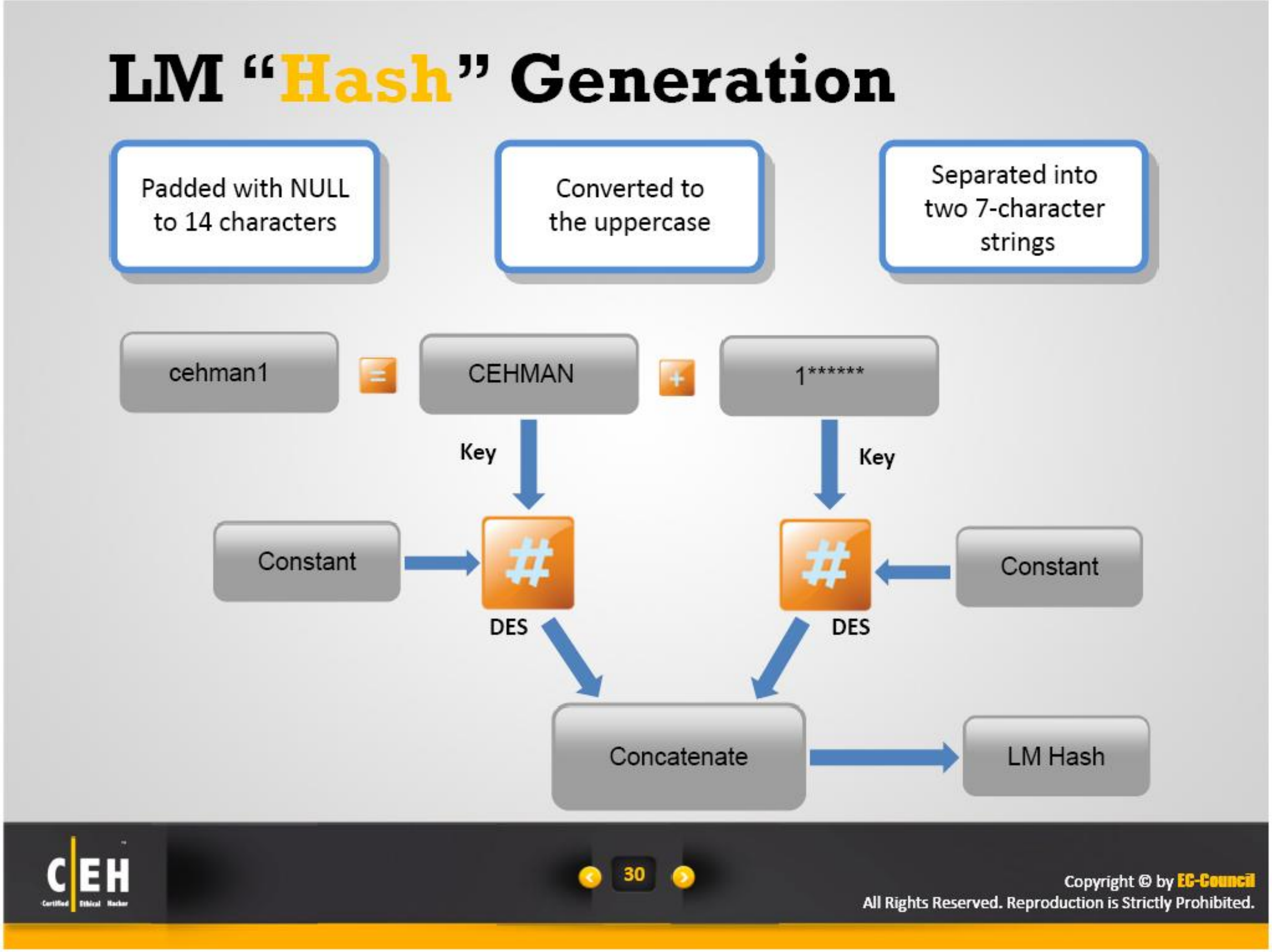
If the password is less than 7 characters, the second half will always be 0xAAD3B435B51404EE

Suppose, for this example, the user's password has an LM hash of 0xC23413A8A1E7665f AAD3B435B51404EE

LC5 cracks the password as "WELCOME”

NTLMv2 is a challenge/response authentication protocol, that offers improved security over the obsolete LM protocol

Note:
LM Hash has been disabled in Windows Vista and Windows 7.



LM "Hash" Generation

Padded with NULL to 14 characters

Converted to the uppercase

Separated into two 7-character strings

cehman1 = CEHMAN + 1******

Key

Key

Constant

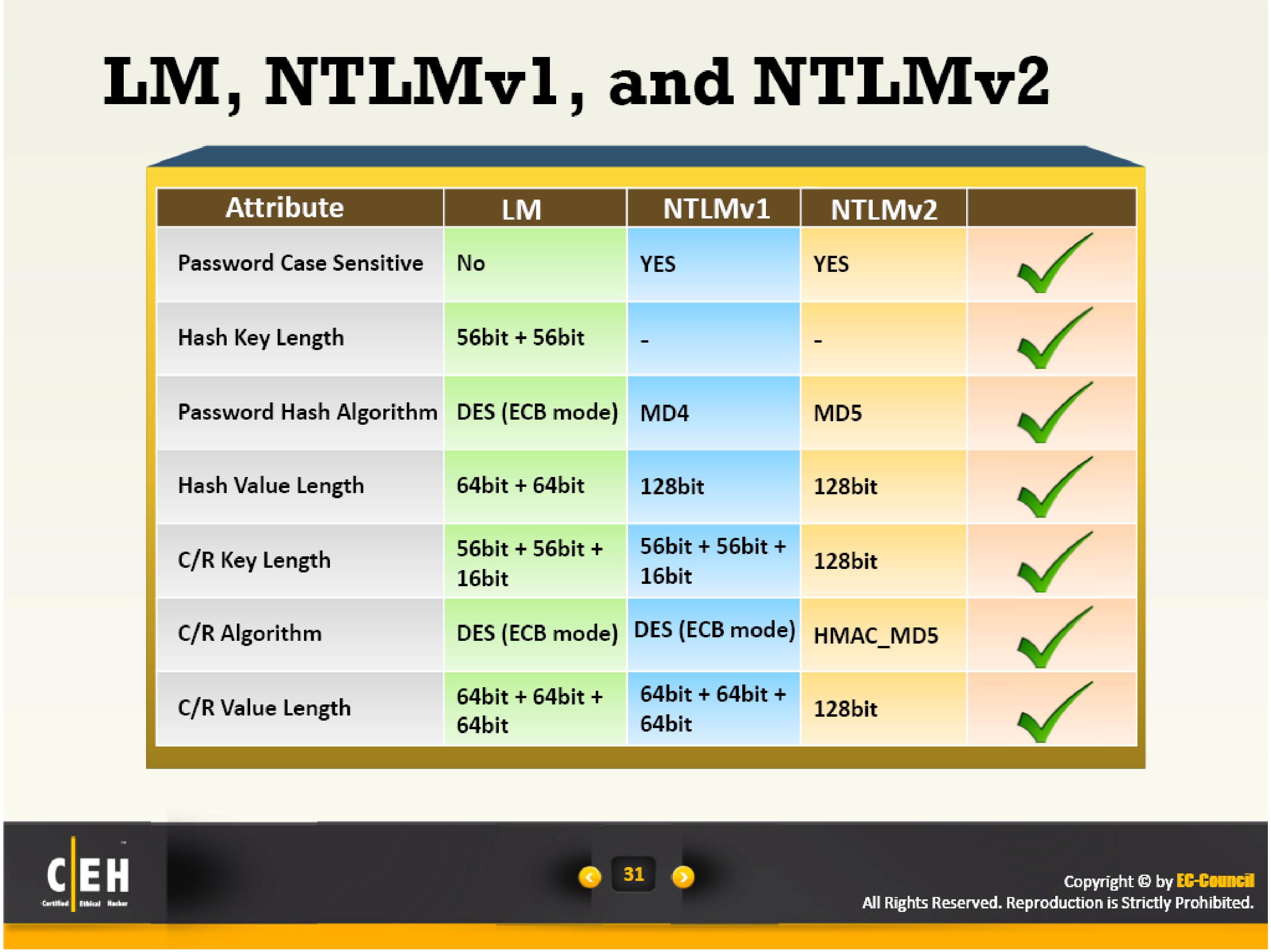
Constant

DES

DES

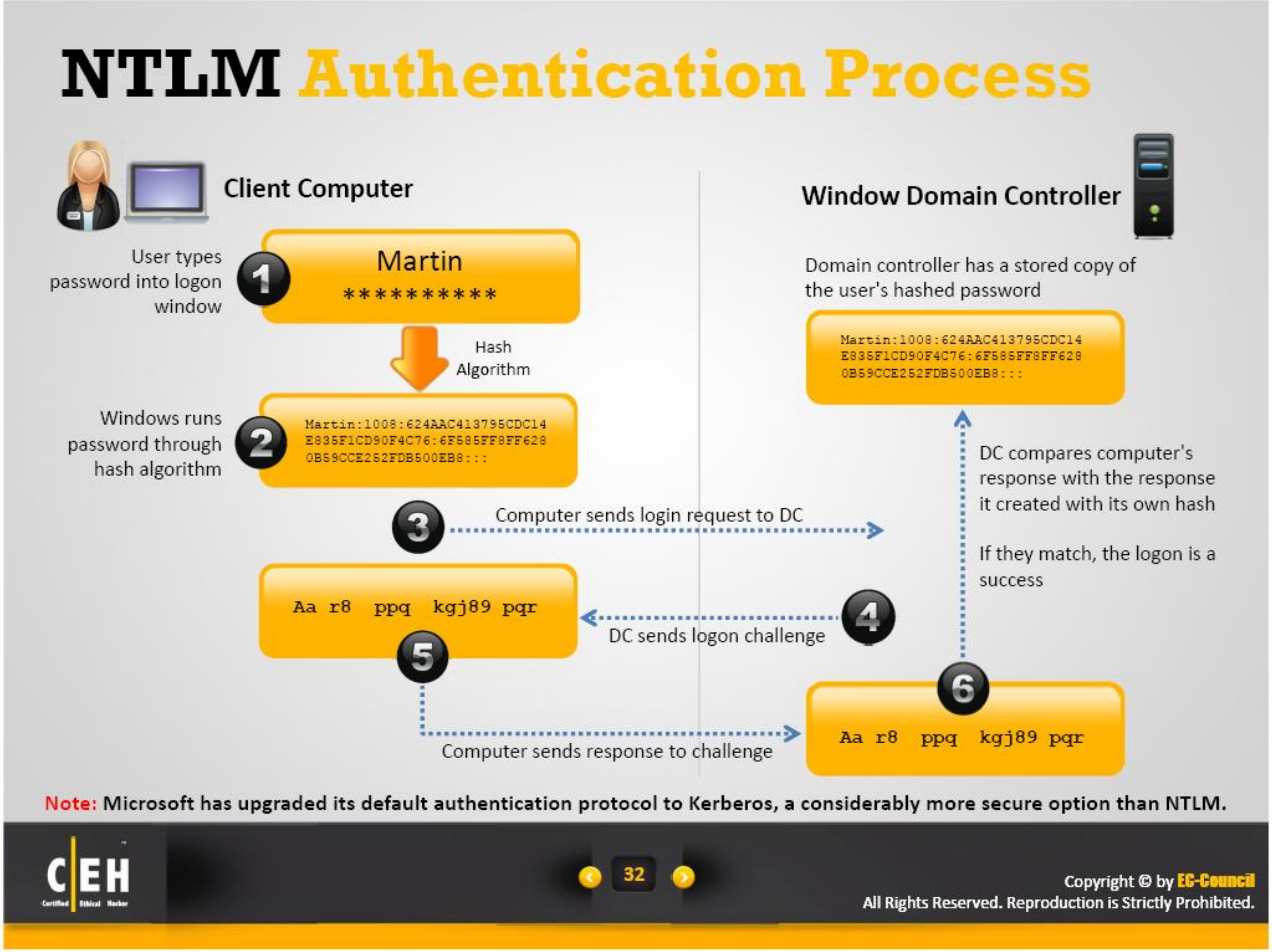
Concatenate

LM Hash



LM, NTLMv1, and NTLMv2

Attribute	LM	NTLMv1	NTLMv2	
Password Case Sensitive	No	YES	YES	✓
Hash Key Length	56bit + 56bit	-	-	✓
Password Hash Algorithm	DES (ECB mode)	MD4	MD5	✓
Hash Value Length	64bit + 64bit	128bit	128bit	✓
C/R Key Length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	✓
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	✓
C/R Value Length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	✓



NTLM Authentication Process

Client Computer

Window Domain Controller

1. User types password into logon window

Martin
****

Hash Algorithm

2. Windows runs password through hash algorithm

```
Martin:1008:624AAC413795CDC14
E835F1CD90F4C76:6F585FF8FF628
0B59CCE252FDB500EB8:::
```

3. Computer sends login request to DC

4. DC sends logon challenge

```
Aa r8  ppq  kgj89 pqr
```

5. Computer sends response to challenge

Domain controller has a stored copy of the user's hashed password

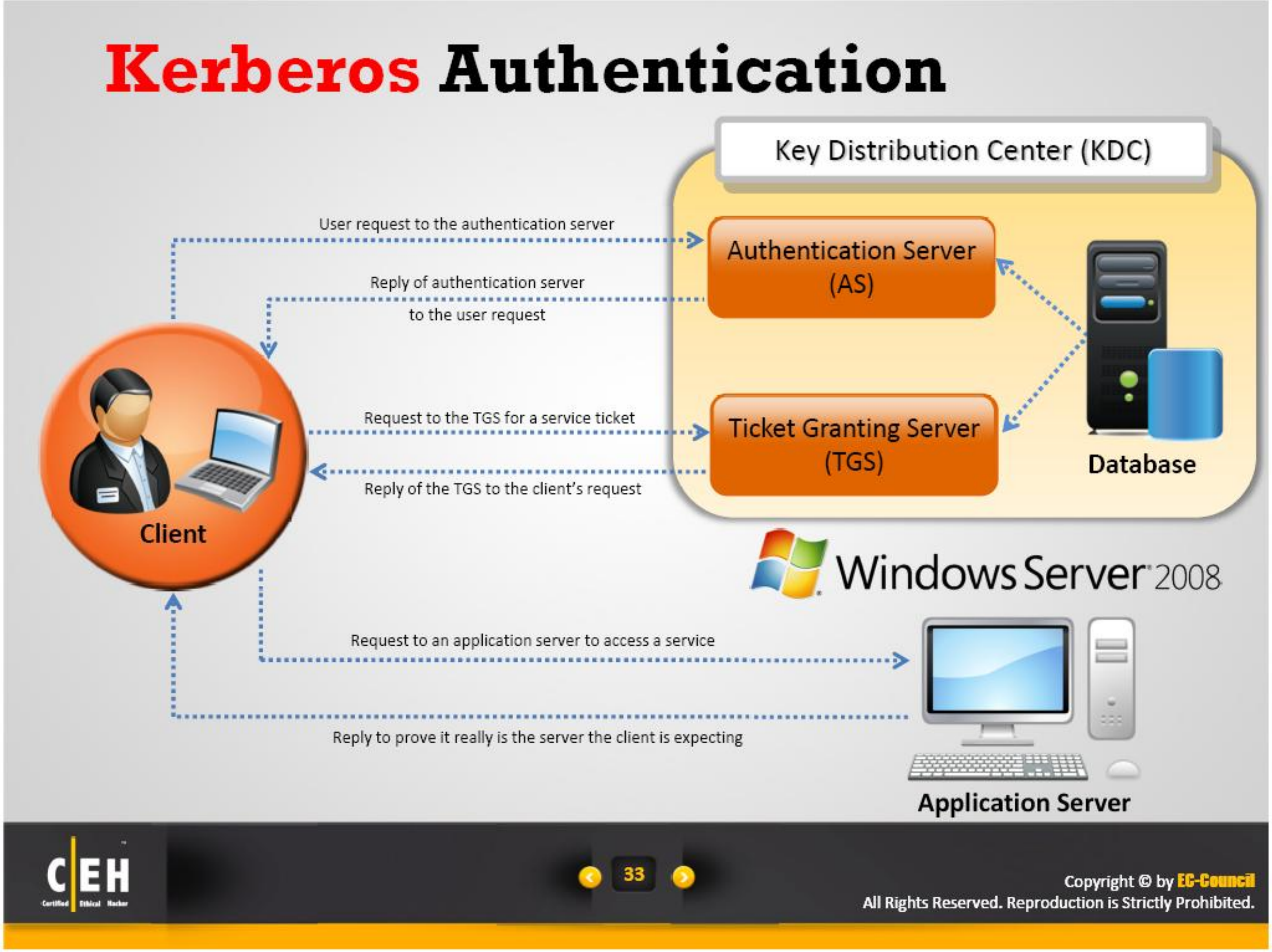
```
Martin:1008:624AAC413795CDC14
E835F1CD90F4C76:6F585FF8FF628
0B59CCE252FDB500EB8:::
```

6. DC compares computer's response with the response it created with its own hash

If they match, the logon is a success

```
Aa r8  ppq  kgj89 pqr
```

Note: Microsoft has upgraded its default authentication protocol to Kerberos, a considerably more secure option than NTLM.



Kerberos Authentication

Key Distribution Center (KDC)

Authentication Server (AS)

Ticket Granting Server (TGS)

Database

Client

User request to the authentication server

Reply of authentication server to the user request

Request to the TGS for a service ticket

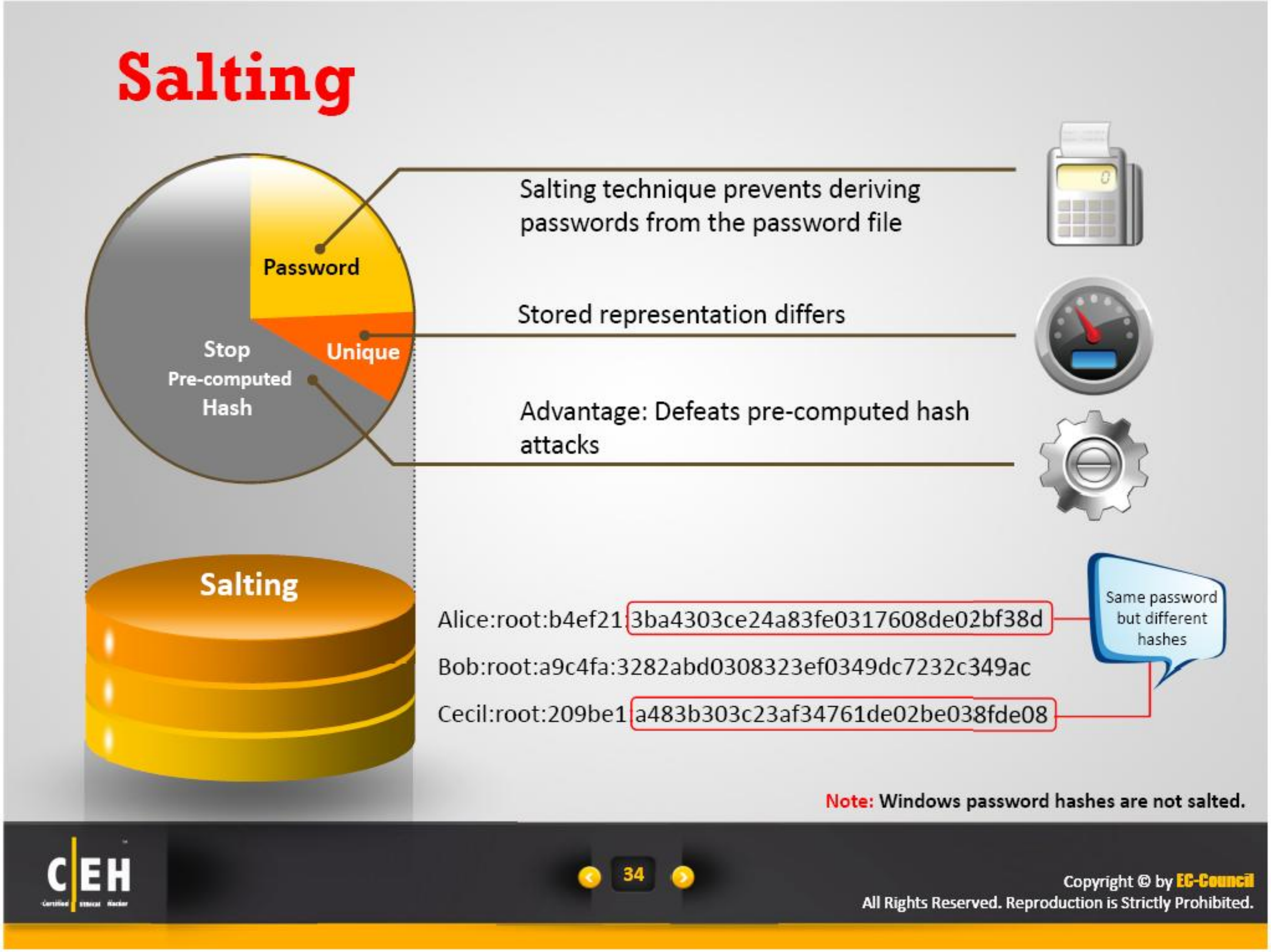
Reply of the TGS to the client's request

Request to an application server to access a service

Reply to prove it really is the server the client is expecting

Windows Server 2008

Application Server



Salting

Salting technique prevents deriving passwords from the password file

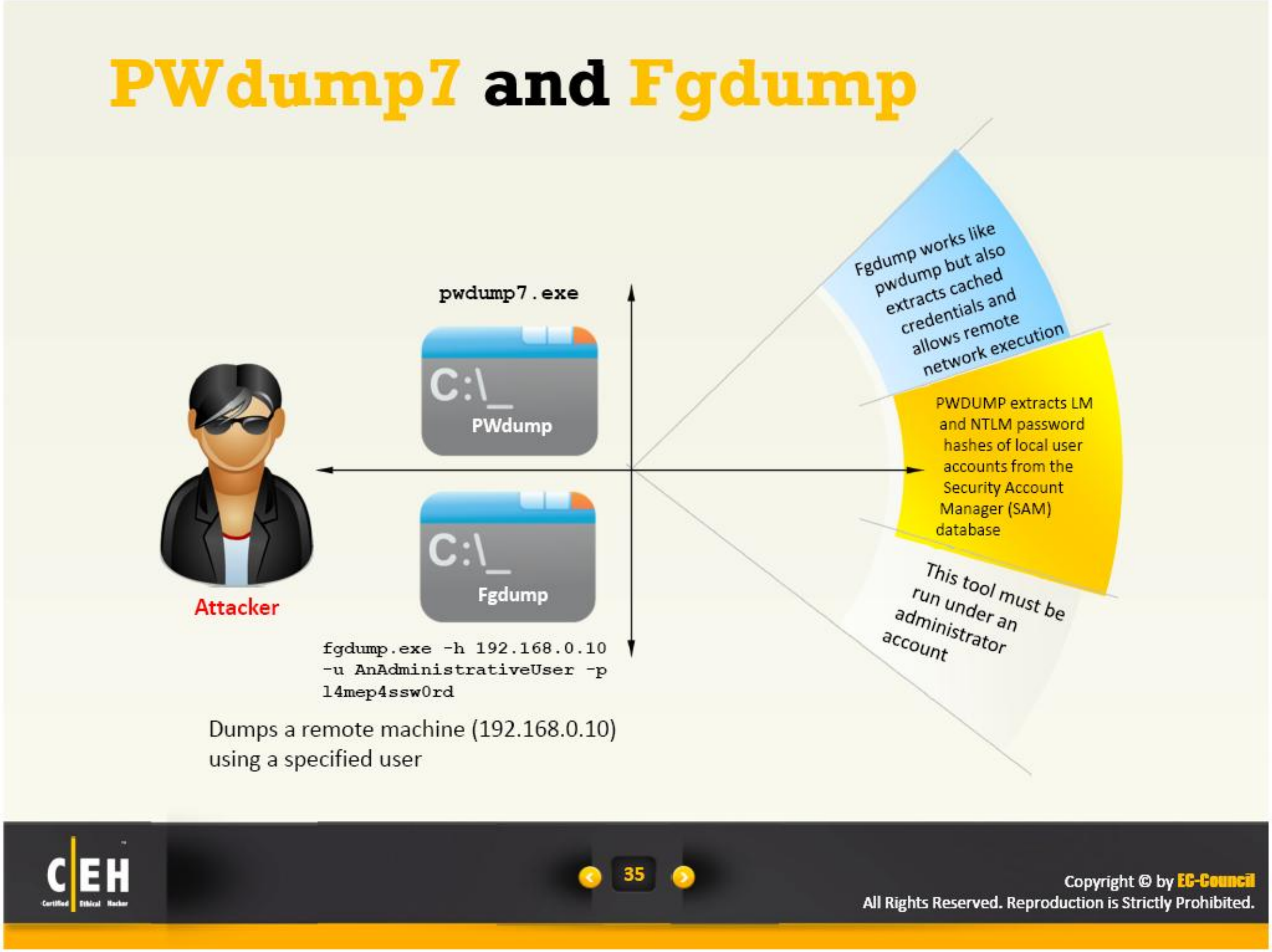
Stored representation differs

Advantage: Defeats pre-computed hash attacks

```
Alice:root:b4ef21:3ba4303ce24a83fe0317608de02bf38d
Bob:root:a9c4fa:3282abd0308323ef0349dc7232c349ac
Cecil:root:209be1a483b303c23af34761de02be038fde08
```

Same password but different hashes

Note: Windows password hashes are not salted.



PWdump7 and Fgdump

```
pwdump7.exe
```

```
fgdump.exe -h 192.168.0.10
-u AnAdministrativeUser -p
14mep4ssw0rd
```

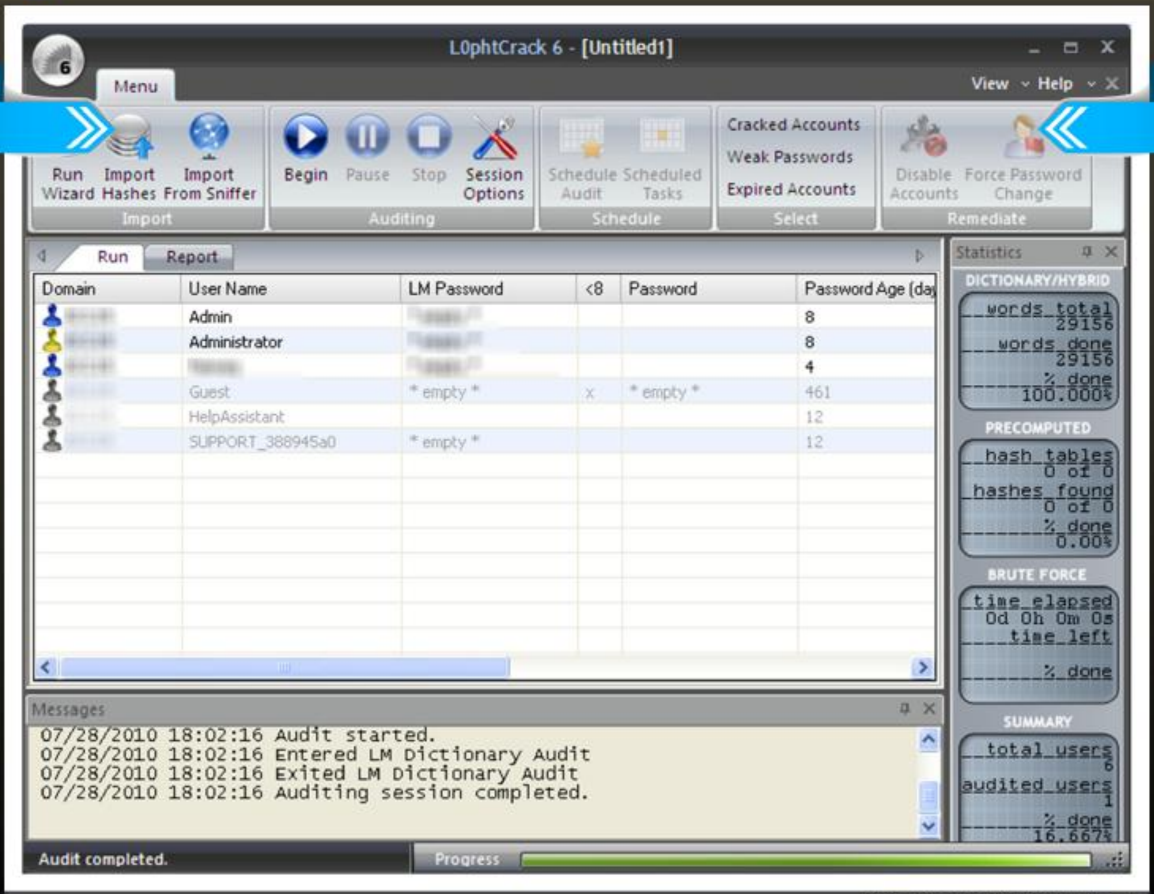
Dumps a remote machine (192.168.0.10) using a specified user

Fgdump works like pwdump but also extracts cached credentials and allows remote network execution

PWDUMP extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database

This tool must be run under an administrator account

L0phtCrack



Domain	User Name	LM Password	<8	Password	Password Age (day
[redacted]	Admin	[redacted]			8
[redacted]	Administrator	[redacted]			8
[redacted]	[redacted]	[redacted]			4
[redacted]	Guest	* empty *	x	* empty *	461
[redacted]	HelpAssistant				12
[redacted]	SUPPORT_388945a0	* empty *			12

DICTIONARY/HYBRID

```
words total 29156
words done 29156
% done 100.000%
```

PRECOMPUTED

```
hash tables 0 of 0
hashes found 0 of 0
% done 0.00%
```

BRUTE FORCE

```
time elapsed 0d 0h 0m 0s
time left
% done
```

SUMMARY

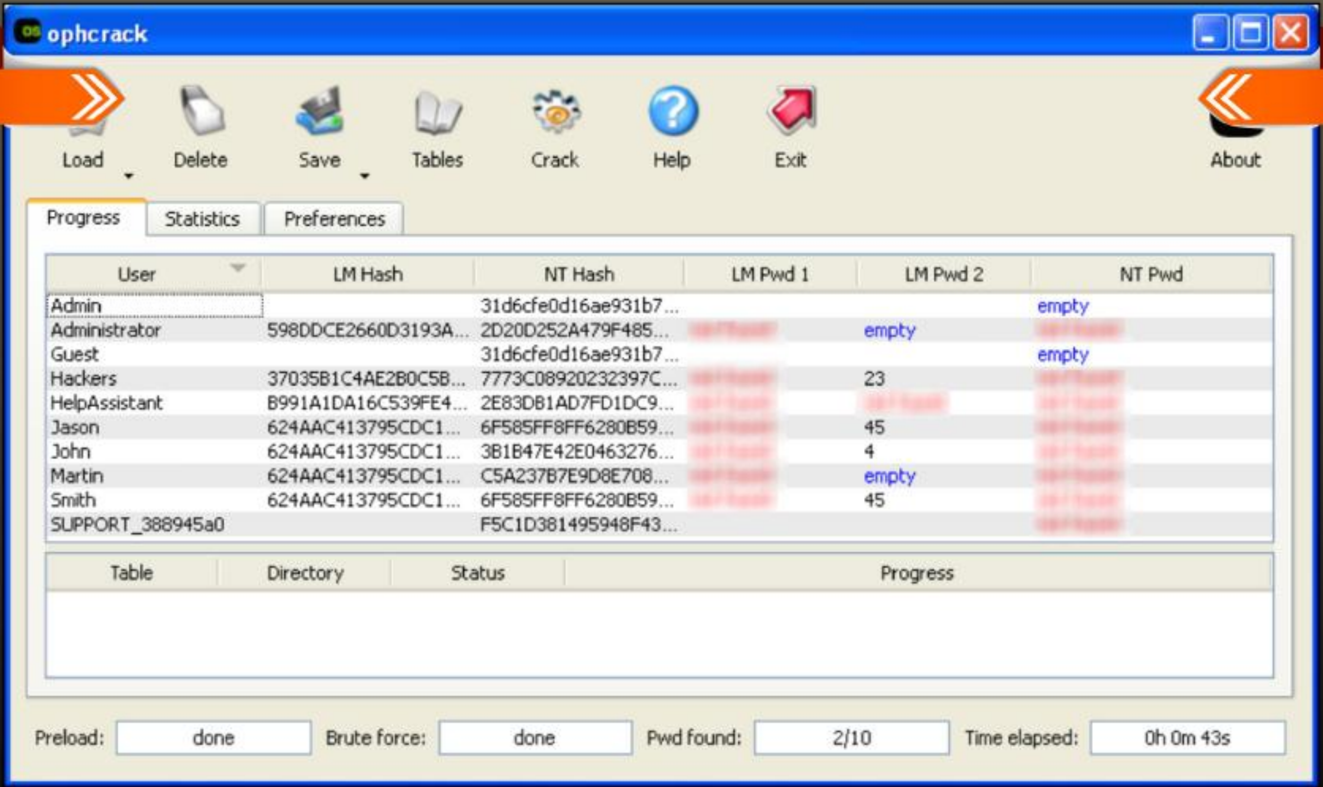
```
total users 6
audited users 1
% done 16.667%
```

```
07/28/2010 18:02:16 Audit started.
07/28/2010 18:02:16 Entered LM Dictionary Audit
07/28/2010 18:02:16 Exited LM Dictionary Audit
07/28/2010 18:02:16 Auditing session completed.
```

Audit completed.

http://www.l0phtcrack.com

Ophcrack



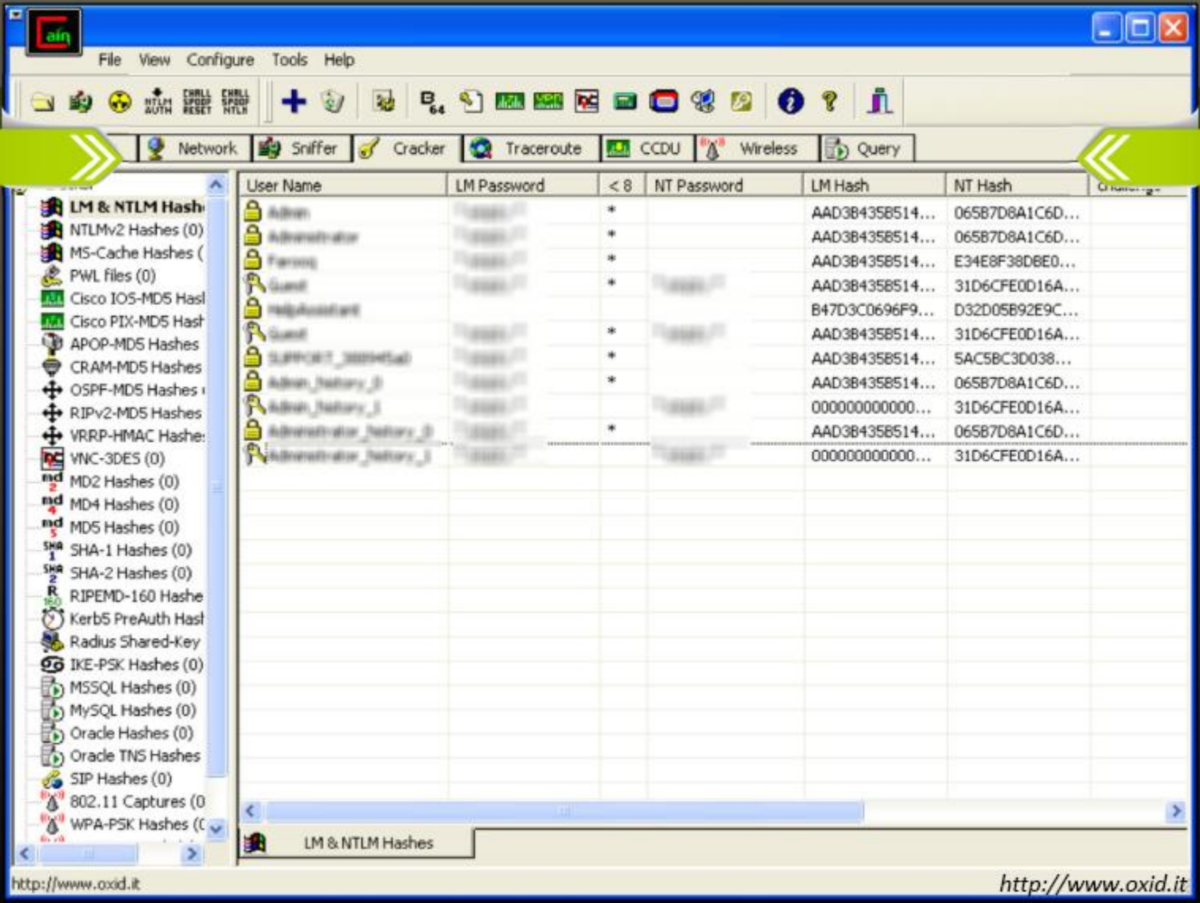
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Admin		31d6cfe0d16ae931b7...			empty
Administrator	598DDCE2660D3193A...	2D20D252A479F485...	[redacted]	empty	[redacted]
Guest		31d6cfe0d16ae931b7...			empty
Hackers	37035B1C4AE2B0C5B...	7773C08920232397C...	[redacted]	23	[redacted]
HelpAssistant	B991A1DA16C539FE4...	2E83DB1AD7FD1DC9...	[redacted]	[redacted]	[redacted]
Jason	624AAC413795CDC1...	6F585FF8FF6280B59...	[redacted]	45	[redacted]
John	624AAC413795CDC1...	3B1B47E42E0463276...	[redacted]	4	[redacted]
Martin	624AAC413795CDC1...	C5A237B7E9D8E708...	[redacted]	empty	[redacted]
Smith	624AAC413795CDC1...	6F585FF8FF6280B59...	[redacted]	45	[redacted]
SUPPORT_388945a0		F5C1D381495948F43...			[redacted]

Table	Directory	Status	Progress

Preload: done Brute force: done Pwd found: 2/10 Time elapsed: 0h 0m 43s

http://ophcrack.sourceforge.net

Cain & Abel

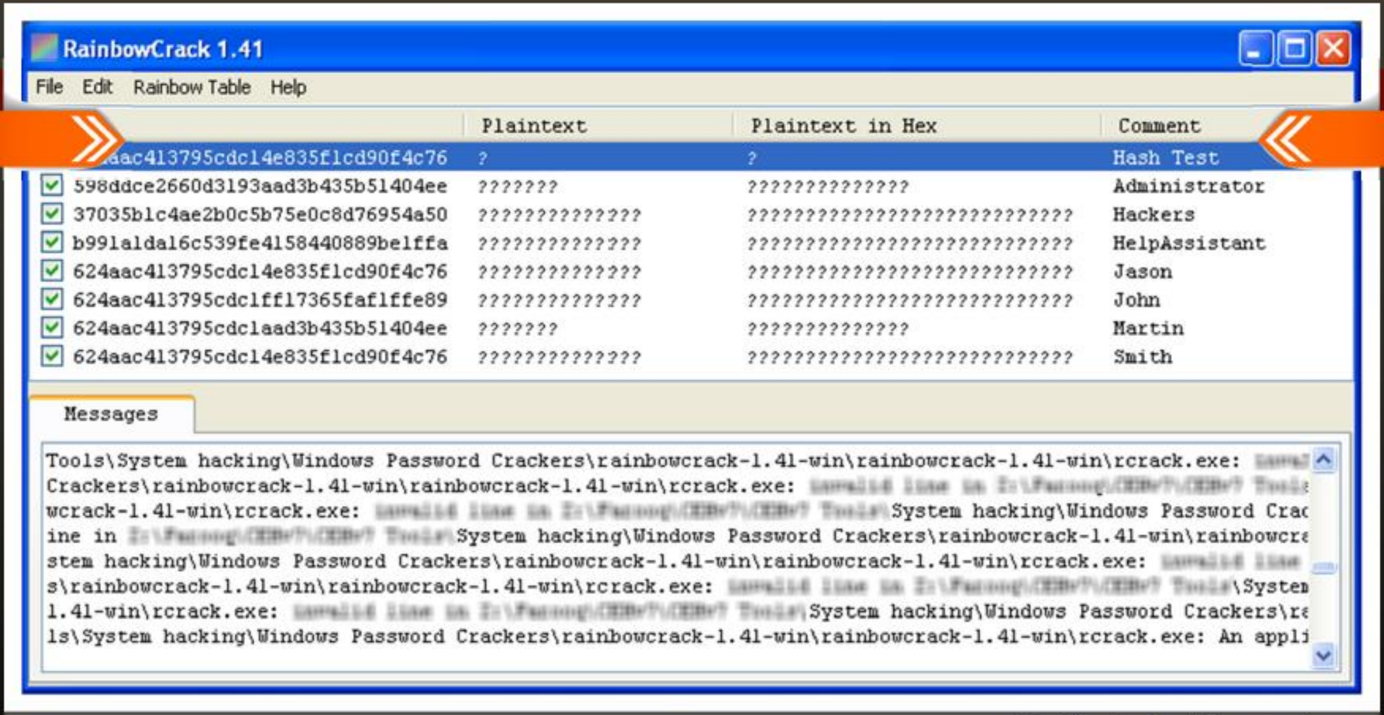


- LM & NTLM Hash
- NTLMv2 Hashes (0)
- MS-Cache Hashes (
- PWL Files (0)
- Cisco IOS-MD5 Hasl
- Cisco PIX-MD5 Hash
- APOP-MD5 Hashes
- CRAM-MD5 Hashes
- OSPF-MD5 Hashes
- RIPv2-MD5 Hashes
- VRRP-HMAC Hashe
- VNC-3DES (0)
- MD2 Hashes (0)
- MD4 Hashes (0)
- MD5 Hashes (0)
- SHA-1 Hashes (0)
- SHA-2 Hashes (0)
- RIPEMD-160 Hashe
- Kerb5 PreAuth Hasl
- Radius Shared-Key
- IKE-PSK Hashes (0)
- MSSQL Hashes (0)
- MySQL Hashes (0)
- Oracle Hashes (0)
- Oracle TNS Hashes
- SIP Hashes (0)
- 802.11 Captures (0
- WPA-PSK Hashes (C

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
[redacted]	[redacted]	*		AAD3B435B514...	065B7D8A1C6D...
[redacted]	[redacted]	*		AAD3B435B514...	065B7D8A1C6D...
[redacted]	[redacted]	*		AAD3B435B514...	E34E8F38DBE0...
[redacted]	[redacted]	*	[redacted]	AAD3B435B514...	31D6CFE0D16A...
[redacted]				B47D3C0696F9...	D32D05B92E9C...
[redacted]	[redacted]	*	[redacted]	AAD3B435B514...	31D6CFE0D16A...
[redacted]	[redacted]	*		AAD3B435B514...	5AC5BC3D038...
[redacted]	[redacted]	*		AAD3B435B514...	065B7D8A1C6D...
[redacted]	[redacted]		[redacted]	000000000000...	31D6CFE0D16A...
[redacted]	[redacted]	*		AAD3B435B514...	065B7D8A1C6D...
[redacted]	[redacted]		[redacted]	000000000000...	31D6CFE0D16A...

http://www.oxid.it

RainbowCrack

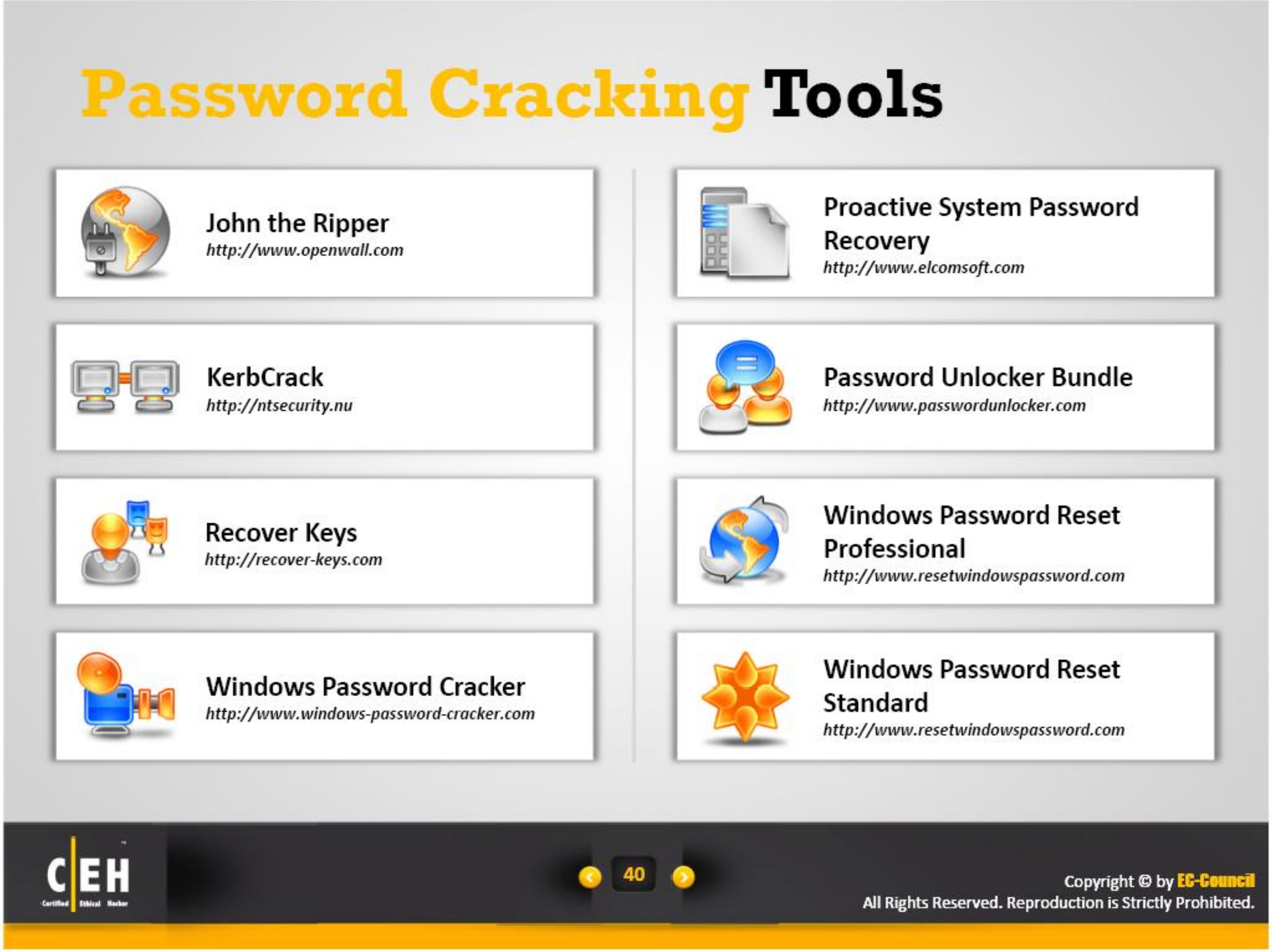


		Plaintext	Plaintext in Hex	Comment
	aac413795cdc14e835f1cd90f4c76	?	?	Hash Test
☑	598ddce2660d3193aad3b435b51404ee	???????	??????????????	Administrator
☑	37035b1c4ae2b0c5b75e0c8d76954a50	??????????????	????????????????????????????	Hackers
☑	b991a1da16c539fe4158440889be1ffa	??????????????	????????????????????????????	HelpAssistant
☑	624aac413795cdc14e835f1cd90f4c76	??????????????	????????????????????????????	Jason
☑	624aac413795cdc1ff17365fa f1ffe89	??????????????	????????????????????????????	John
☑	624aac413795cdc1aad3b435b51404ee	???????	??????????????	Martin
☑	624aac413795cdc14e835f1cd90f4c76	??????????????	????????????????????????????	Smith

Messages

```
Tools\System hacking\Windows Password Crackers\rainbowcrack-1.41-win\rainbowcrack-1.41-win\rcrack.exe: [redacted]
Crackers\rainbowcrack-1.41-win\rainbowcrack-1.41-win\rcrack.exe: [redacted]
wcrack-1.41-win\rcrack.exe: [redacted]System hacking\Windows Password Crac
ine in [redacted]System hacking\Windows Password Crackers\rainbowcrack-1.41-win\rainbowcra
stem hacking\Windows Password Crackers\rainbowcrack-1.41-win\rainbowcrack-1.41-win\rcrack.exe: [redacted]
s\rainbowcrack-1.41-win\rainbowcrack-1.41-win\rcrack.exe: [redacted]\System
1.41-win\rcrack.exe: [redacted]System hacking\Windows Password Crackers\ra
ls\System hacking\Windows Password Crackers\rainbowcrack-1.41-win\rainbowcrack-1.41-win\rcrack.exe: An appli
```

http://project-rainbowcrack.com



Password Cracking Tools

John the Ripper
http://www.openwall.com

KerbCrack
http://ntsecurity.nu

Recover Keys
http://recover-keys.com

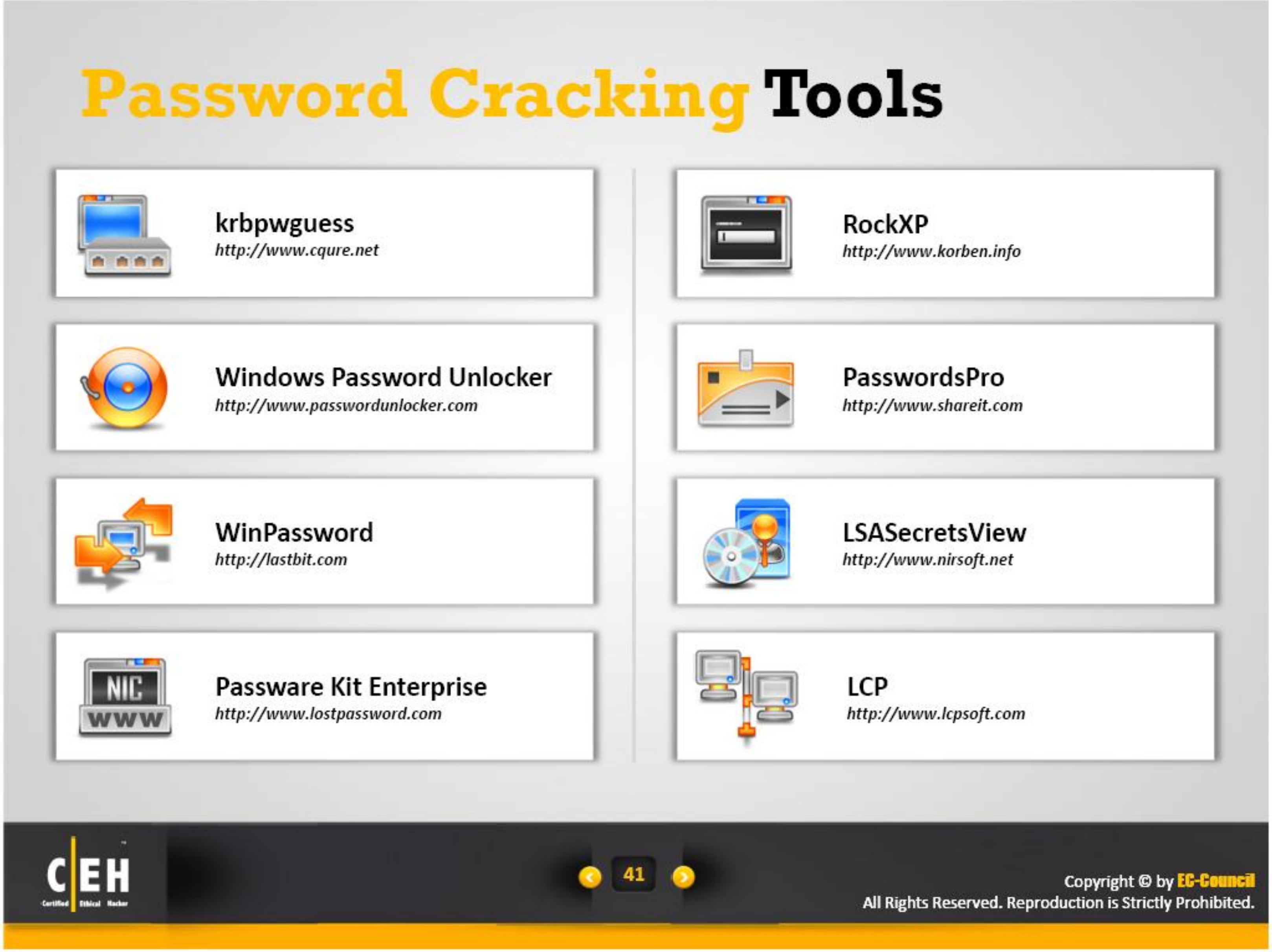
Windows Password Cracker
http://www.windows-password-cracker.com

Proactive System Password Recovery
http://www.elcomsoft.com

Password Unlocker Bundle
http://www.passwordunlocker.com

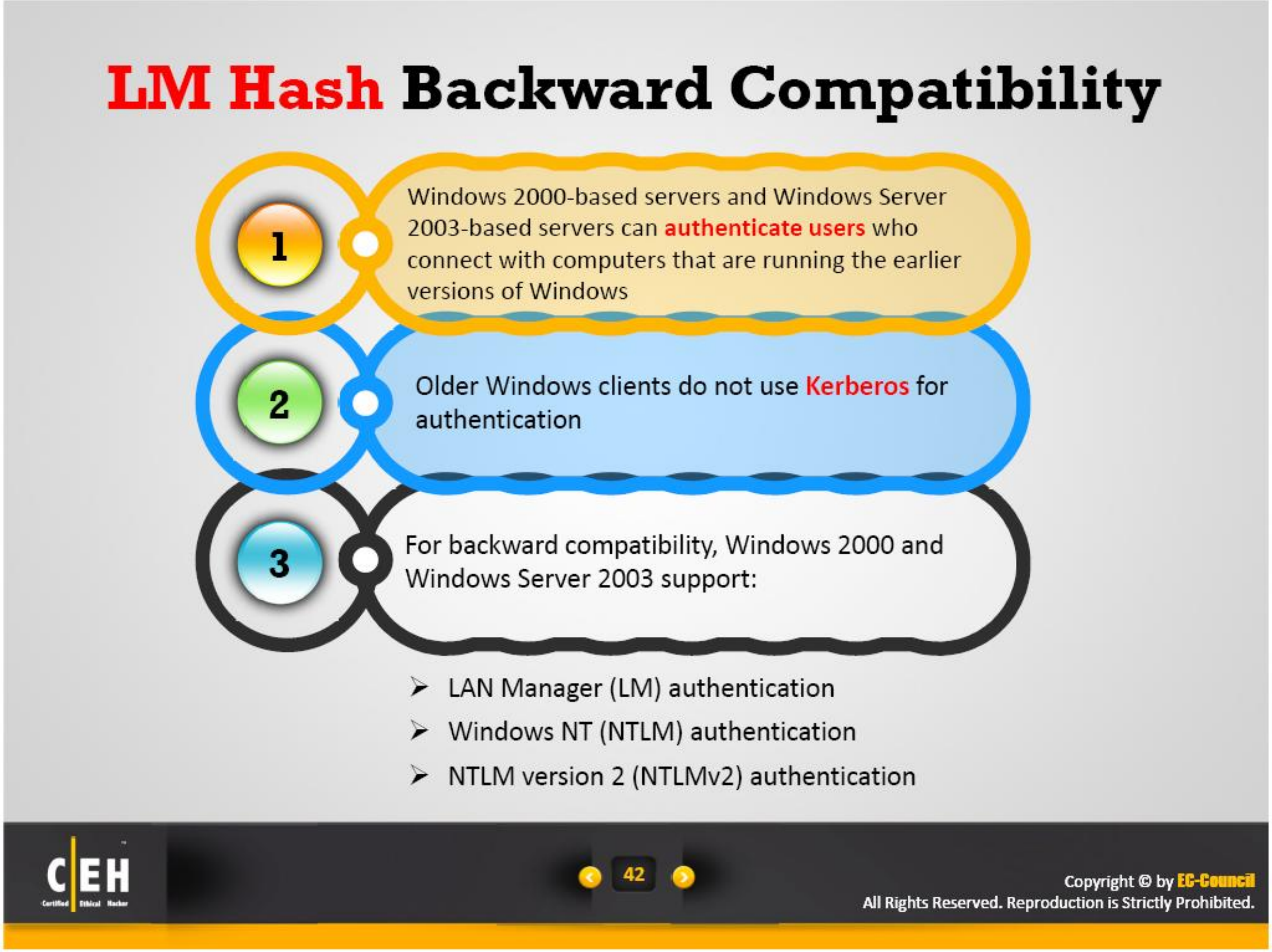
Windows Password Reset Professional
http://www.resetwindowspassword.com

Windows Password Reset Standard
http://www.resetwindowspassword.com



Password Cracking Tools

- krbpwguess
  http://www.cqure.net
- Windows Password Unlocker
  http://www.passwordunlocker.com
- WinPassword
  http://lastbit.com
- Passware Kit Enterprise
  http://www.lostpassword.com
- RockXP
  http://www.korben.info
- PasswordsPro
  http://www.shareit.com
- LSASecretsView
  http://www.nirsoft.net
- LCP
  http://www.lcpsoft.com



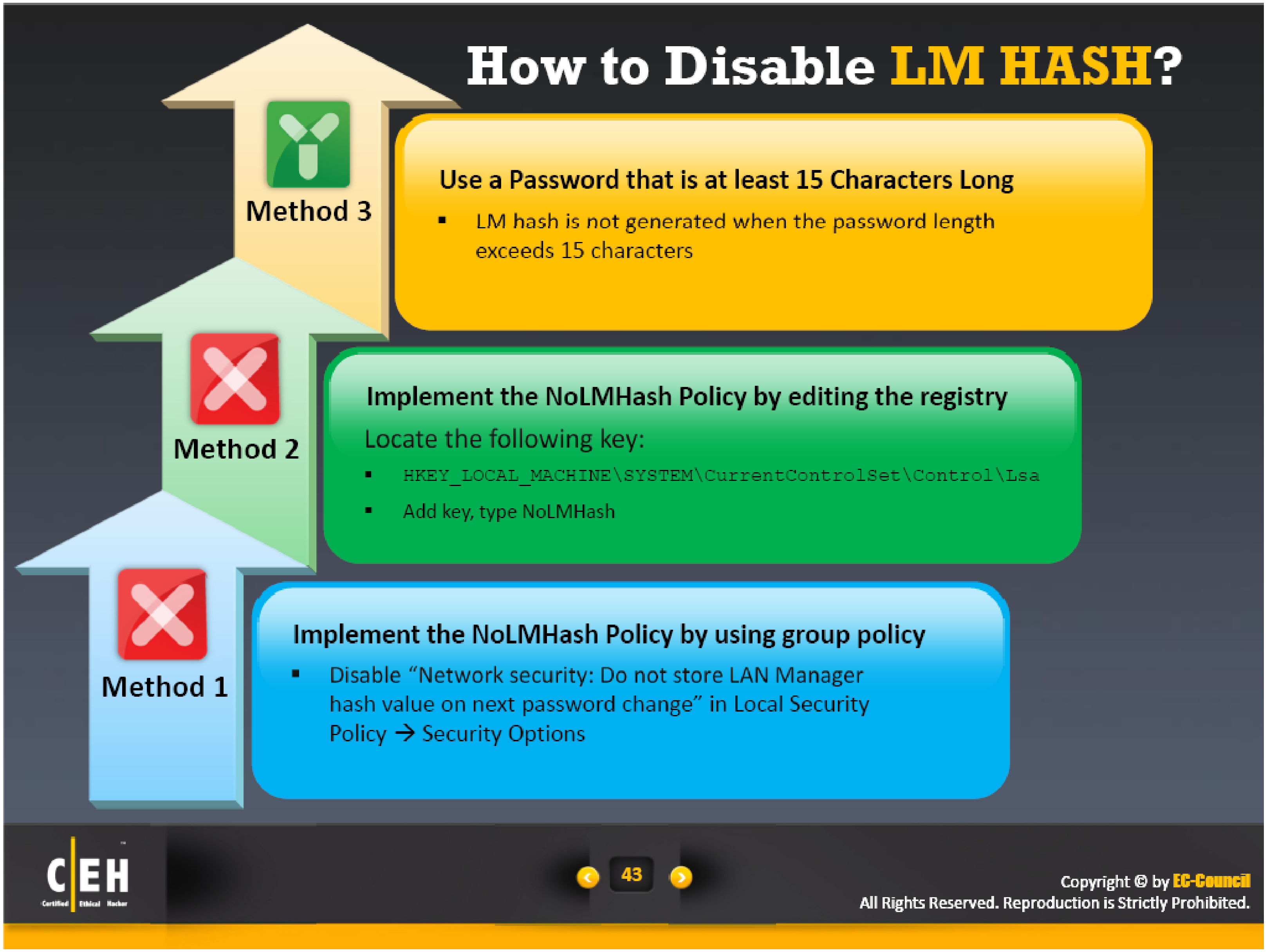
LM Hash Backward Compatibility

1 Windows 2000-based servers and Windows Server 2003-based servers can **authenticate users** who connect with computers that are running the earlier versions of Windows

2 Older Windows clients do not use **Kerberos** for authentication

3 For backward compatibility, Windows 2000 and Windows Server 2003 support:

- LAN Manager (LM) authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication



How to Disable LM HASH?

Use a Password that is at least 15 Characters Long

- LM hash is not generated when the password length exceeds 15 characters

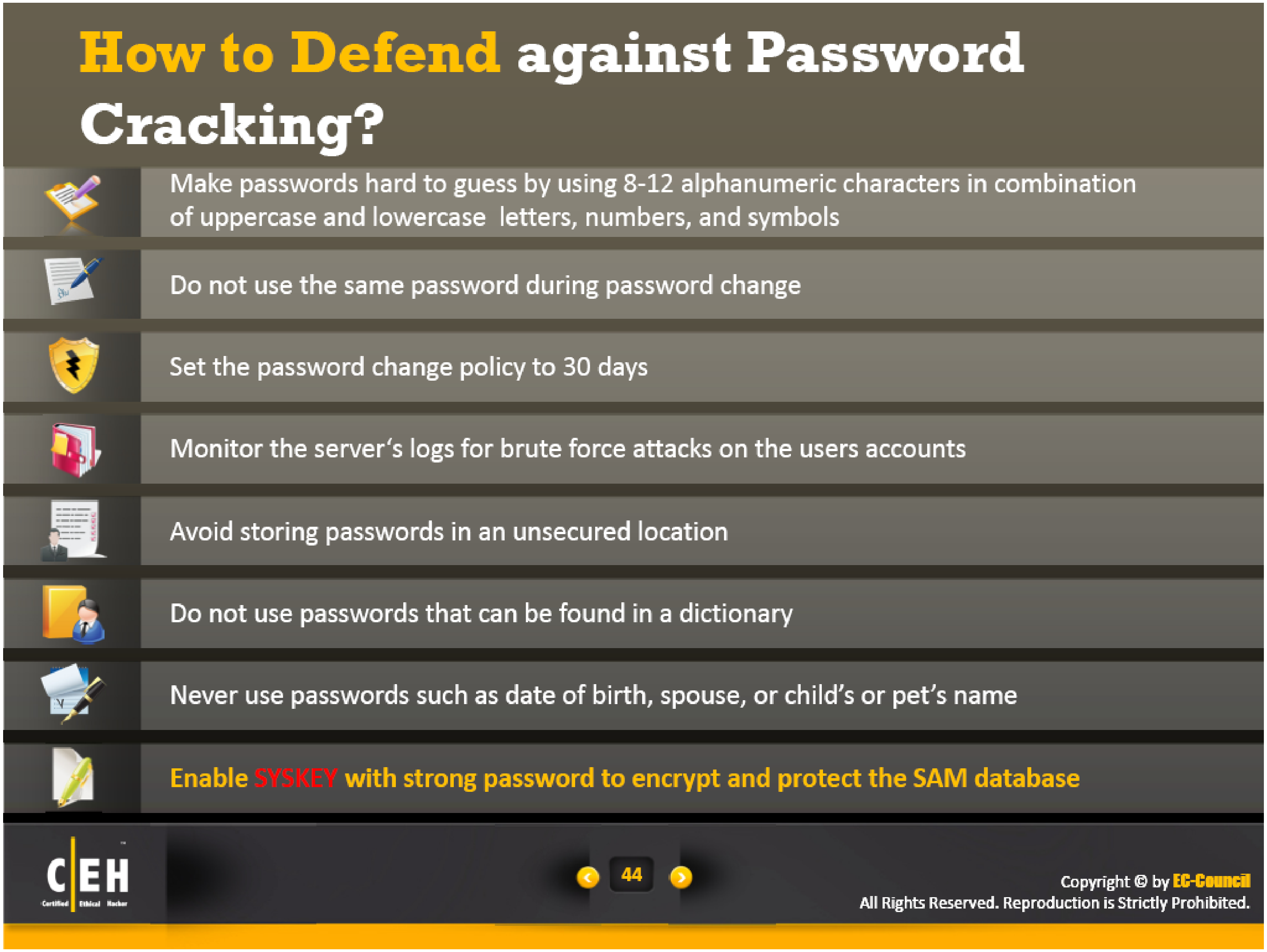
Implement the NoLMHash Policy by editing the registry

Locate the following key:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`
- Add key, type NoLMHash

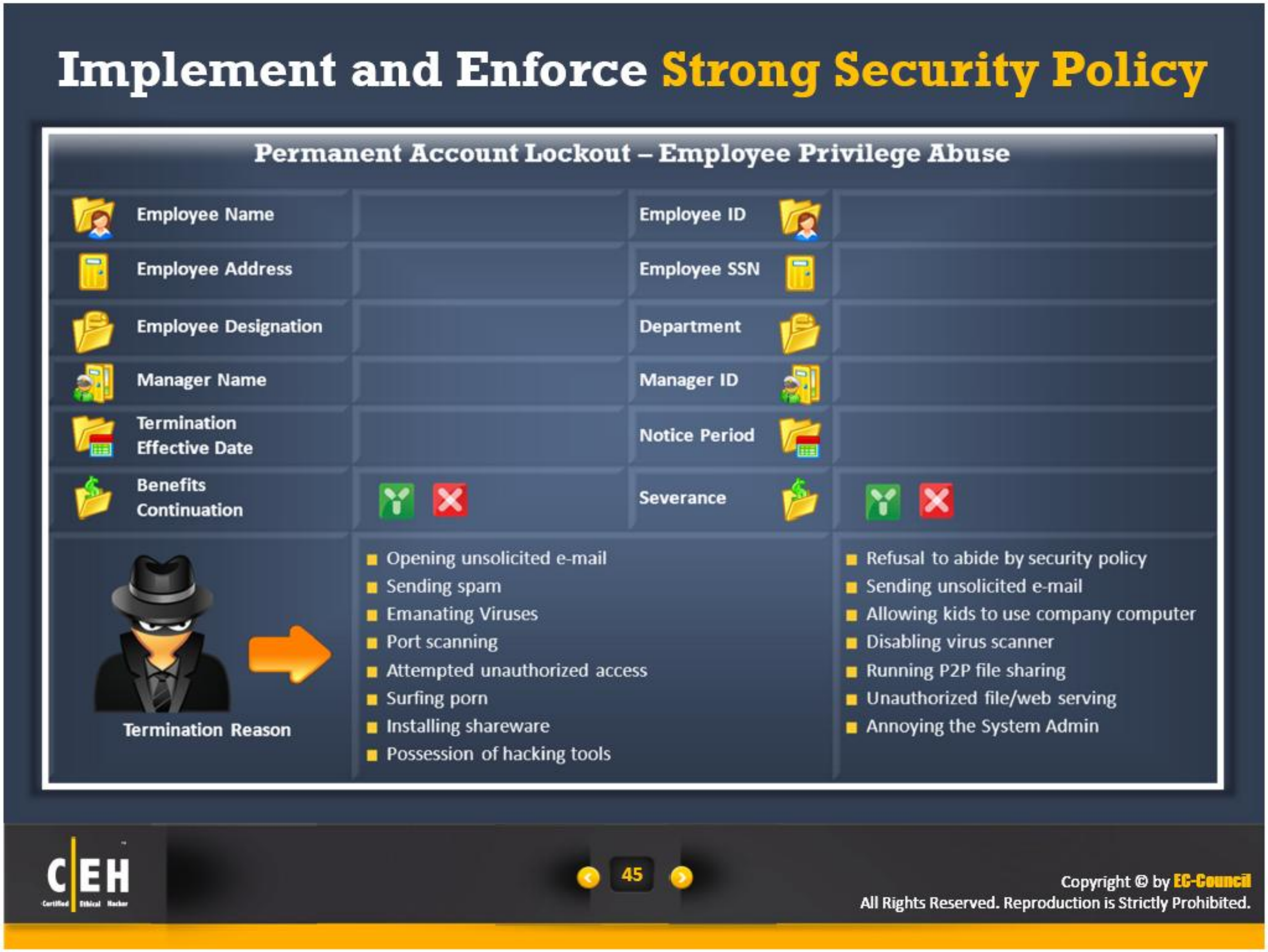
Implement the NoLMHash Policy by using group policy

- Disable “Network security: Do not store LAN Manager hash value on next password change” in Local Security Policy → Security Options



How to Defend against Password Cracking?

- Make passwords hard to guess by using 8-12 alphanumeric characters in combination of uppercase and lowercase letters, numbers, and symbols
- Do not use the same password during password change
- Set the password change policy to 30 days
- Monitor the server's logs for brute force attacks on the users accounts
- Avoid storing passwords in an unsecured location
- Do not use passwords that can be found in a dictionary
- Never use passwords such as date of birth, spouse, or child's or pet's name
- Enable SYSKEY with strong password to encrypt and protect the SAM database



Implement and Enforce Strong Security Policy

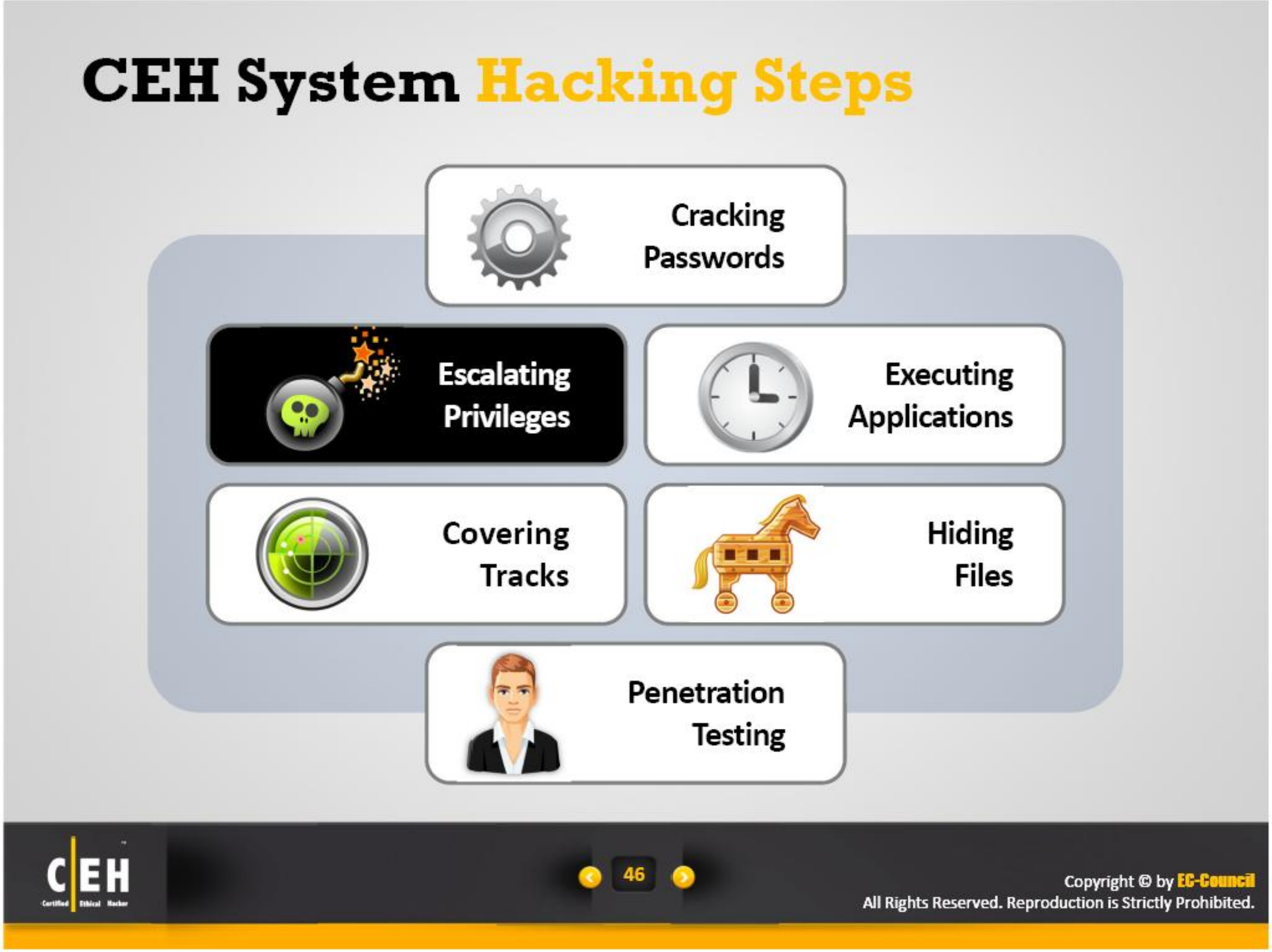
Permanent Account Lockout – Employee Privilege Abuse

Employee Name		Employee ID	
Employee Address		Employee SSN	
Employee Designation		Department	
Manager Name		Manager ID	
Termination Effective Date		Notice Period	
Benefits Continuation	✓ ✗	Severance	✓ ✗

Termination Reason

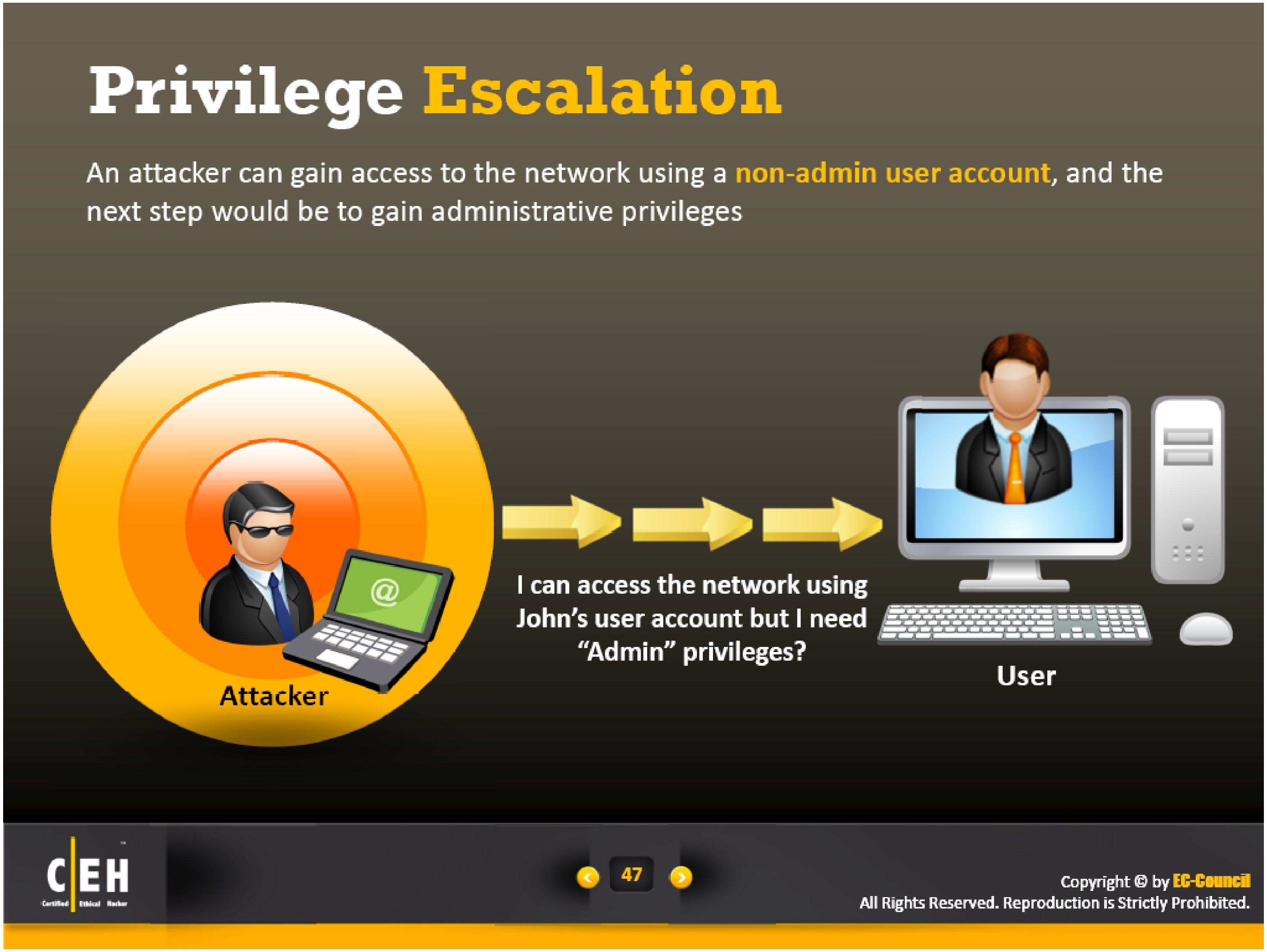
- Opening unsolicited e-mail
- Sending spam
- Emanating Viruses
- Port scanning
- Attempted unauthorized access
- Surfing porn
- Installing shareware
- Possession of hacking tools

- Refusal to abide by security policy
- Sending unsolicited e-mail
- Allowing kids to use company computer
- Disabling virus scanner
- Running P2P file sharing
- Unauthorized file/web serving
- Annoying the System Admin



CEH System Hacking Steps

- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Covering Tracks
- Hiding Files
- Penetration Testing



Privilege Escalation

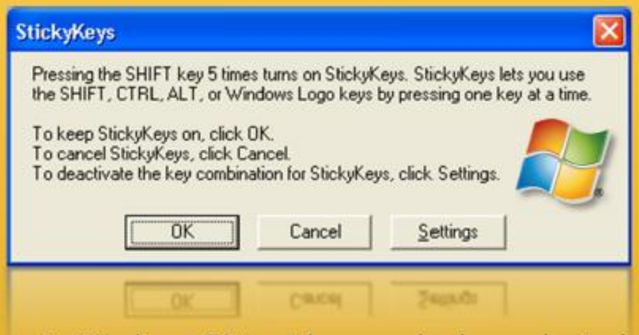
An attacker can gain access to the network using a non-admin user account, and the next step would be to gain administrative privileges

Attacker
User

I can access the network using John's user account but I need "Admin" privileges?

Escalation of Privileges

StickyKeys | AdminUser | DomainUser



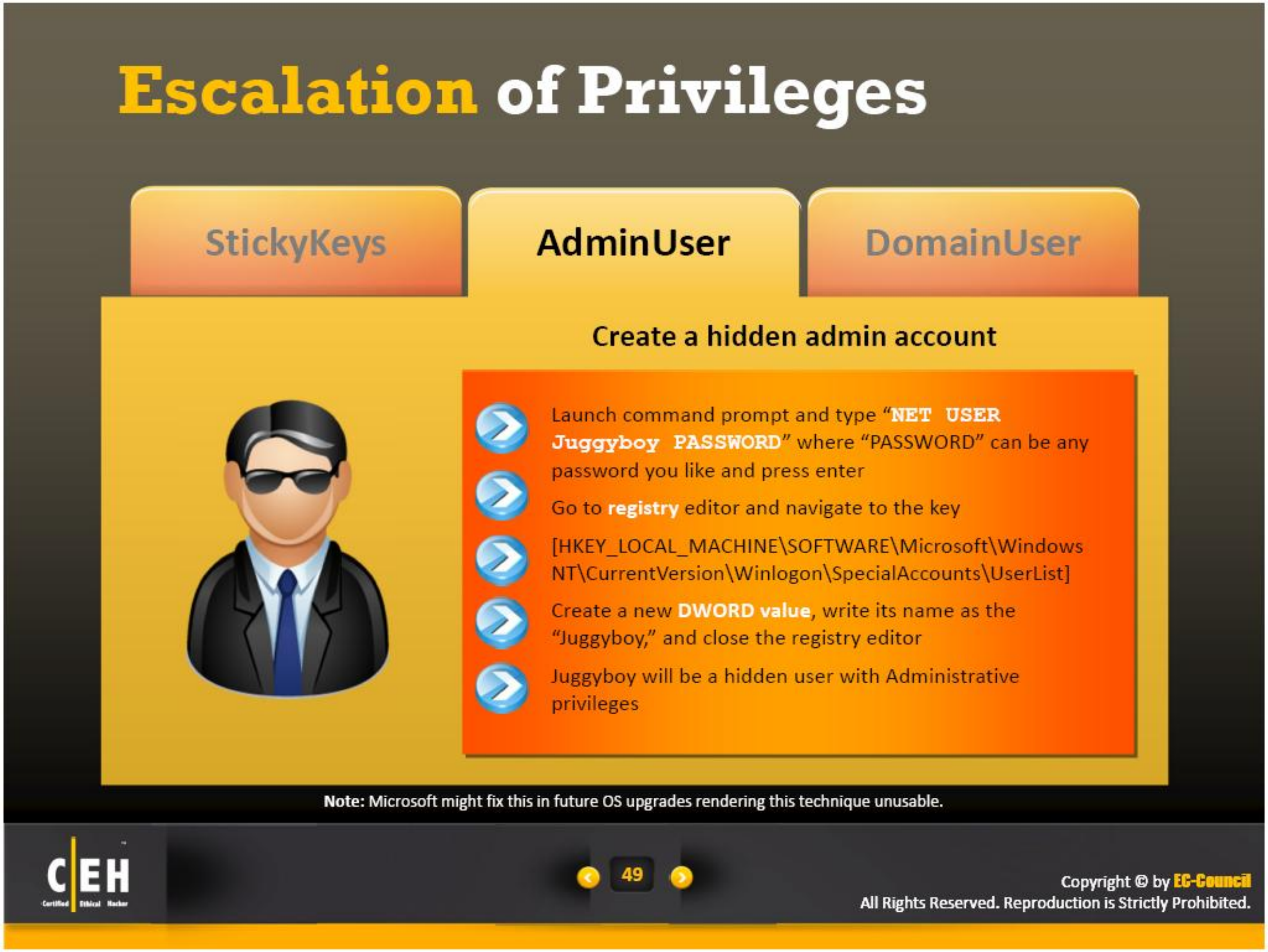
StickyKeys

Pressing the SHIFT key 5 times turns on StickyKeys. StickyKeys lets you use the SHIFT, CTRL, ALT, or Windows Logo keys by pressing one key at a time.

To keep StickyKeys on, click OK.
To cancel StickyKeys, click Cancel.
To deactivate the key combination for StickyKeys, click Settings.

- StickyKeys is an accessibility feature in Windows OS to aid users who have physical disabilities. **Press shift key 5 times** at the logon screen and the StickyKey dialog shows up
- The program that launches the StickyKeys is located at **c:\windows\system32\sethc.exe**
- If we replace the sethc.exe which is responsible for the sticky key dialog, with **cmd.exe**, and then call **sethc.exe** by pressing shift key 5 times at logon screen, we will get a command prompt with administrator privileges

Note: Microsoft might fix this in future OS upgrades rendering this technique unusable.



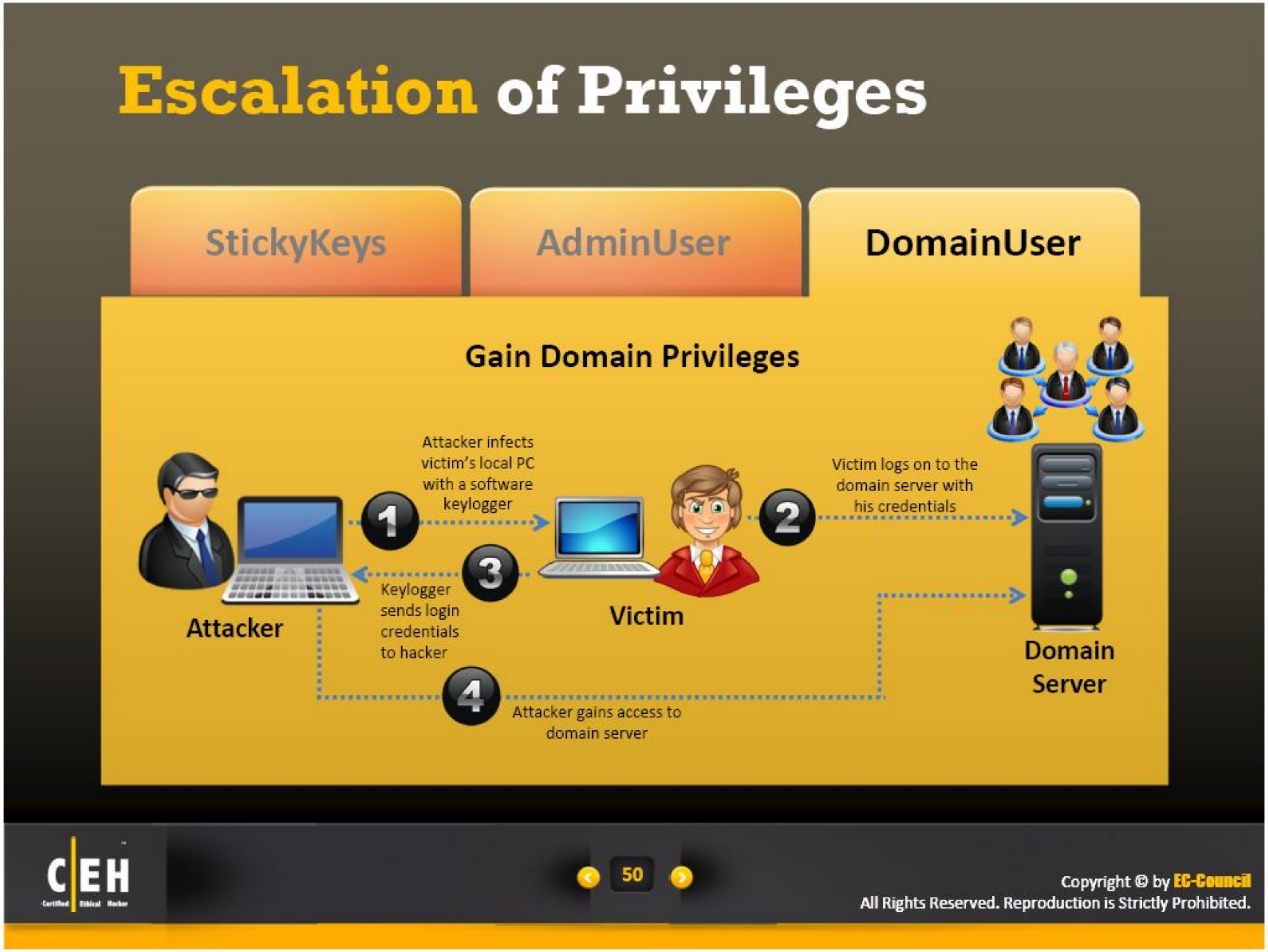
Escalation of Privileges

StickyKeys
AdminUser
DomainUser

Create a hidden admin account

- Launch command prompt and type "`NET USER Juggyboy PASSWORD`" where "PASSWORD" can be any password you like and press enter
- Go to **registry** editor and navigate to the key
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList]
- Create a new **DWORD value**, write its name as the "Juggyboy," and close the registry editor
- Juggyboy will be a hidden user with Administrative privileges

Note: Microsoft might fix this in future OS upgrades rendering this technique unusable.



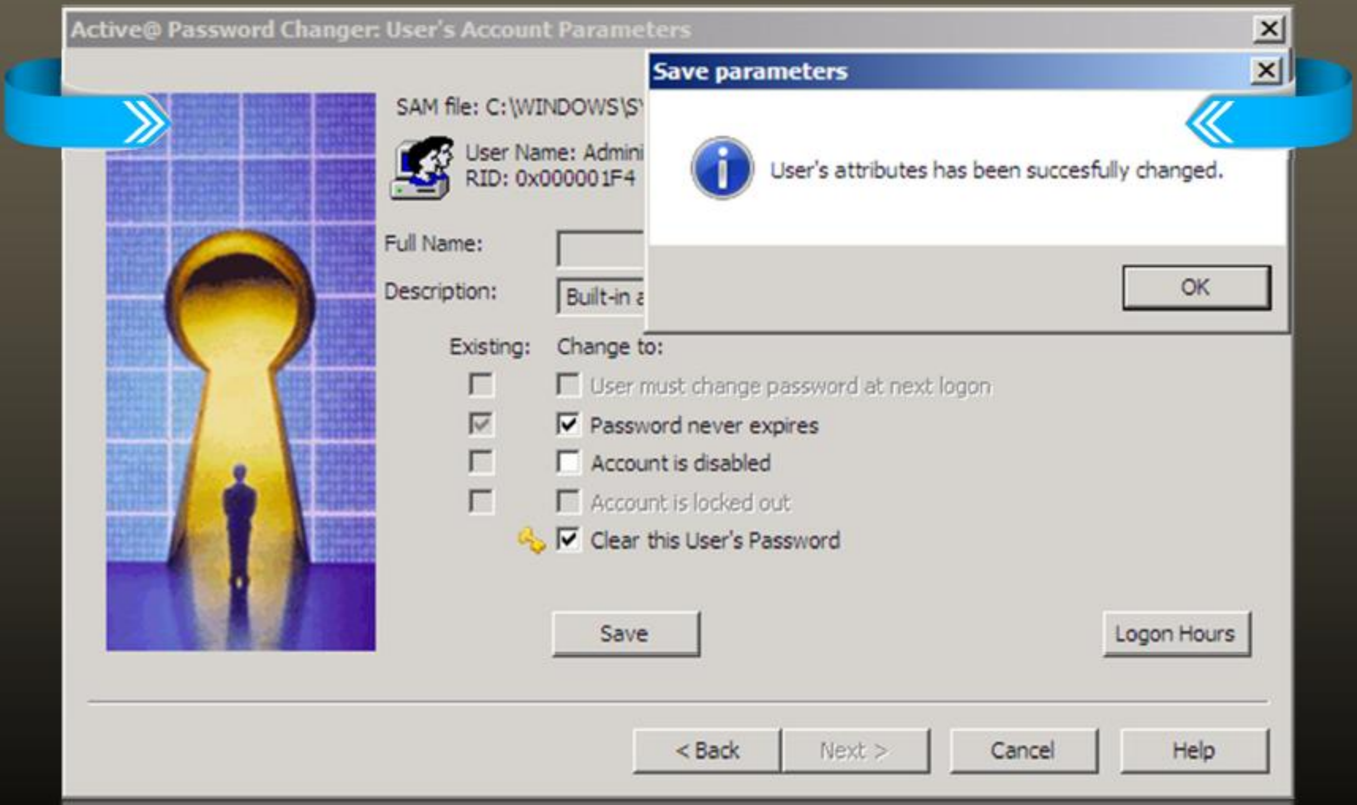
Escalation of Privileges

StickyKeys | AdminUser | DomainUser

Gain Domain Privileges

1. Attacker infects victim's local PC with a software keylogger
2. Victim logs on to the domain server with his credentials
3. Keylogger sends login credentials to hacker
4. Attacker gains access to domain server

Active@ Password Changer



Active@ Password Changer: User's Account Parameters

SAM file: C:\WINDOWS\S

User Name: Admini
RID: 0x000001F4

Full Name:

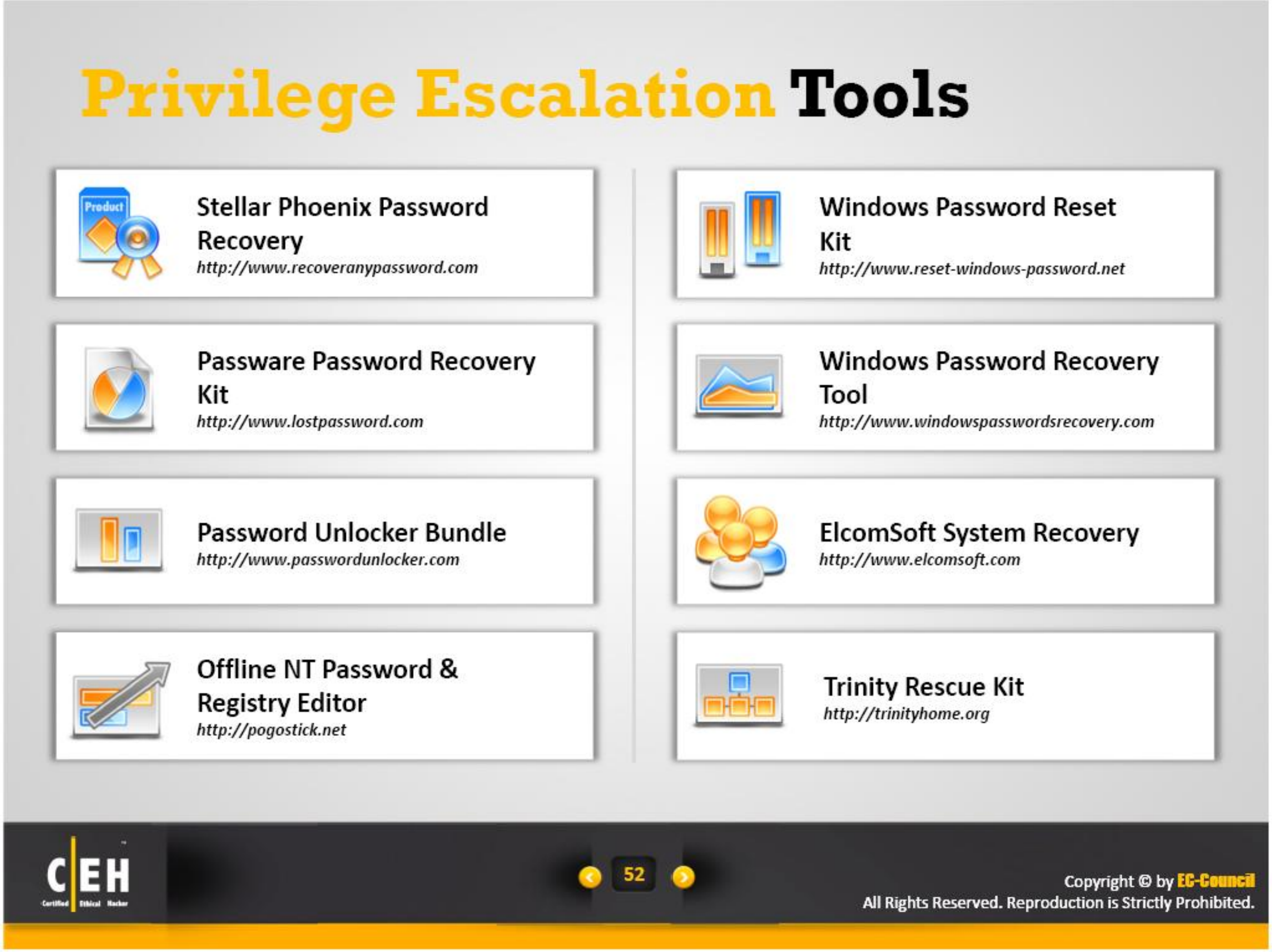
Description: Built-in a

Existing:	Change to:
□	□ User must change password at next logon
☑	☑ Password never expires
□	□ Account is disabled
□	□ Account is locked out
	☑ Clear this User's Password

Save parameters

User's attributes has been succesfully changed.

http://www.password-changer.com



Privilege Escalation Tools

Stellar Phoenix Password Recovery
http://www.recoveranypassword.com

Windows Password Reset Kit
http://www.reset-windows-password.net

Passware Password Recovery Kit
http://www.lostpassword.com

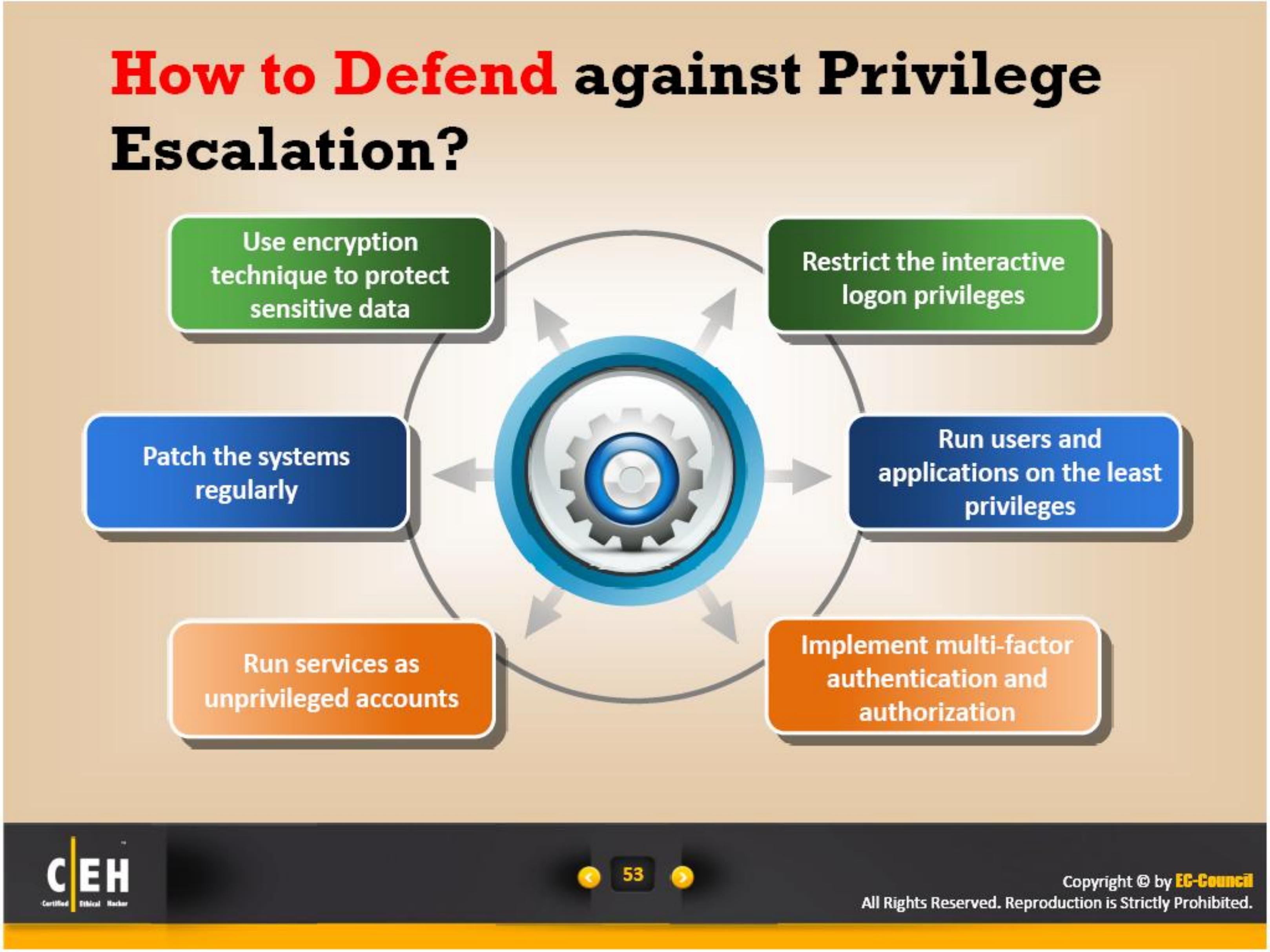
Windows Password Recovery Tool
http://www.windowspasswordsrecovery.com

Password Unlocker Bundle
http://www.passwordunlocker.com

ElcomSoft System Recovery
http://www.elcomsoft.com

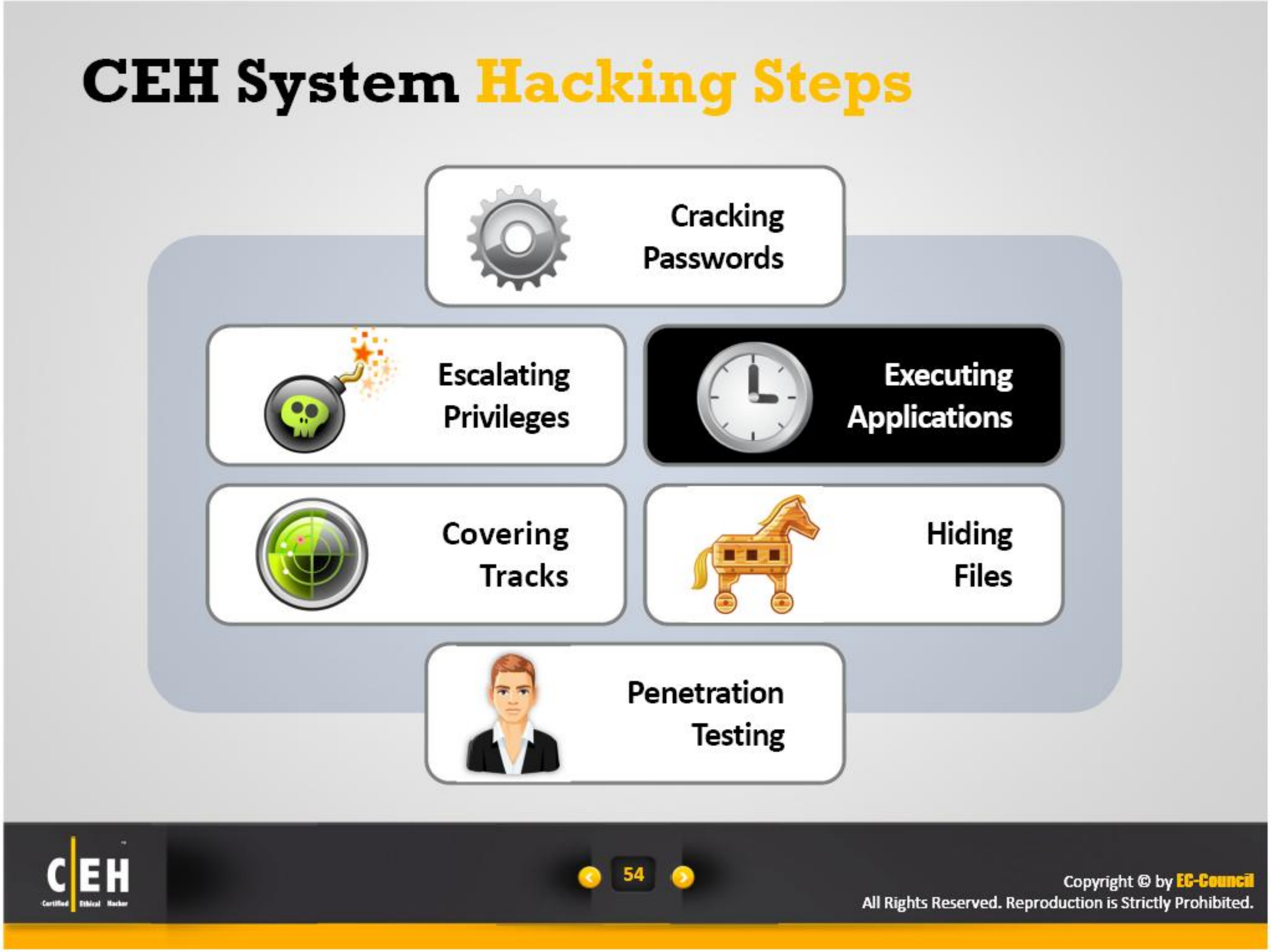
Offline NT Password & Registry Editor
http://pogostick.net

Trinity Rescue Kit
http://trinityhome.org



How to Defend against Privilege Escalation?

- Use encryption technique to protect sensitive data
- Restrict the interactive logon privileges
- Patch the systems regularly
- Run users and applications on the least privileges
- Run services as unprivileged accounts
- Implement multi-factor authentication and authorization



CEH System Hacking Steps

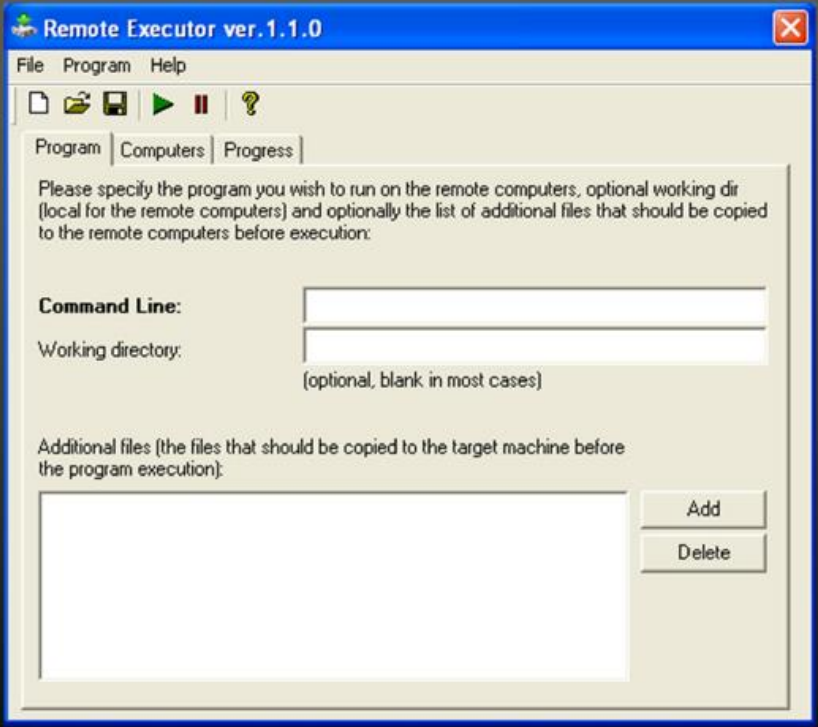
- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Hiding Files
- Covering Tracks
- Penetration Testing

Executing Applications

Attackers execute malicious applications in this stage. This is called "**owning**" the system

Alchemy Remote Executor

- Alchemy Remote Executor is a system management tool that allows you to execute programs on **remote network computers**
- The program executes on **multiple remote computers** simultaneously



Please specify the program you wish to run on the remote computers, optional working dir (local for the remote computers) and optionally the list of additional files that should be copied to the remote computers before execution:

Command Line:

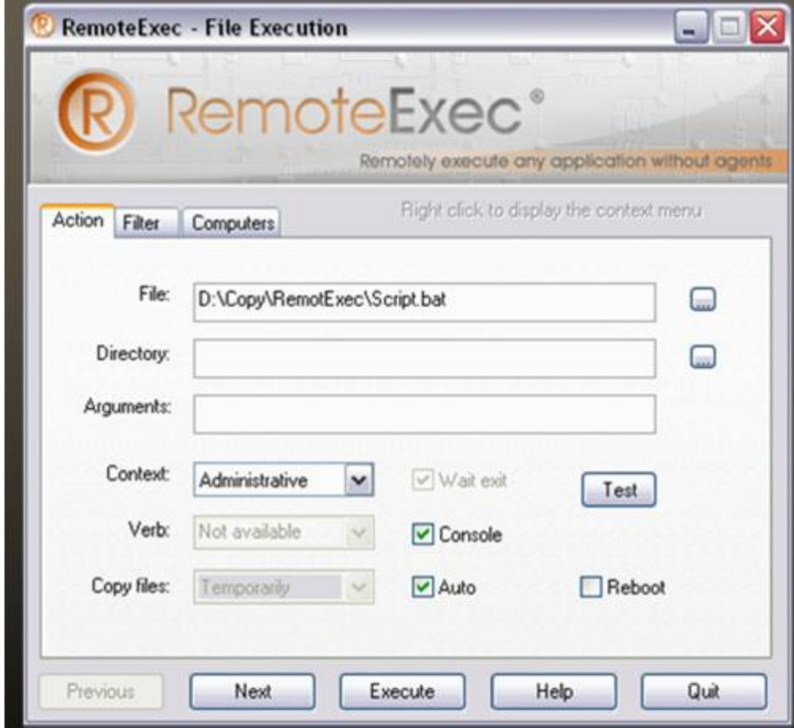
Working directory:

(optional, blank in most cases)

Additional files (the files that should be copied to the target machine before the program execution):

http://www.alchemy-lab.com

RemoteExec



RemoteExec - File Execution

RemoteExec® Remotely execute any application without agents

File: D:\Copy\RemotExec\Script.bat

Directory:

Arguments:

Context: Administrative

☑ Wait exit

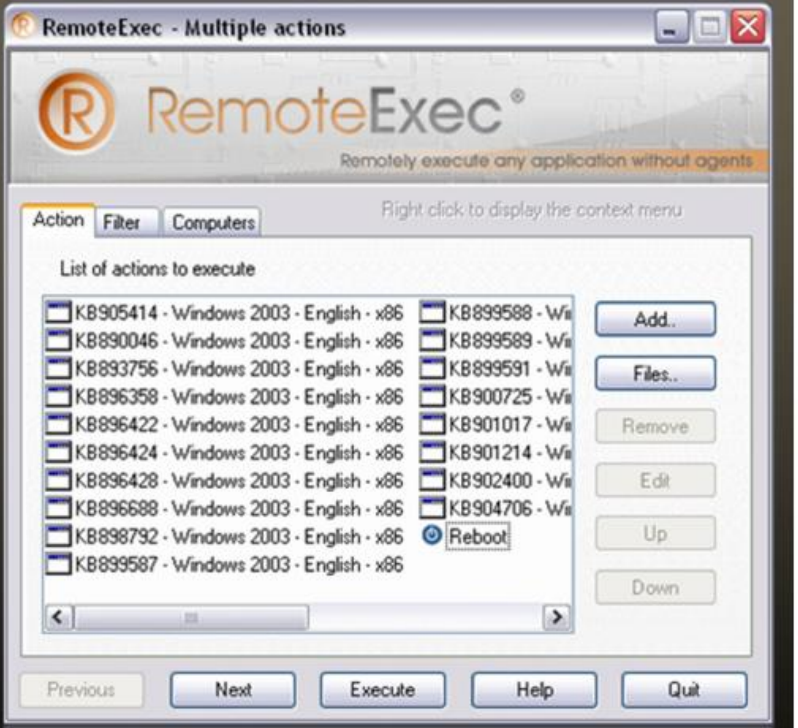
Verb: Not available

☑ Console

Copy files: Temporarily

☑ Auto

□ Reboot



RemoteExec - Multiple actions

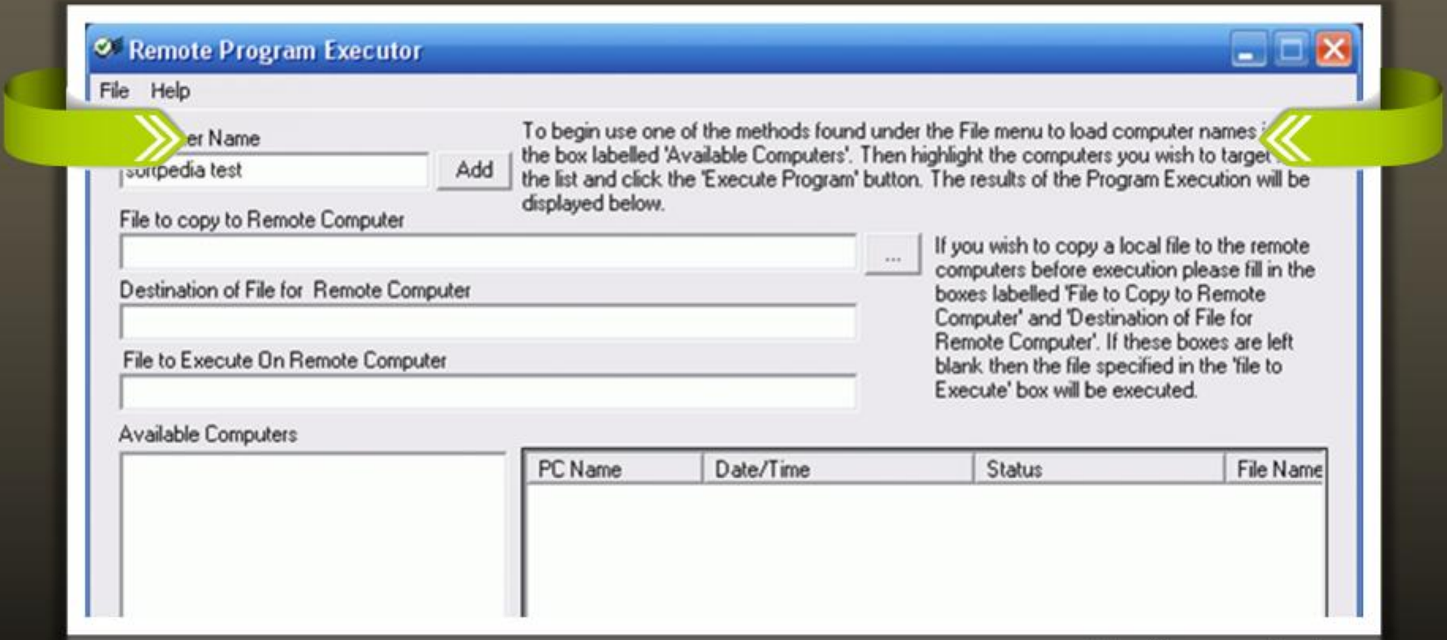
RemoteExec® Remotely execute any application without agents

List of actions to execute

- KB905414 - Windows 2003 - English - x86
- KB890046 - Windows 2003 - English - x86
- KB893756 - Windows 2003 - English - x86
- KB896358 - Windows 2003 - English - x86
- KB896422 - Windows 2003 - English - x86
- KB896424 - Windows 2003 - English - x86
- KB896428 - Windows 2003 - English - x86
- KB896688 - Windows 2003 - English - x86
- KB898792 - Windows 2003 - English - x86
- KB899587 - Windows 2003 - English - x86
- KB899588 - Wi
- KB899589 - Wi
- KB899591 - Wi
- KB900725 - Wi
- KB901017 - Wi
- KB901214 - Wi
- KB902400 - Wi
- KB904706 - Wi
- Reboot

http://www.pnltools.com

Execute This!



Remote Program Executor

sortpedia test

To begin use one of the methods found under the File menu to load computer names into the box labelled 'Available Computers'. Then highlight the computers you wish to target in the list and click the 'Execute Program' button. The results of the Program Execution will be displayed below.

File to copy to Remote Computer

Destination of File for Remote Computer

File to Execute On Remote Computer

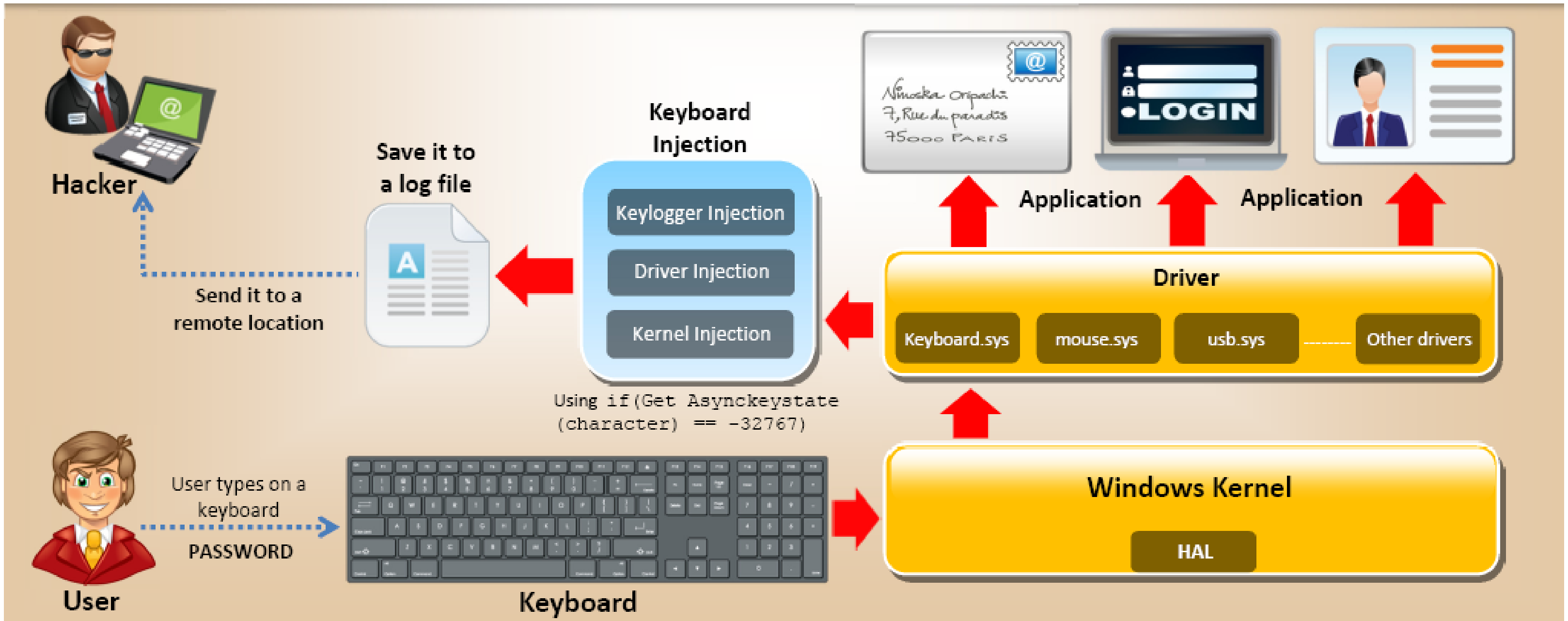
If you wish to copy a local file to the remote computers before execution please fill in the boxes labelled 'File to Copy to Remote Computer' and 'Destination of File for Remote Computer'. If these boxes are left blank then the file specified in the 'file to Execute' box will be executed.

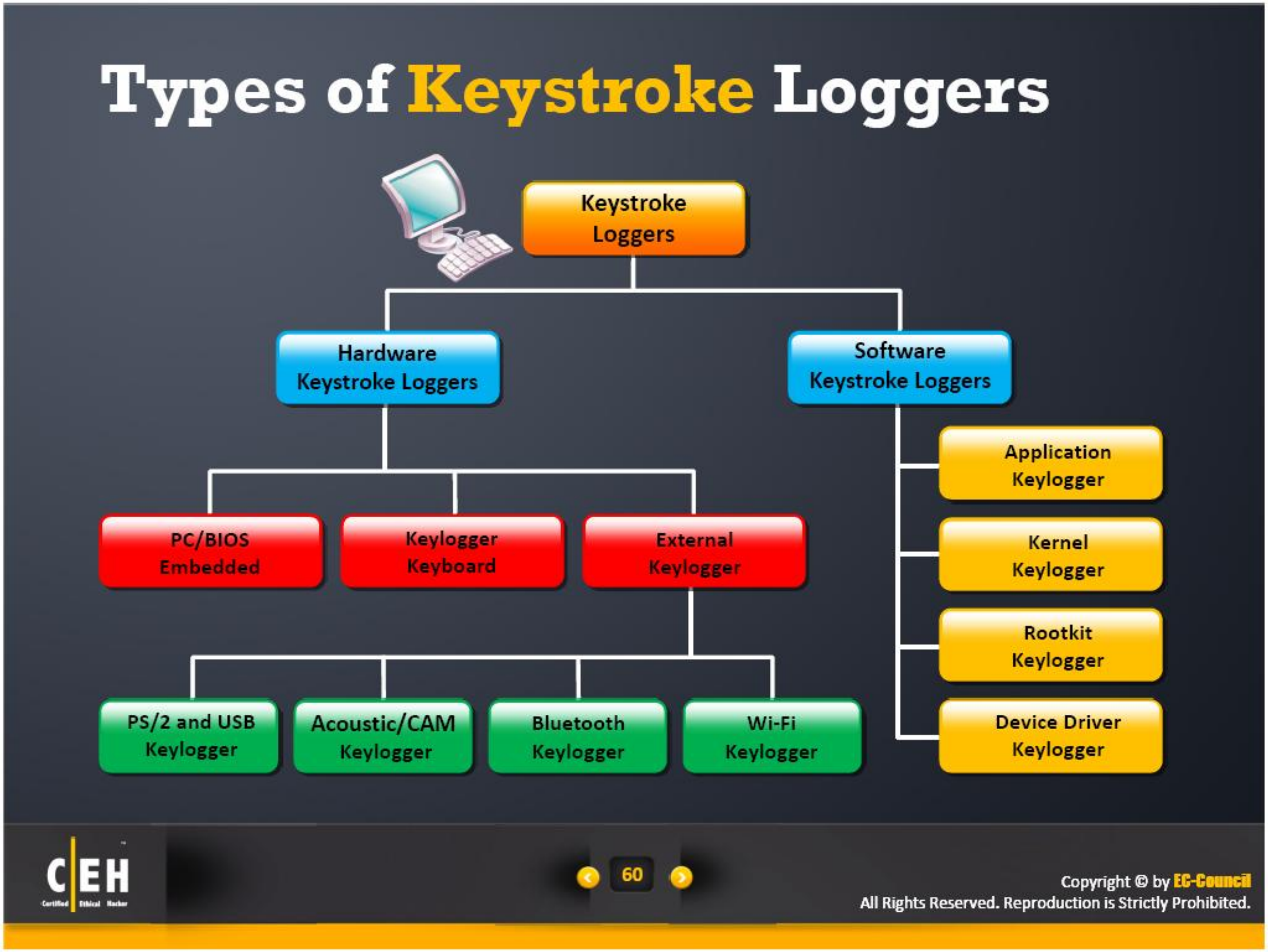
Available Computers

http://www.cyntrigal.com

Keylogger

- Keystroke loggers are programs or hardware devices that **monitor each keystroke** as user types on a keyboard; logs on to a file or transmits them to a remote location
- Keyloggers are placed between the **keyboard hardware** and the **operating system**
- Legitimate applications for keyloggers include in office and industrial settings to monitor employees' computer activities and in home environments where parents can monitor and spy on children's activity

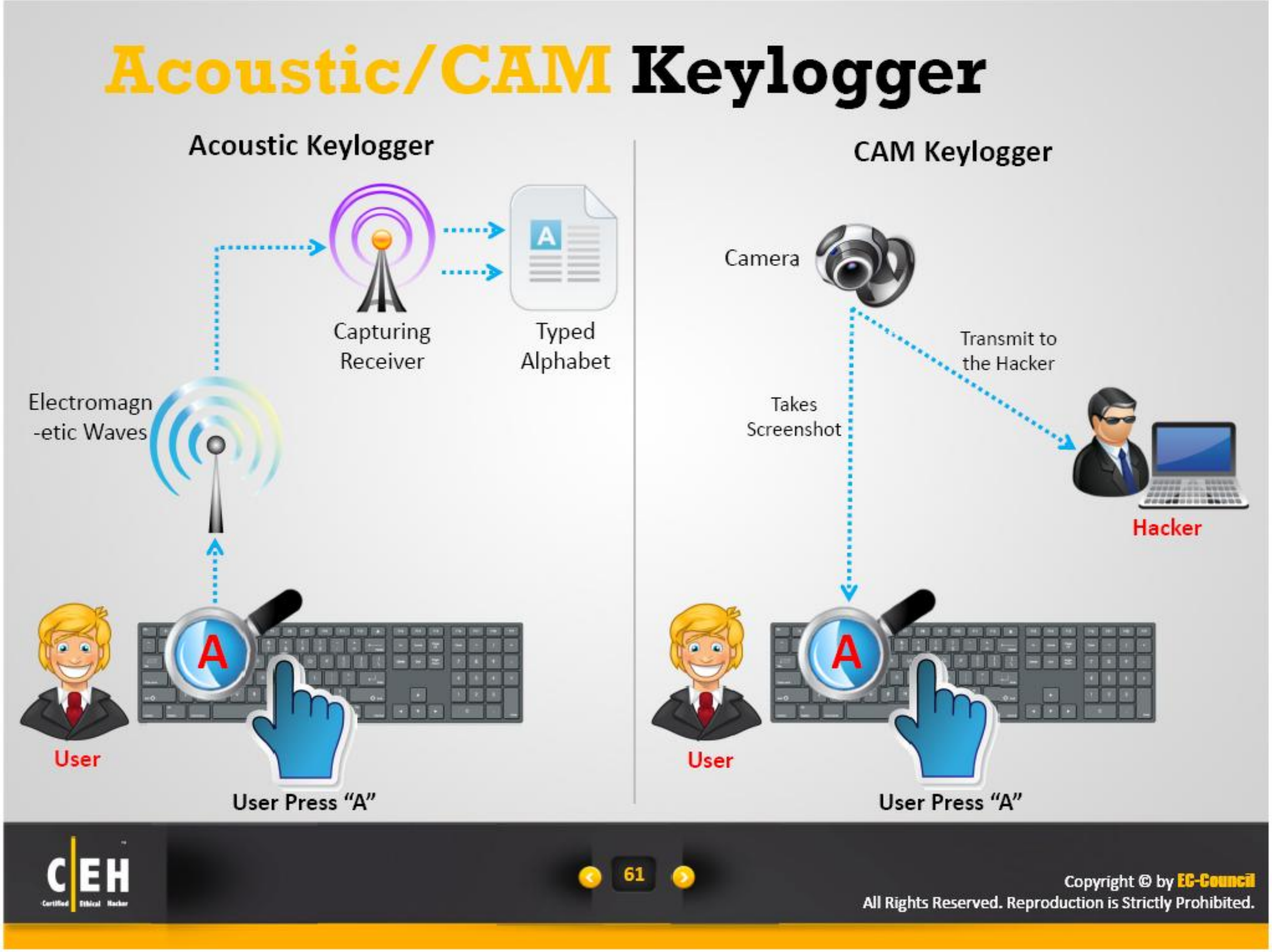




Types of Keystroke Loggers

Keystroke Loggers

- Hardware Keystroke Loggers
  - PC/BIOS Embedded
  - Keylogger Keyboard
  - External Keylogger
    - PS/2 and USB Keylogger
    - Acoustic/CAM Keylogger
    - Bluetooth Keylogger
    - Wi-Fi Keylogger
- Software Keystroke Loggers
  - Application Keylogger
  - Kernel Keylogger
  - Rootkit Keylogger
  - Device Driver Keylogger



Acoustic/CAM Keylogger

Acoustic Keylogger

Capturing Receiver

Typed Alphabet

Electromagn
-etic Waves

User

User Press "A"

CAM Keylogger

Camera

Transmit to the Hacker

Takes Screenshot

Hacker

User

User Press "A"

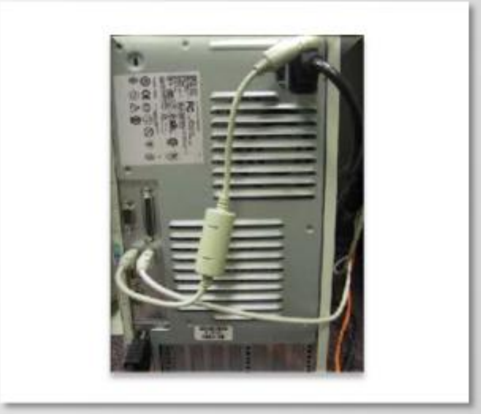
PS/2 Keylogger

USB Keylogger

Wi-Fi Keylogger

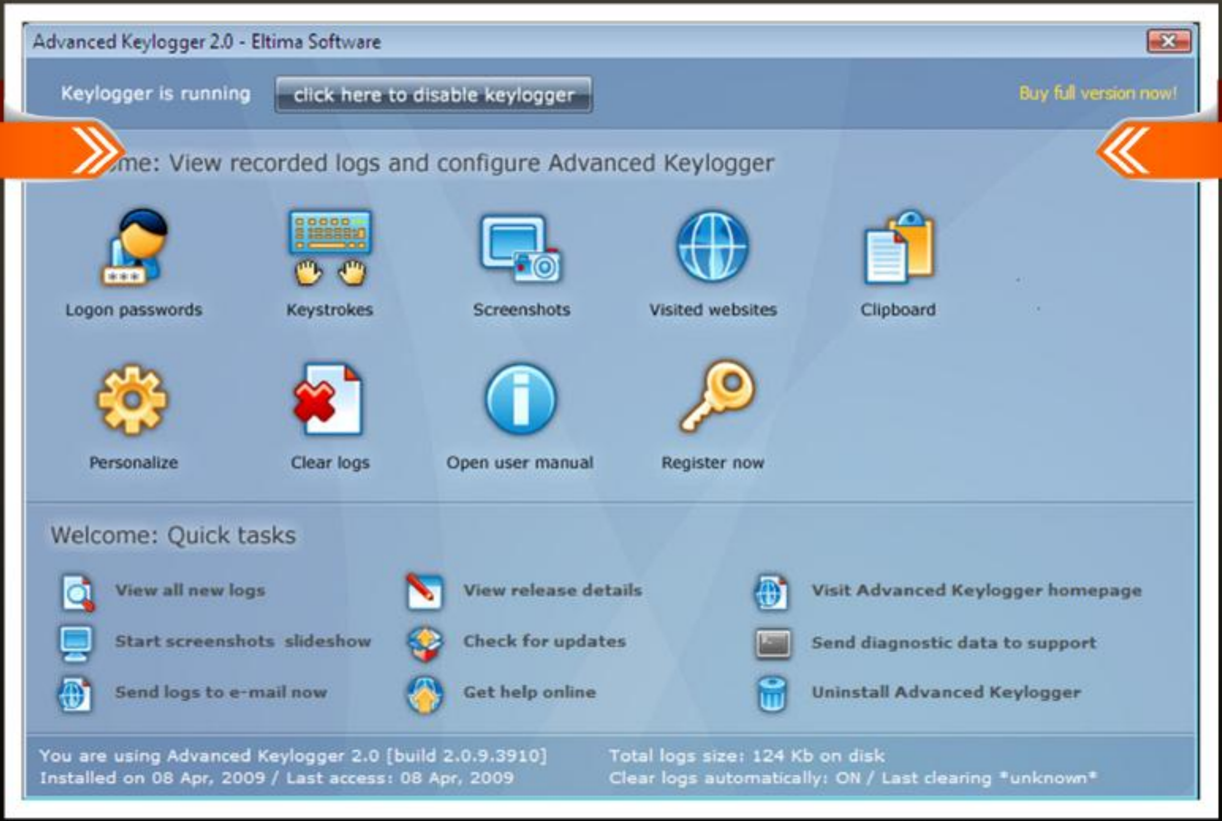
Keylogger embedded
inside the keyboard

Bluetooth Keylogger



Hardware Keylogger

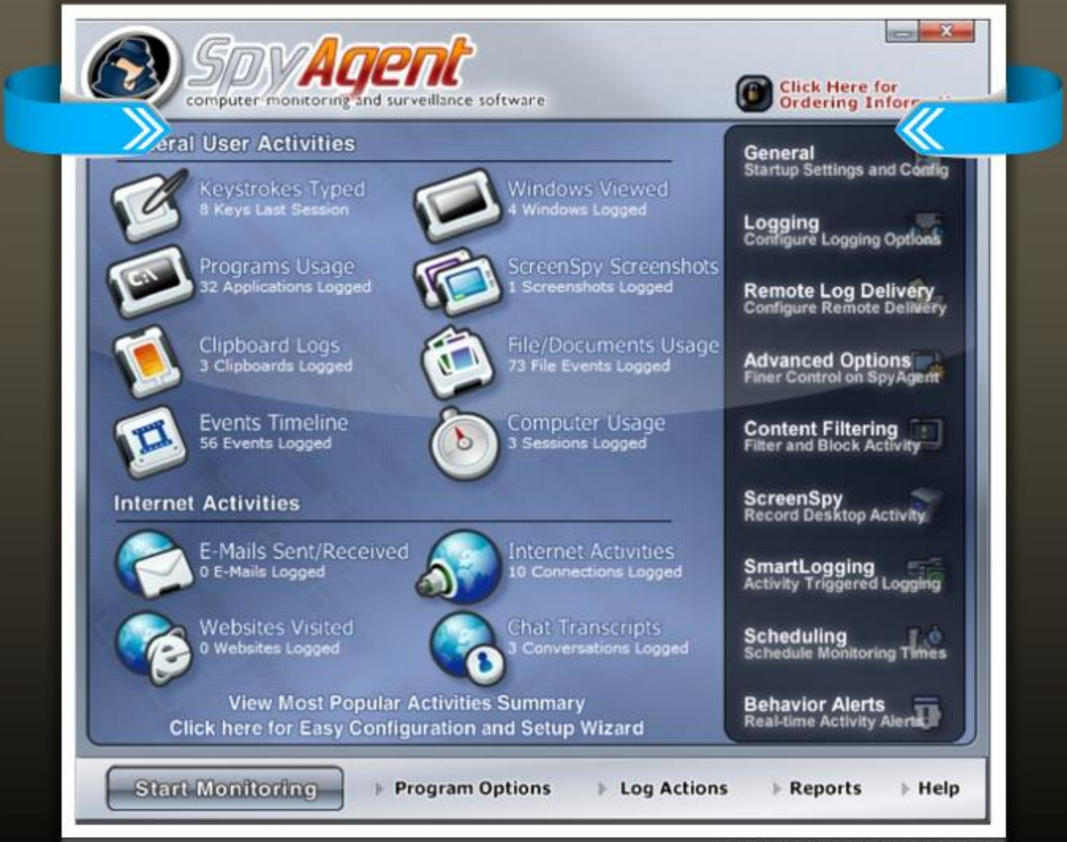
Keylogger: Advanced Keylogger



You are using Advanced Keylogger 2.0 [build 2.0.9.3910]
Installed on 08 Apr, 2009 / Last access: 08 Apr, 2009
Total logs size: 124 Kb on disk
Clear logs automatically: ON / Last clearing *unknown*

http://www.mykeylogger.com

Keylogger: Spytech SpyAgent



SpyAgent
computer monitoring and surveillance software

Click Here for Ordering Infor...

...eral User Activities

Keystrokes Typed
8 Keys Last Session

Windows Viewed
4 Windows Logged

Programs Usage
32 Applications Logged

ScreenSpy Screenshots
1 Screenshots Logged

Clipboard Logs
3 Clipboards Logged

File/Documents Usage
73 File Events Logged

Events Timeline
56 Events Logged

Computer Usage
3 Sessions Logged

Internet Activities

E-Mails Sent/Received
0 E-Mails Logged

Internet Activities
10 Connections Logged

Websites Visited
0 Websites Logged

Chat Transcripts
3 Conversations Logged

View Most Popular Activities Summary
Click here for Easy Configuration and Setup Wizard

General
Startup Settings and Config

Logging
Configure Logging Options

Remote Log Delivery
Configure Remote Delivery

Advanced Options
Finer Control on SpyAgent

Content Filtering
Filter and Block Activity

ScreenSpy
Record Desktop Activity

SmartLogging
Activity Triggered Logging

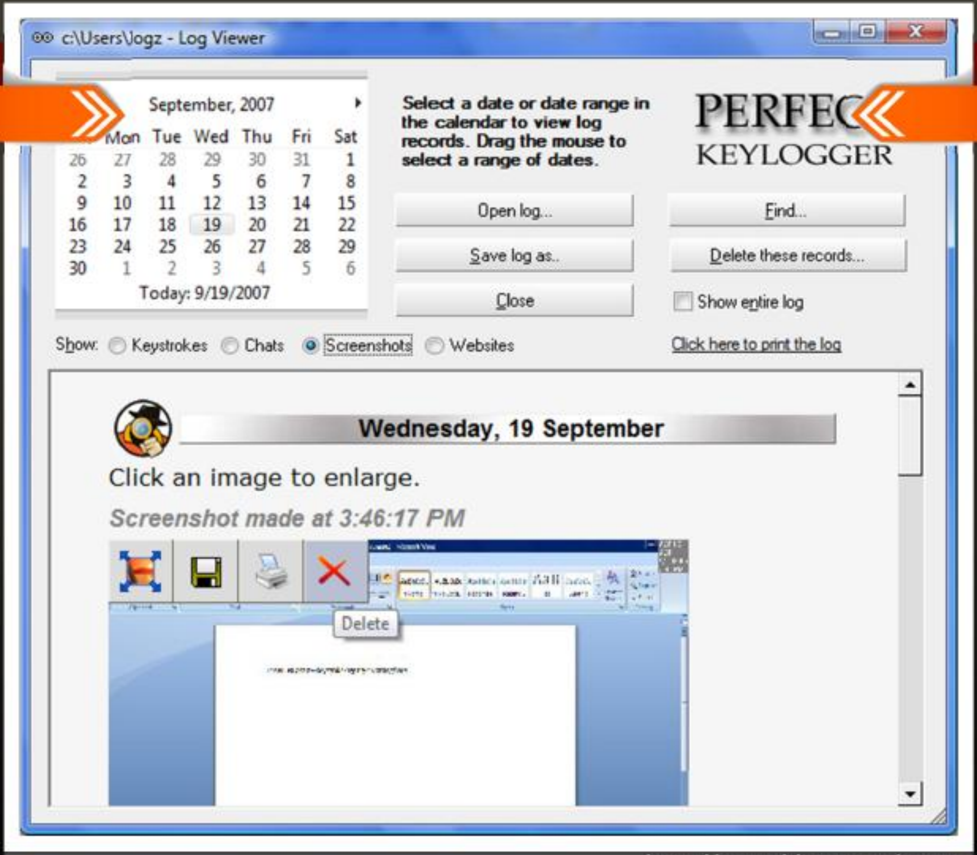
Scheduling
Schedule Monitoring Times

Behavior Alerts
Real-time Activity Alerts

Start Monitoring | Program Options | Log Actions | Reports | Help

http://www.keylogger.org

Keylogger: Perfect Keylogger



c:\Users\logz - Log Viewer

September, 2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 9/19/2007

Select a date or date range in the calendar to view log records. Drag the mouse to select a range of dates.

Show: ○ Keystrokes ○ Chats ● Screenshots ○ Websites

□ Show entire log

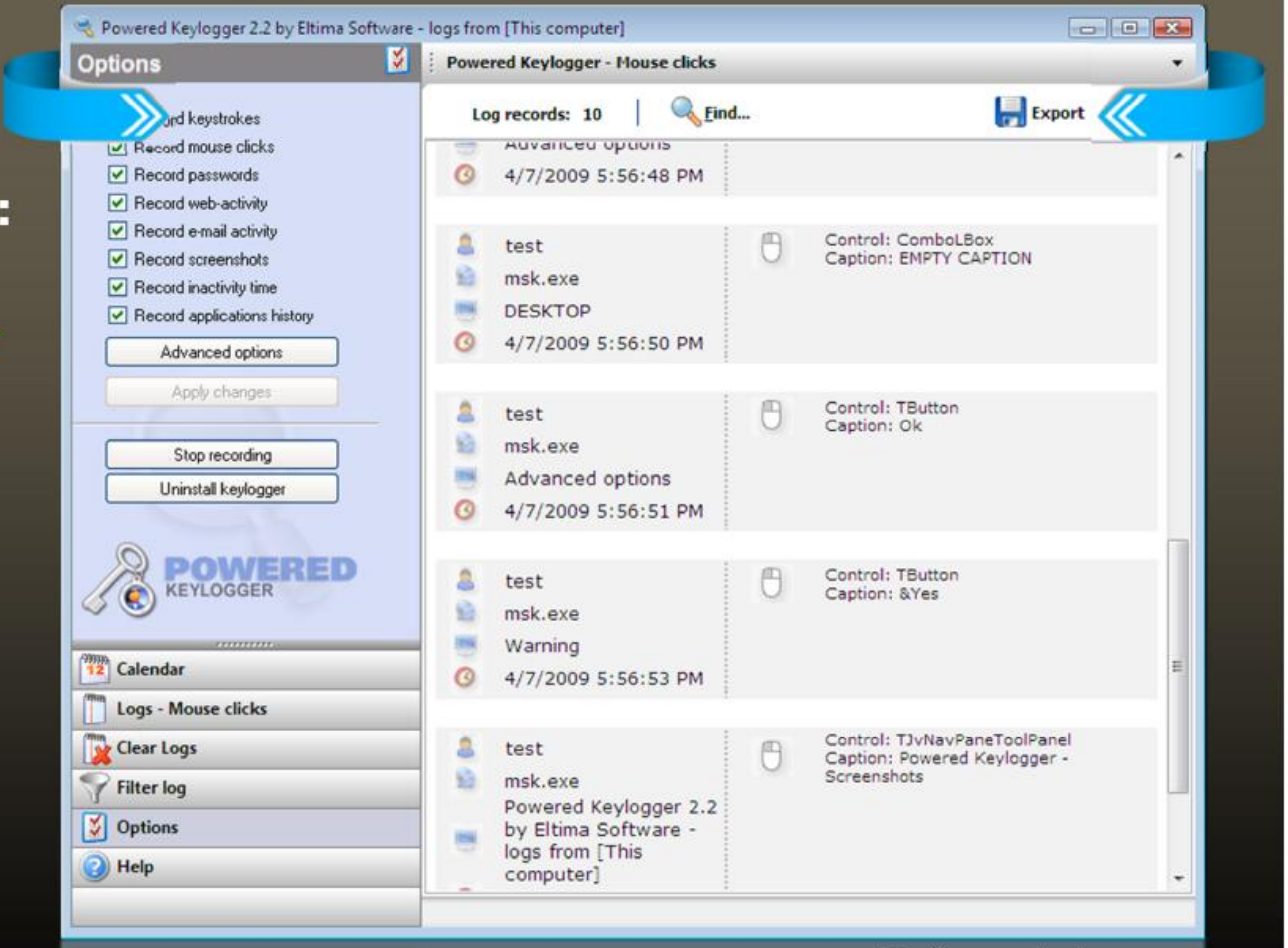
Wednesday, 19 September

Click an image to enlarge.

Screenshot made at 3:46:17 PM

http://www.blazingtools.com

Keylogger: Powered Keylogger



Powered Keylogger 2.2 by Eltima Software - logs from [This computer]

Options

- ☑ Record keystrokes
- ☑ Record mouse clicks
- ☑ Record passwords
- ☑ Record web-activity
- ☑ Record e-mail activity
- ☑ Record screenshots
- ☑ Record inactivity time
- ☑ Record applications history

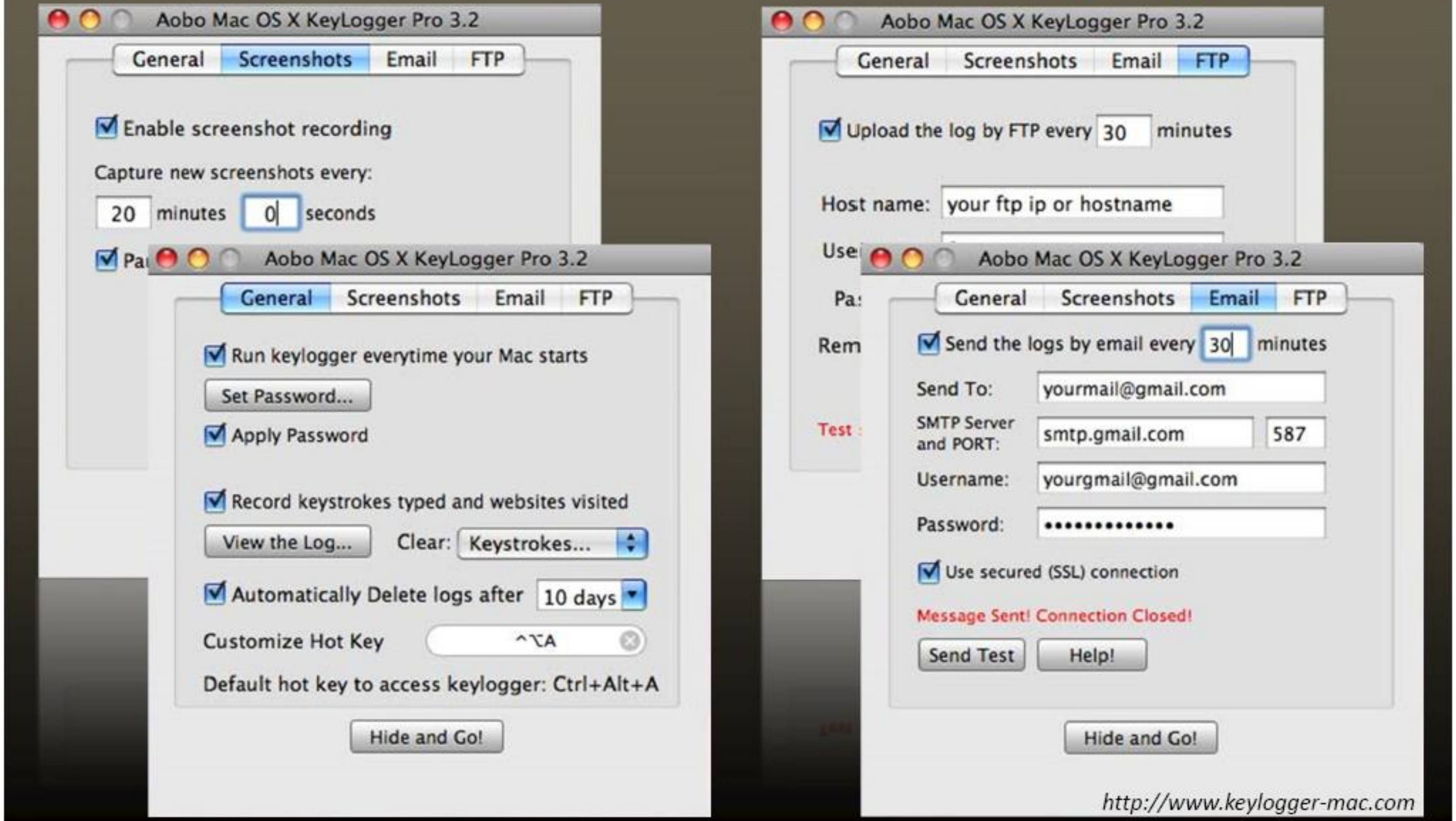
Powered Keylogger - Mouse clicks

Log records: 10

```
Advanced options
4/7/2009 5:56:48 PM

test                          Control: ComboLBox
msk.exe                       Caption: EMPTY CAPTION
DESKTOP
4/7/2009 5:56:50 PM

test                          Control: TButton
msk.exe                       Caption: Ok
Advanced options
4/7/2009 5:56:51 PM

test                          Control: TButton
msk.exe                       Caption: &Yes
Warning
4/7/2009 5:56:53 PM

test                          Control: TJvNavPaneToolPanel
msk.exe                       Caption: Powered Keylogger -
Powered Keylogger 2.2         Screenshots
by Eltima Software -
logs from [This
computer]
```

http://www.mykeylogger.com

Keylogger for Mac: Aobo Mac OS X KeyLogger



Aobo Mac OS X KeyLogger Pro 3.2

☑ Enable screenshot recording

Capture new screenshots every:

20 minutes 0 seconds

☑ Pa

Aobo Mac OS X KeyLogger Pro 3.2

☑ Upload the log by FTP every 30 minutes

Host name: your ftp ip or hostname

Use

Pa

Rem

Test

Aobo Mac OS X KeyLogger Pro 3.2

☑ Run keylogger everytime your Mac starts

☑ Apply Password

☑ Record keystrokes typed and websites visited

Clear: Keystrokes...

☑ Automatically Delete logs after 10 days

Customize Hot Key ^⌥A

Default hot key to access keylogger: Ctrl+Alt+A

Aobo Mac OS X KeyLogger Pro 3.2

☑ Send the logs by email every 30 minutes

Send To: yourmail@gmail.com

SMTP Server and PORT: smtp.gmail.com 587

Username: yourgmail@gmail.com

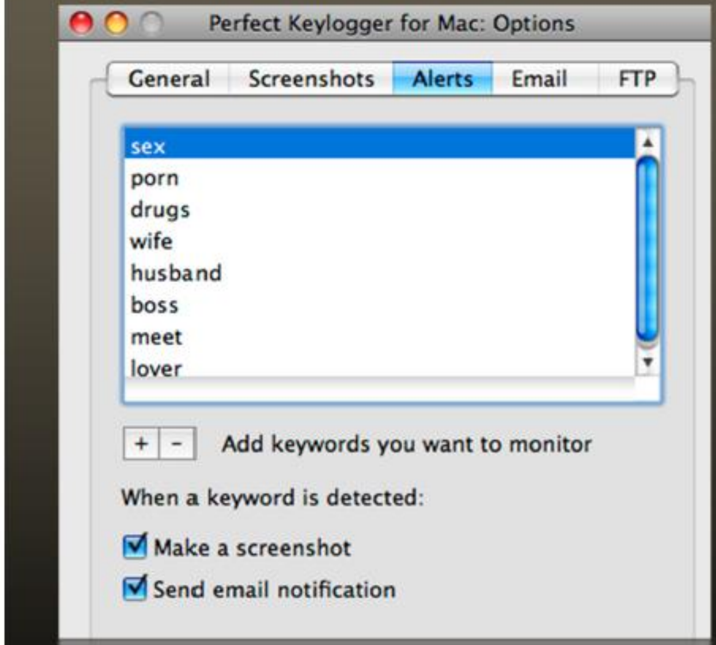
Password: •••••••••••••

☑ Use secured (SSL) connection

Message Sent! Connection Closed!

http://www.keylogger-mac.com

Keylogger for Mac: Perfect Keylogger for Mac



Perfect Keylogger for Mac: Options

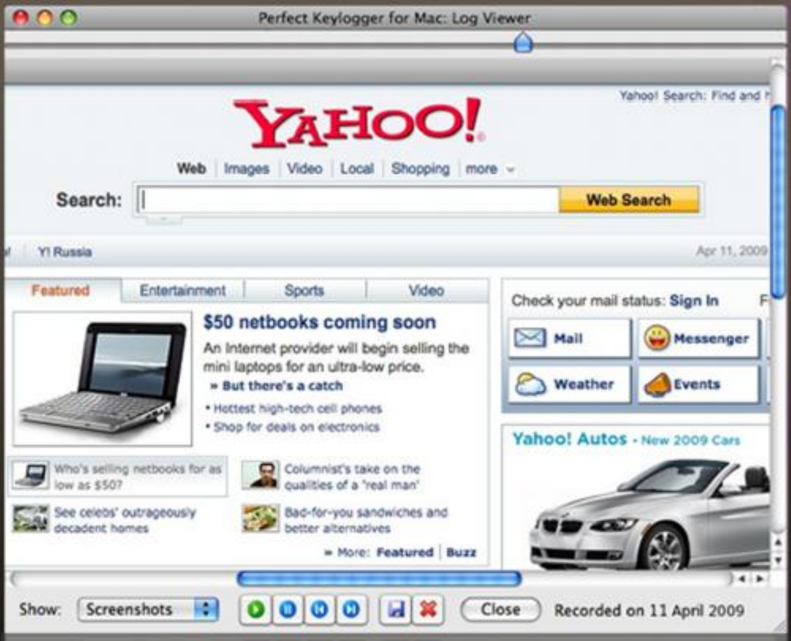
sex
porn
drugs
wife
husband
boss
meet
lover

+ - Add keywords you want to monitor

When a keyword is detected:

☑ Make a screenshot

☑ Send email notification



Perfect Keylogger for Mac: Log Viewer

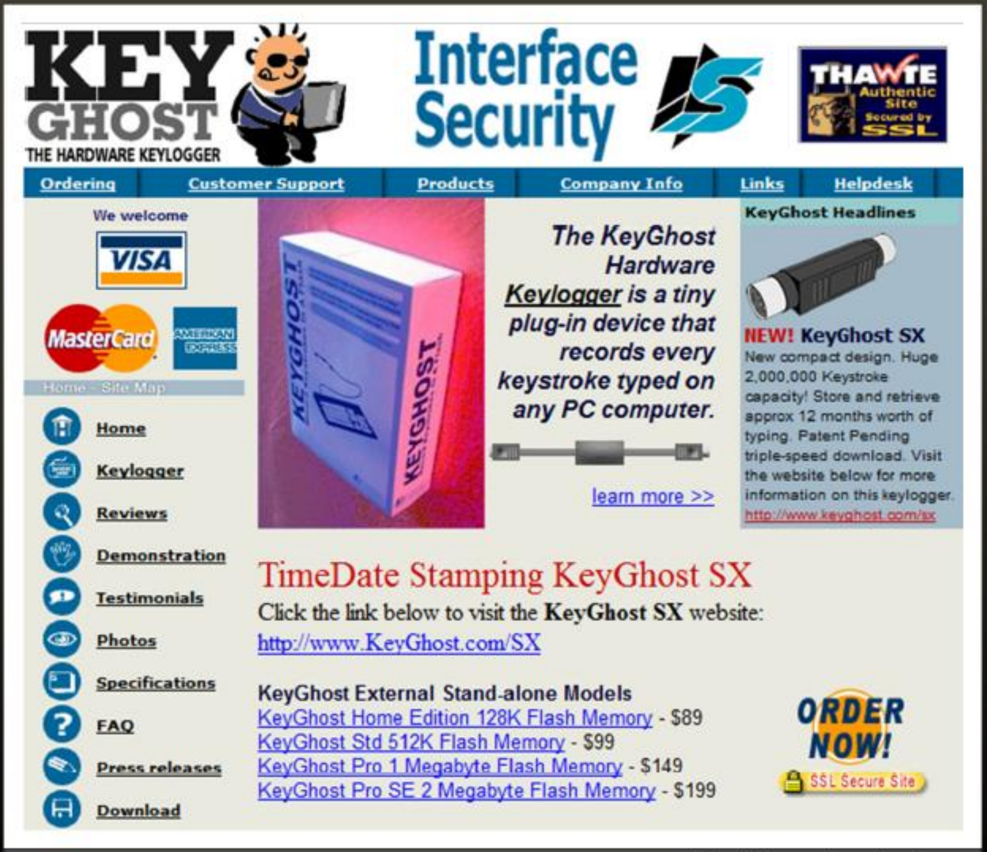
YAHOO!
Web | Images | Video | Local | Shopping | more
Search:
Web Search
Yahoo! Search: Find and
Y! Russia
Apr 11, 2009
Featured
Entertainment
Sports
Video
$50 netbooks coming soon
An Internet provider will begin selling the mini laptops for an ultra-low price.
» But there's a catch
• Hottest high-tech cell phones
• Shop for deals on electronics
Who's selling netbooks for as low as $50?
Columnist's take on the qualities of a 'real man'
See celebs' outrageously decadent homes
Bad-for-you sandwiches and better alternatives
» More: Featured | Buzz
Check your mail status: Sign In
Mail
Messenger
Weather
Events
Yahoo! Autos - New 2009 Cars
Close

Show: Screenshots

Recorded on 11 April 2009

http://www.blazingtools.com

Hardware Keylogger: KeyGhost



Ordering | Customer Support | Products | Company Info | Links | Helpdesk

We welcome

VISA MasterCard AMERICAN EXPRESS

Home · Site Map

- Home
- Keylogger
- Reviews
- Demonstration
- Testimonials
- Photos
- Specifications
- FAQ
- Press releases
- Download

The KeyGhost Hardware Keylogger is a tiny plug-in device that records every keystroke typed on any PC computer.

learn more >>

KeyGhost Headlines

NEW! KeyGhost SX

New compact design. Huge 2,000,000 Keystroke capacity! Store and retrieve approx 12 months worth of typing. Patent Pending triple-speed download. Visit the website below for more information on this keylogger.

http://www.keyghost.com/sx

TimeDate Stamping KeyGhost SX

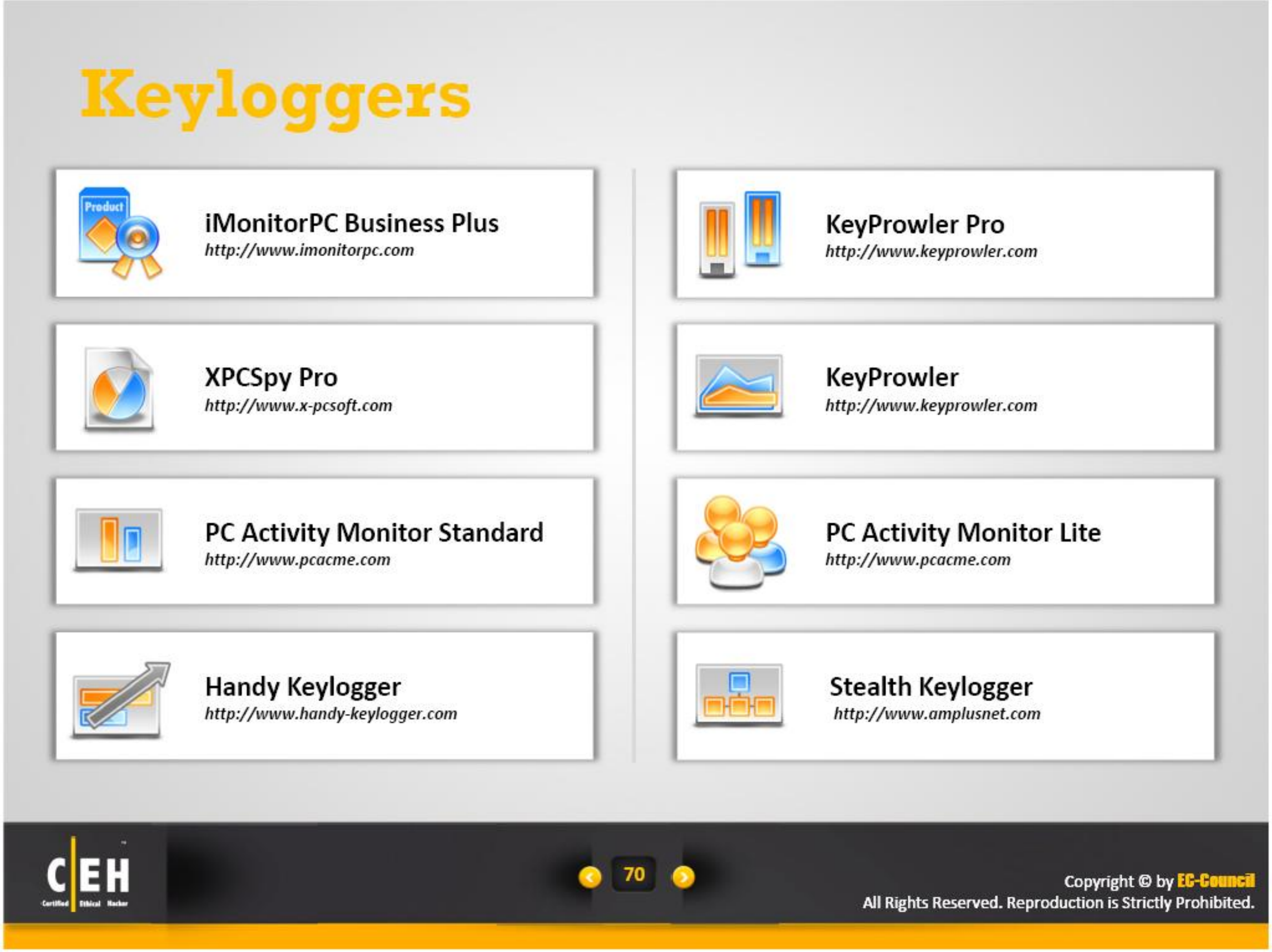
Click the link below to visit the **KeyGhost SX** website:

http://www.KeyGhost.com/SX

KeyGhost External Stand-alone Models

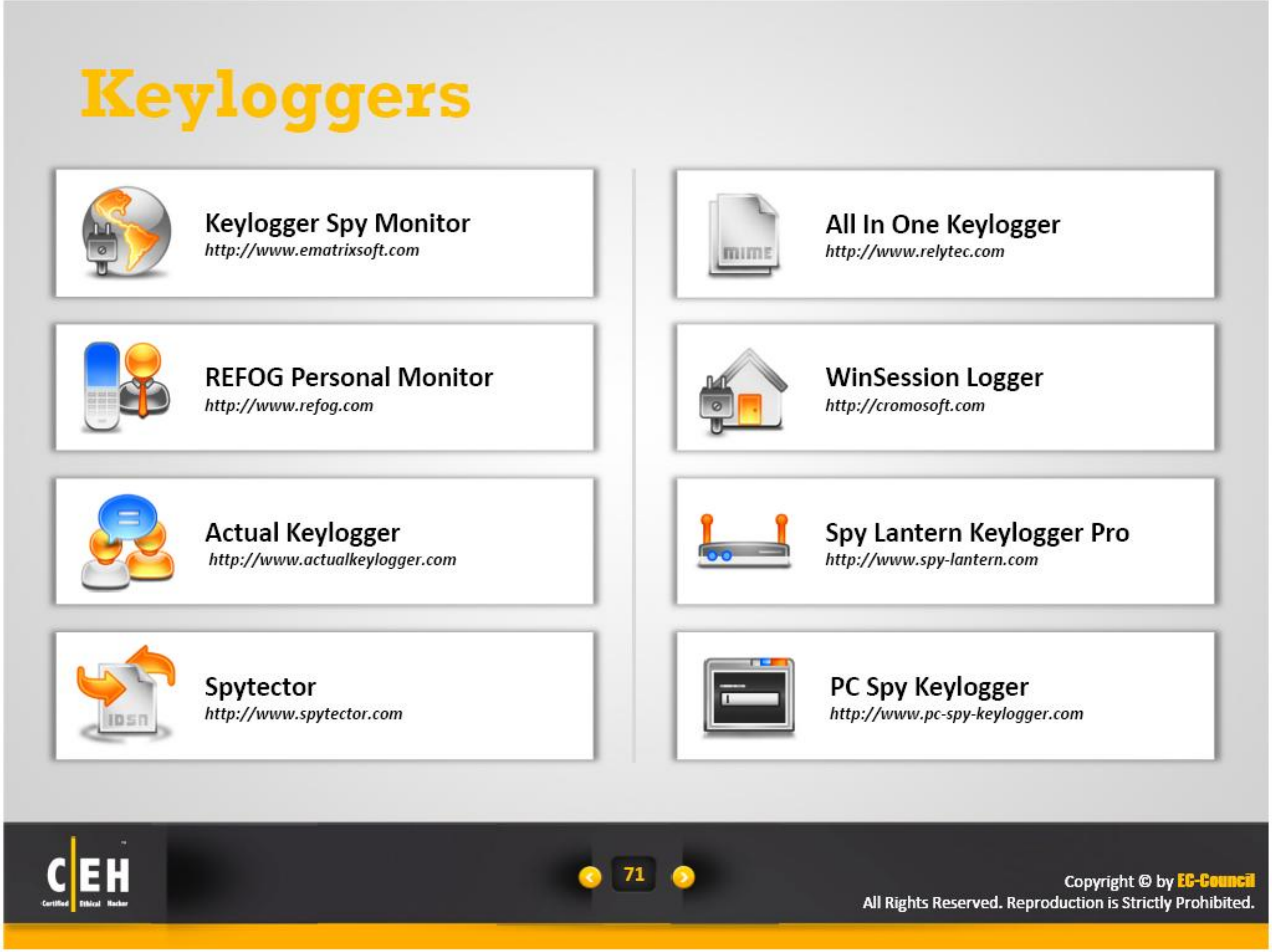
KeyGhost Home Edition 128K Flash Memory - $89
KeyGhost Std 512K Flash Memory - $99
KeyGhost Pro 1 Megabyte Flash Memory - $149
KeyGhost Pro SE 2 Megabyte Flash Memory - $199

http://www.keyghost.com



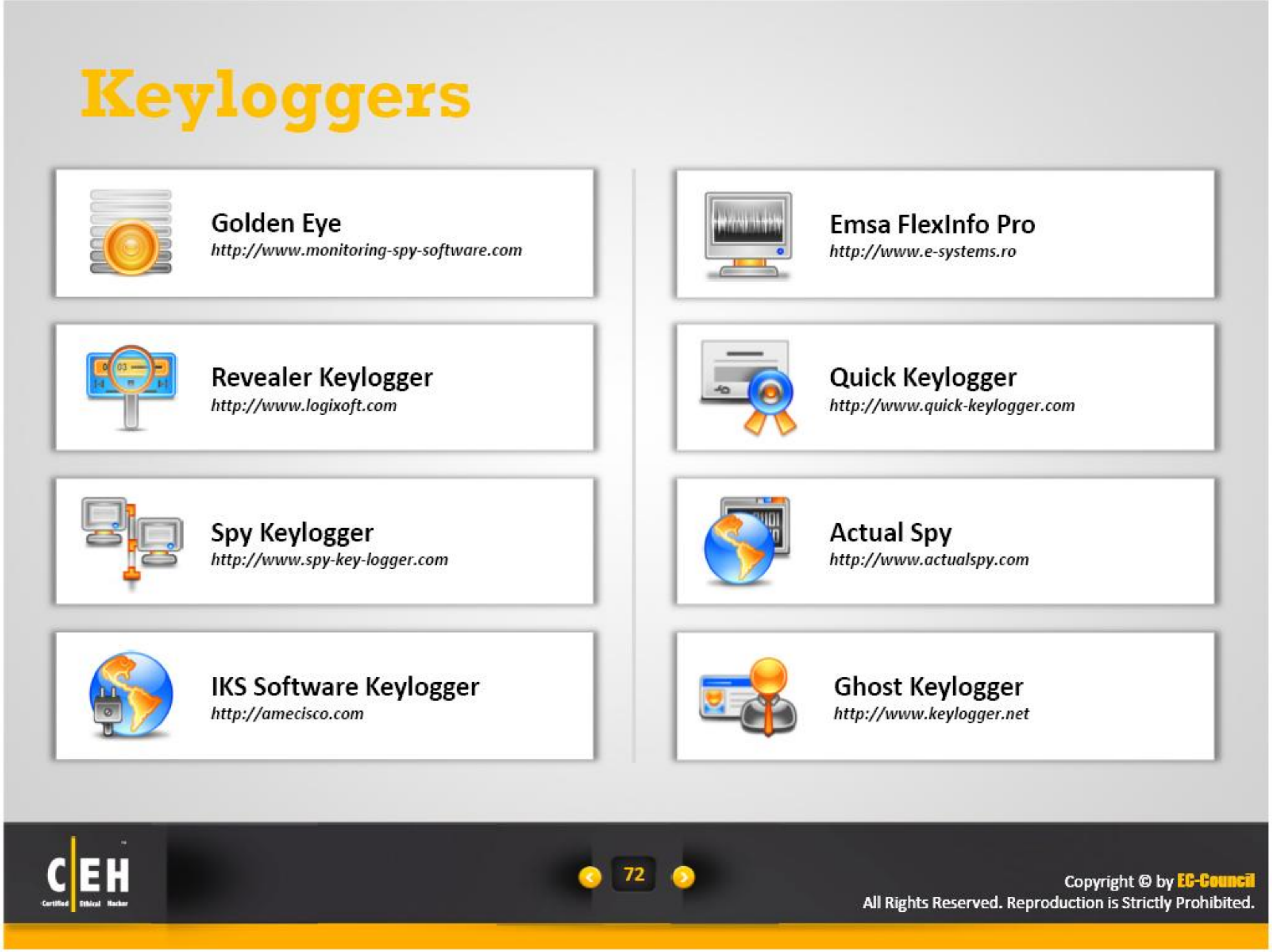
Keyloggers

- iMonitorPC Business Plus
  http://www.imonitorpc.com
- XPCSpy Pro
  http://www.x-pcsoft.com
- PC Activity Monitor Standard
  http://www.pcacme.com
- Handy Keylogger
  http://www.handy-keylogger.com
- KeyProwler Pro
  http://www.keyprowler.com
- KeyProwler
  http://www.keyprowler.com
- PC Activity Monitor Lite
  http://www.pcacme.com
- Stealth Keylogger
  http://www.amplusnet.com



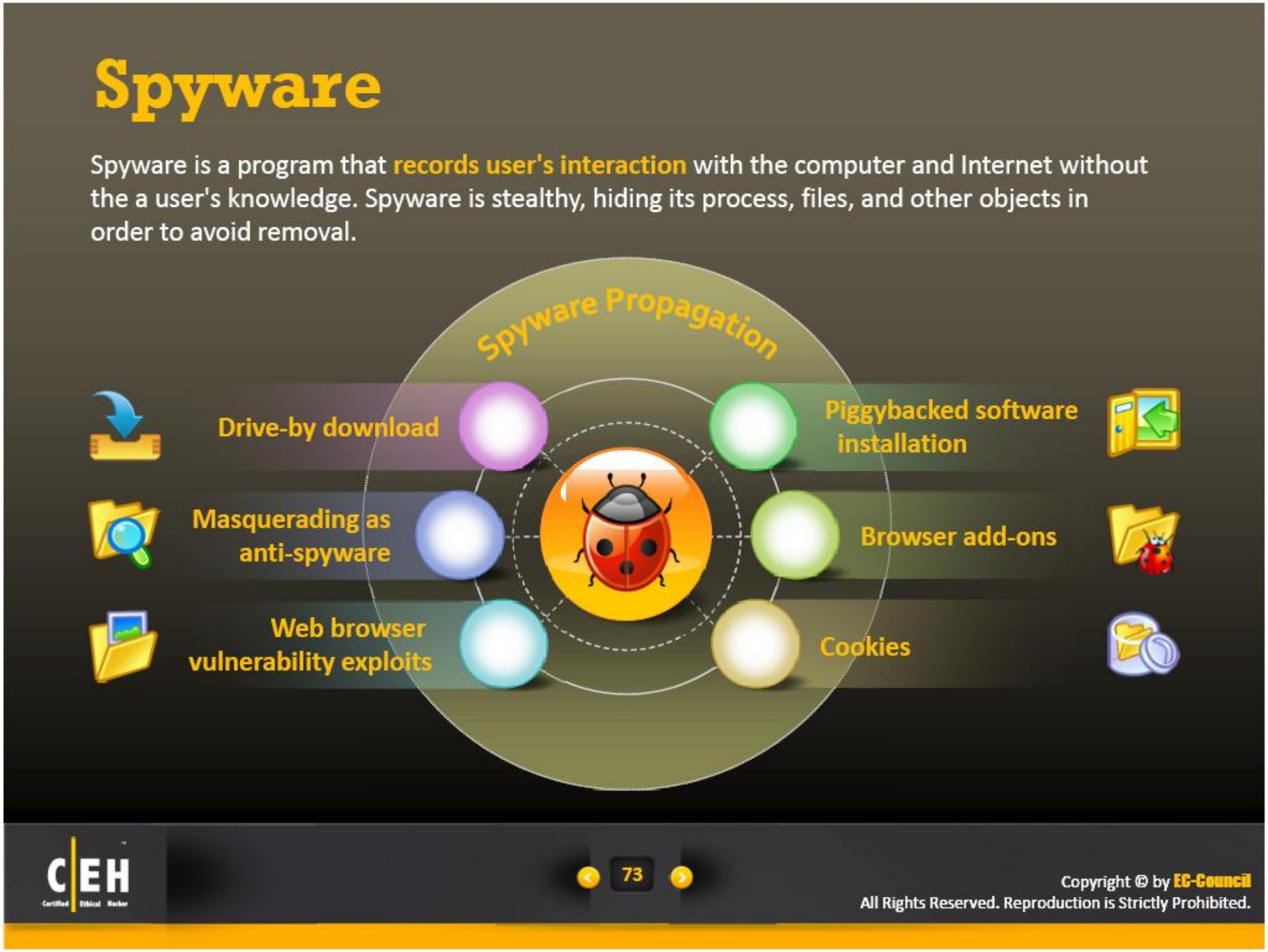
Keyloggers

- Keylogger Spy Monitor
  http://www.ematrixsoft.com
- REFOG Personal Monitor
  http://www.refog.com
- Actual Keylogger
  http://www.actualkeylogger.com
- Spytector
  http://www.spytector.com
- All In One Keylogger
  http://www.relytec.com
- WinSession Logger
  http://cromosoft.com
- Spy Lantern Keylogger Pro
  http://www.spy-lantern.com
- PC Spy Keylogger
  http://www.pc-spy-keylogger.com



Keyloggers

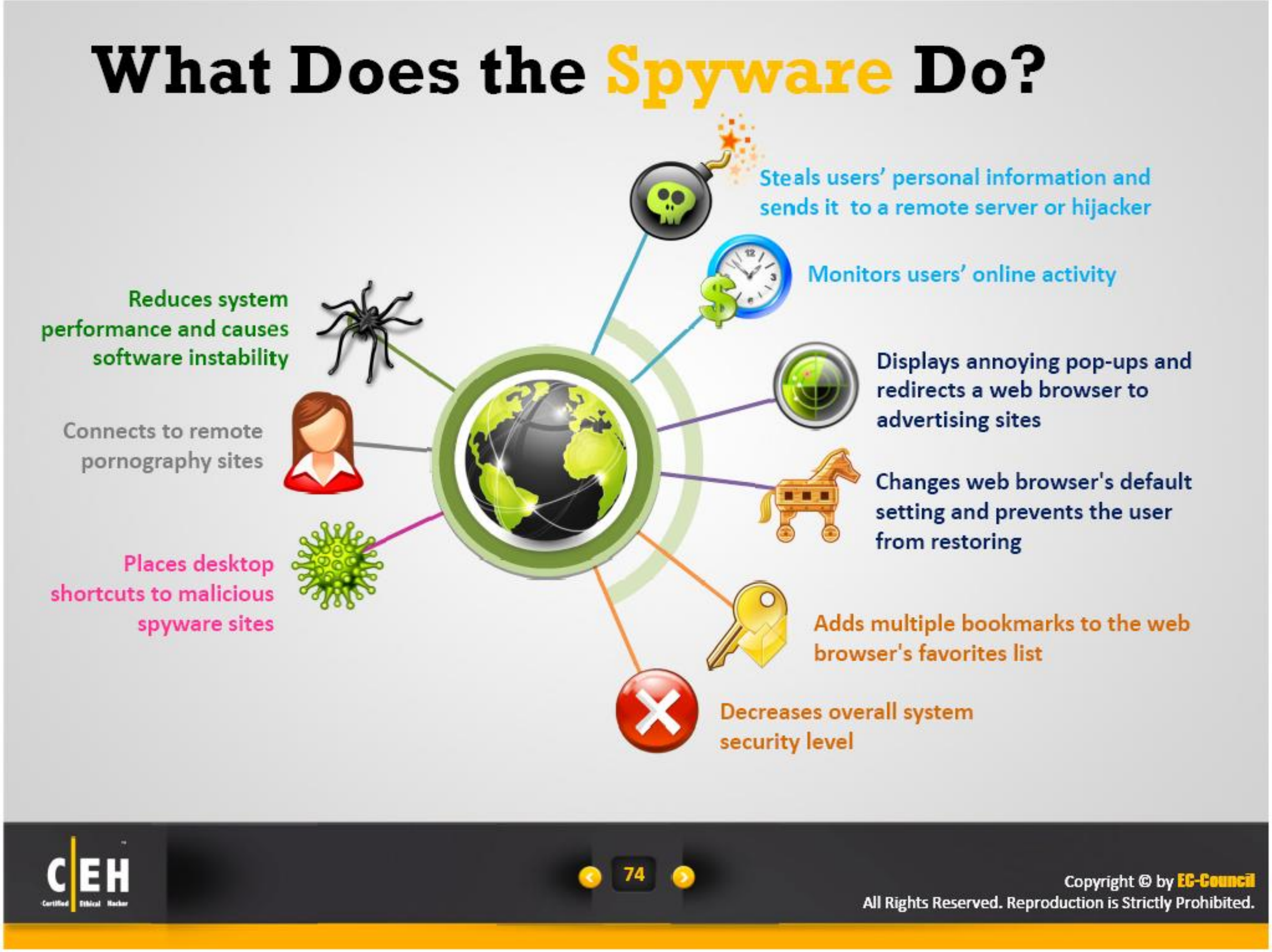
- **Golden Eye** *http://www.monitoring-spy-software.com*
- **Revealer Keylogger** *http://www.logixoft.com*
- **Spy Keylogger** *http://www.spy-key-logger.com*
- **IKS Software Keylogger** *http://amecisco.com*
- **Emsa FlexInfo Pro** *http://www.e-systems.ro*
- **Quick Keylogger** *http://www.quick-keylogger.com*
- **Actual Spy** *http://www.actualspy.com*
- **Ghost Keylogger** *http://www.keylogger.net*



Spyware

Spyware is a program that **records user's interaction** with the computer and Internet without the a user's knowledge. Spyware is stealthy, hiding its process, files, and other objects in order to avoid removal.

Spyware Propagation
Drive-by download
Masquerading as anti-spyware
Web browser vulnerability exploits
Piggybacked software installation
Browser add-ons
Cookies



What Does the Spyware Do?

Reduces system performance and causes software instability

Connects to remote pornography sites

Places desktop shortcuts to malicious spyware sites

Steals users' personal information and sends it to a remote server or hijacker

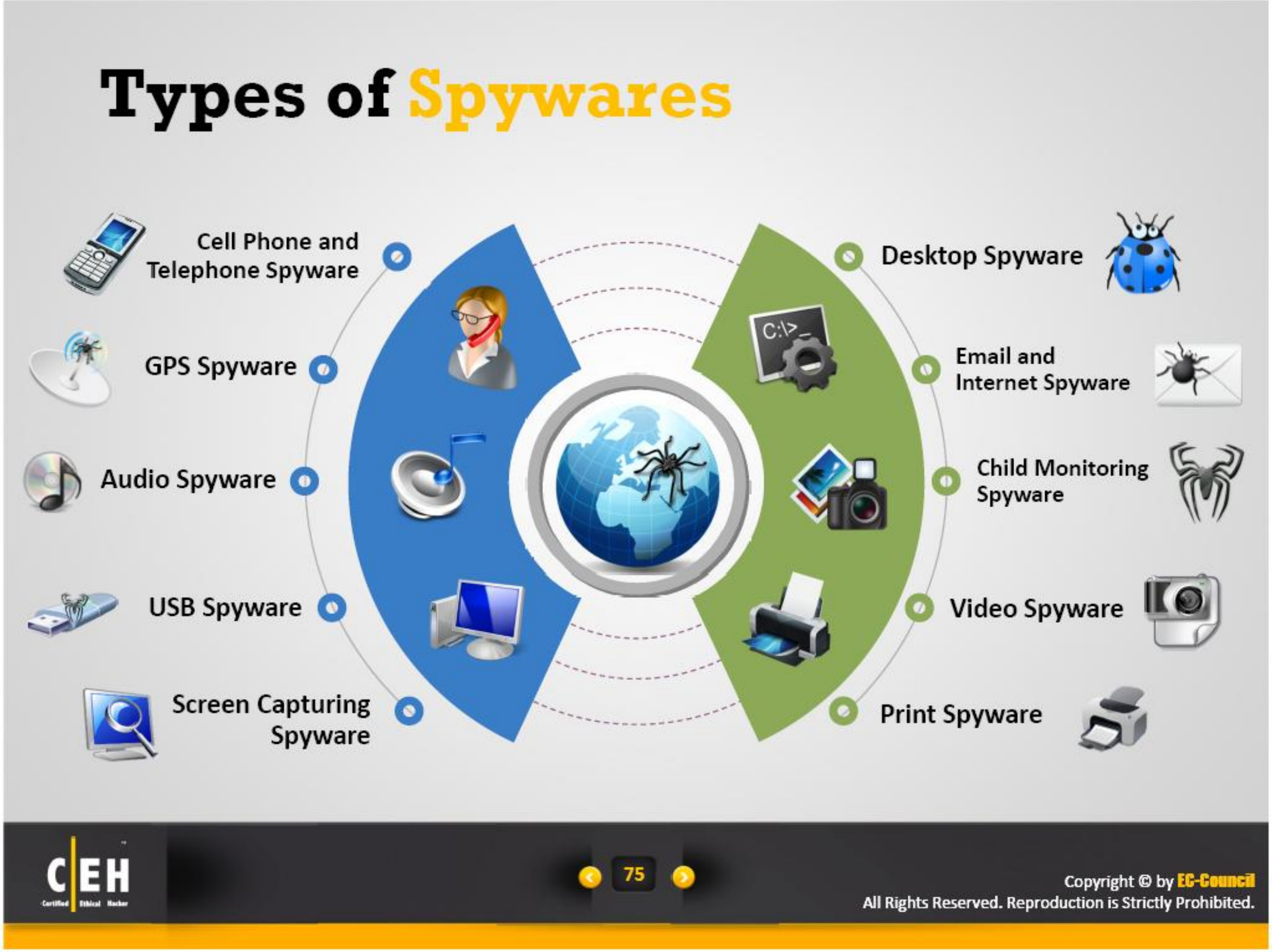
Monitors users' online activity

Displays annoying pop-ups and redirects a web browser to advertising sites

Changes web browser's default setting and prevents the user from restoring

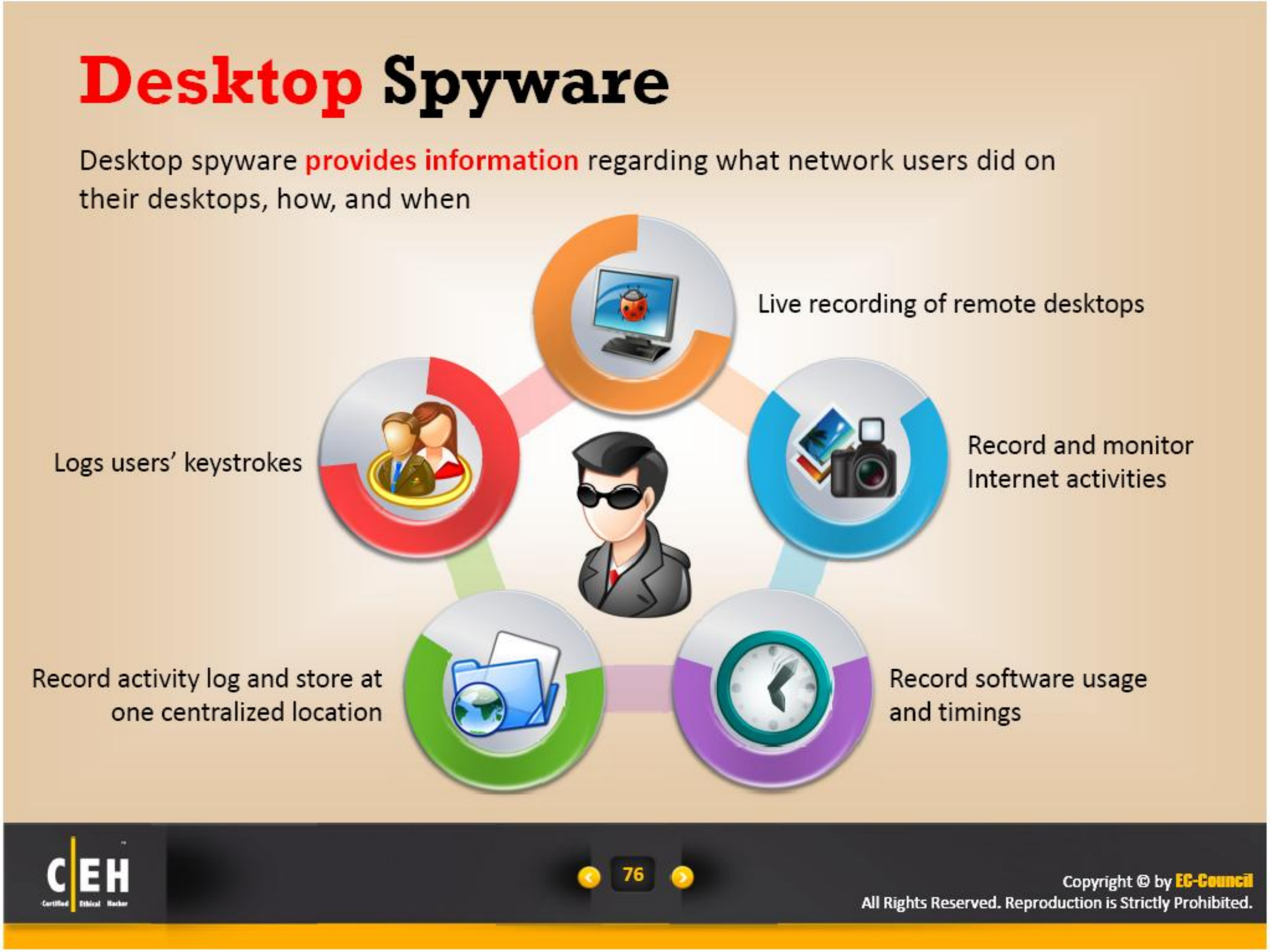
Adds multiple bookmarks to the web browser's favorites list

Decreases overall system security level



Types of Spywares

- Cell Phone and Telephone Spyware
- GPS Spyware
- Audio Spyware
- USB Spyware
- Screen Capturing Spyware
- Desktop Spyware
- Email and Internet Spyware
- Child Monitoring Spyware
- Video Spyware
- Print Spyware

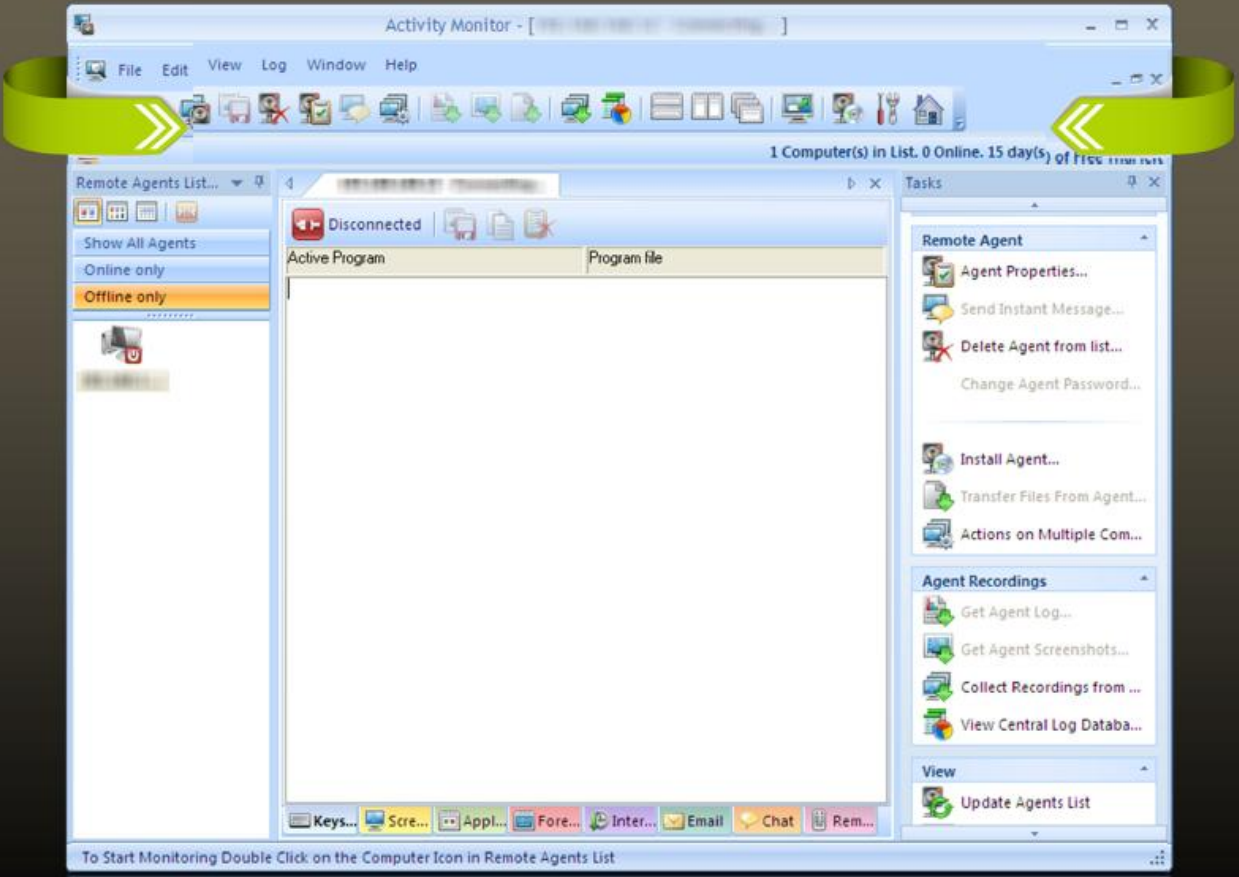


Desktop Spyware

Desktop spyware **provides information** regarding what network users did on their desktops, how, and when

- Live recording of remote desktops
- Record and monitor Internet activities
- Record software usage and timings
- Record activity log and store at one centralized location
- Logs users' keystrokes

Desktop Spyware: Activity Monitor

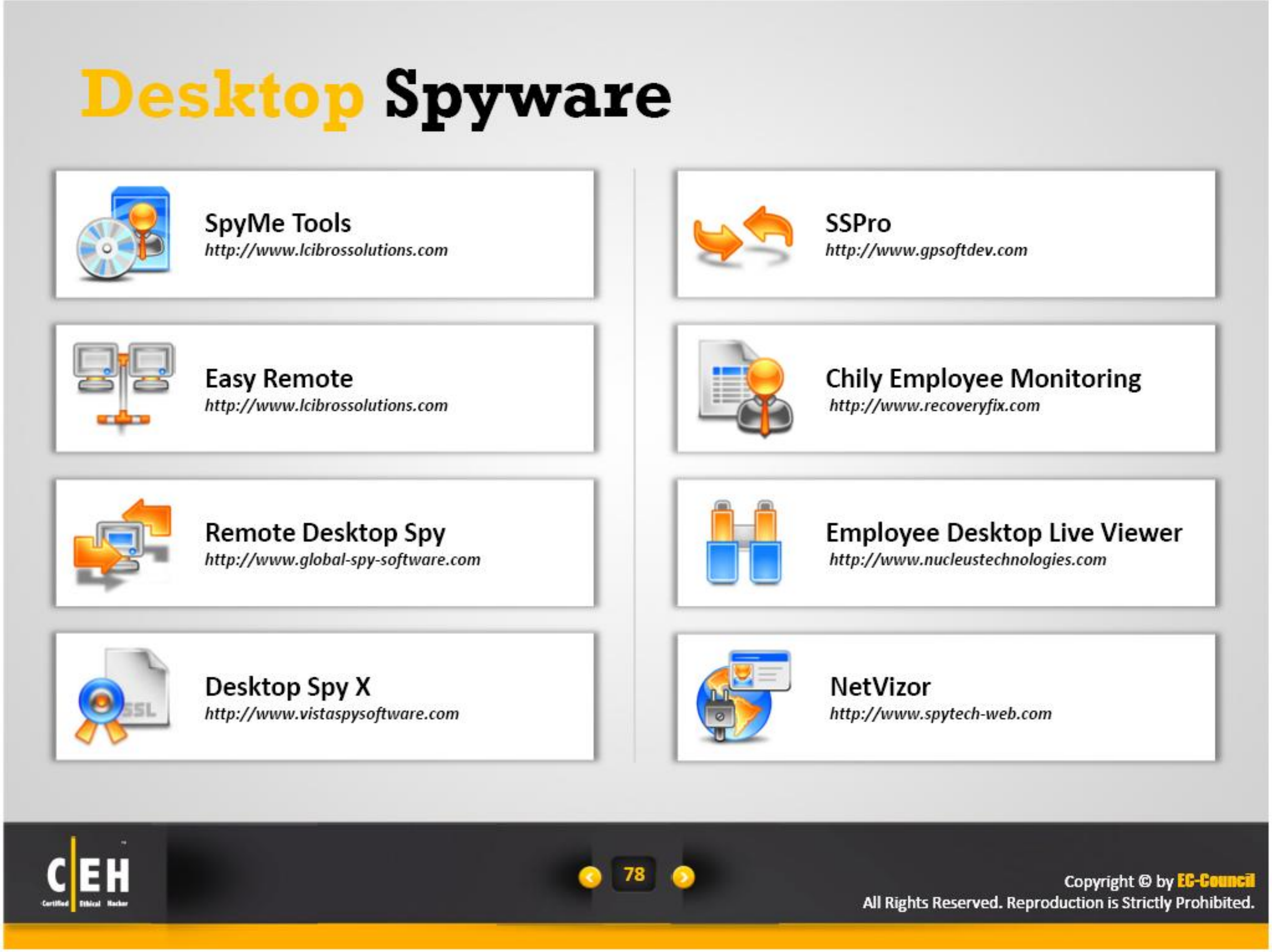


1 Computer(s) in List. 0 Online. 15 day(s) of free trial left

Active Program	Program file

To Start Monitoring Double Click on the Computer Icon in Remote Agents List

http://www.softactivity.com



Desktop Spyware

SpyMe Tools
http://www.lcibrossolutions.com

Easy Remote
http://www.lcibrossolutions.com

Remote Desktop Spy
http://www.global-spy-software.com

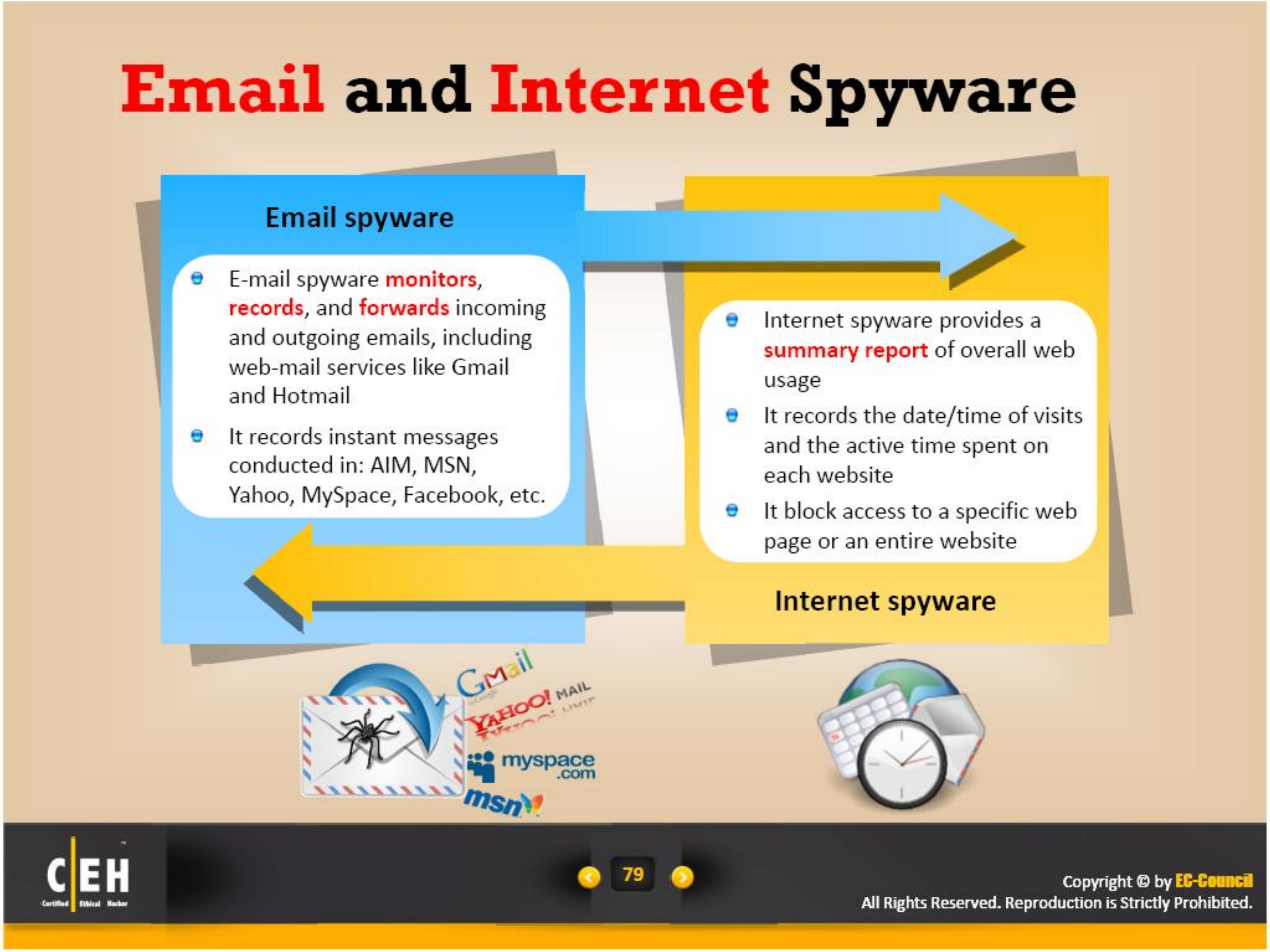
Desktop Spy X
http://www.vistaspysoftware.com

SSPro
http://www.gpsoftdev.com

Chily Employee Monitoring
http://www.recoveryfix.com

Employee Desktop Live Viewer
http://www.nucleustechnologies.com

NetVizor
http://www.spytech-web.com



Email and Internet Spyware

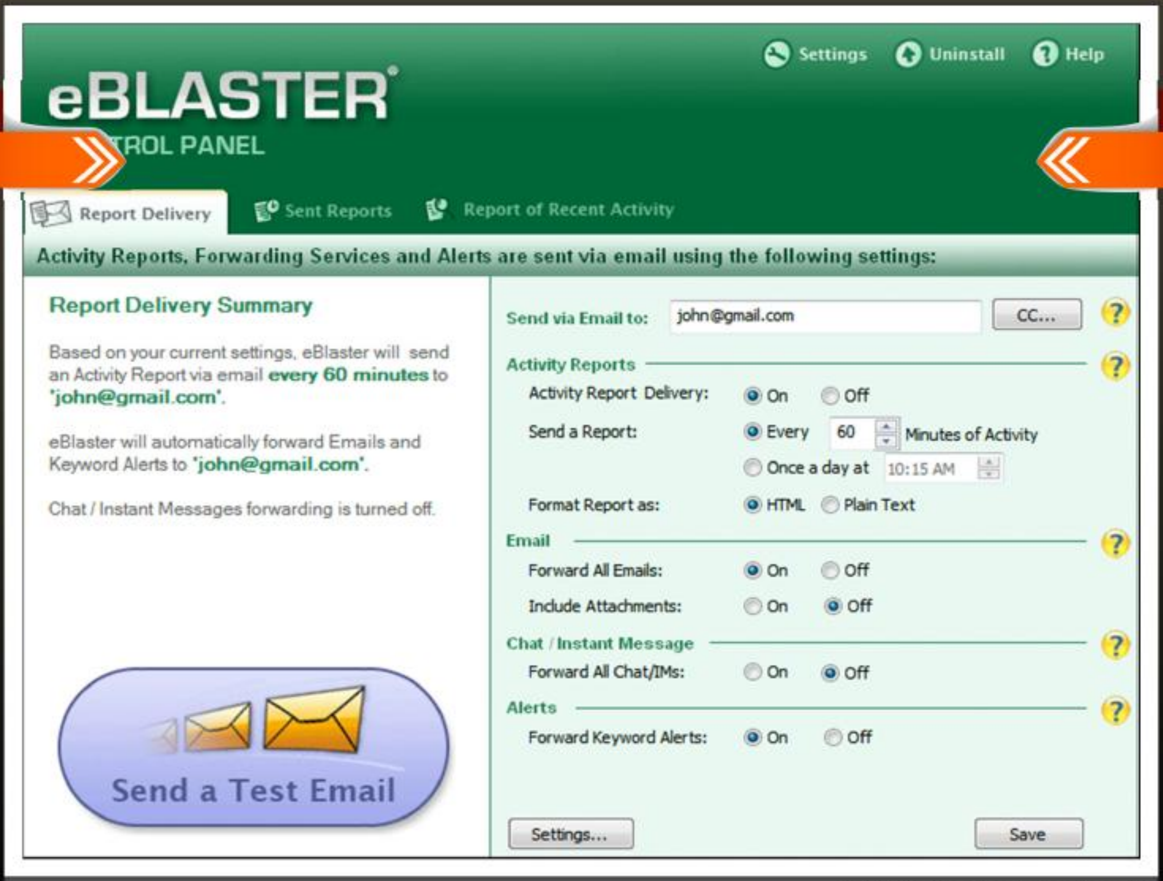
Email spyware

- E-mail spyware **monitors**, **records**, and **forwards** incoming and outgoing emails, including web-mail services like Gmail and Hotmail
- It records instant messages conducted in: AIM, MSN, Yahoo, MySpace, Facebook, etc.

Internet spyware

- Internet spyware provides a **summary report** of overall web usage
- It records the date/time of visits and the active time spent on each website
- It block access to a specific web page or an entire website

Email and Internet Spyware: eBLASTER



Activity Reports, Forwarding Services and Alerts are sent via email using the following settings:

Report Delivery Summary

Based on your current settings, eBlaster will send an Activity Report via email **every 60 minutes** to **'john@gmail.com'**.

eBlaster will automatically forward Emails and Keyword Alerts to **'john@gmail.com'**.

Chat / Instant Messages forwarding is turned off.

Send via Email to: john@gmail.com

Activity Reports

Activity Report Delivery: ● On ○ Off

Send a Report: ● Every 60 Minutes of Activity

○ Once a day at 10:15 AM

Format Report as: ● HTML ○ Plain Text

Email

Forward All Emails: ● On ○ Off

Include Attachments: ○ On ● Off

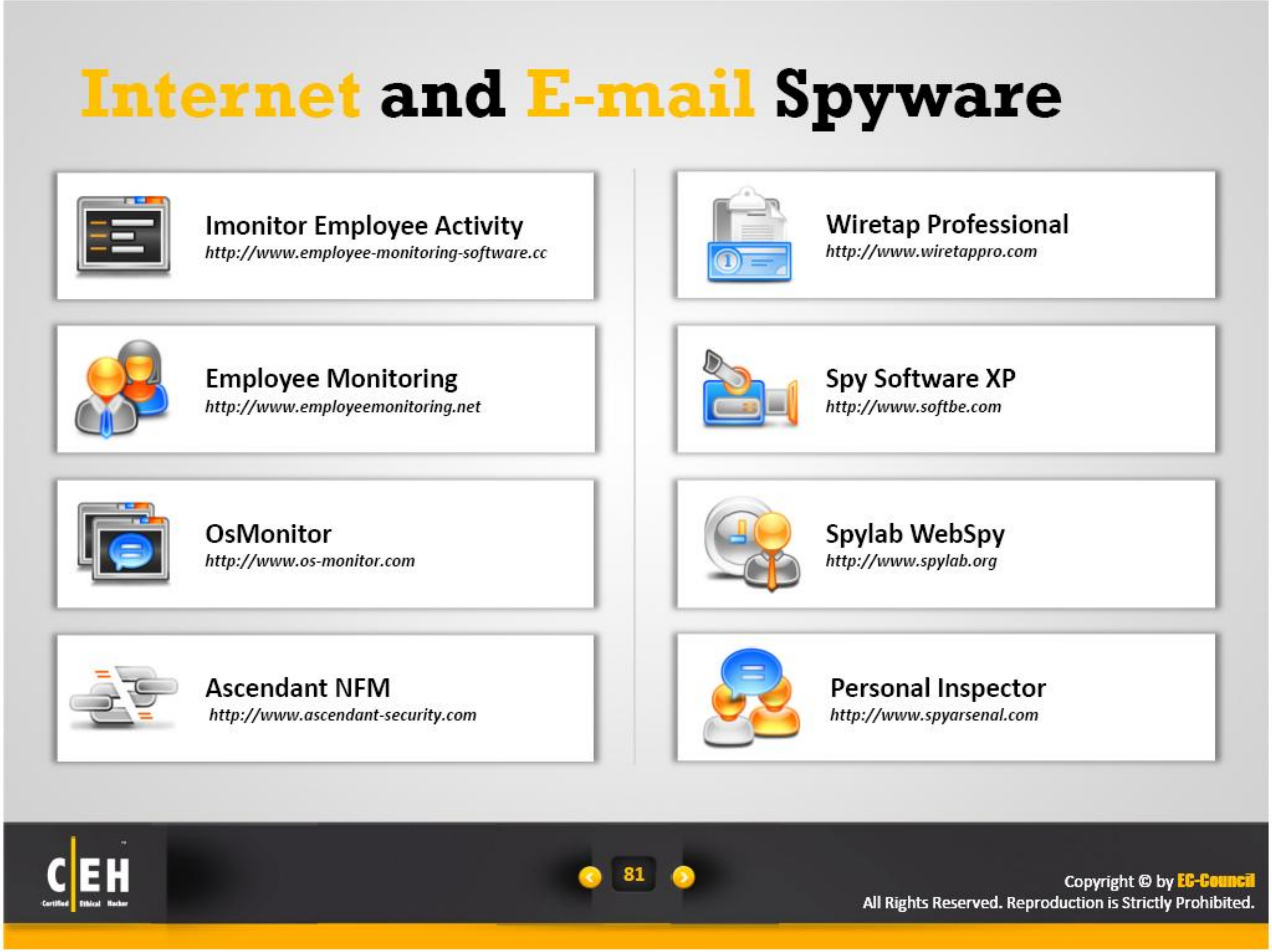
Chat / Instant Message

Forward All Chat/IMs: ○ On ● Off

Alerts

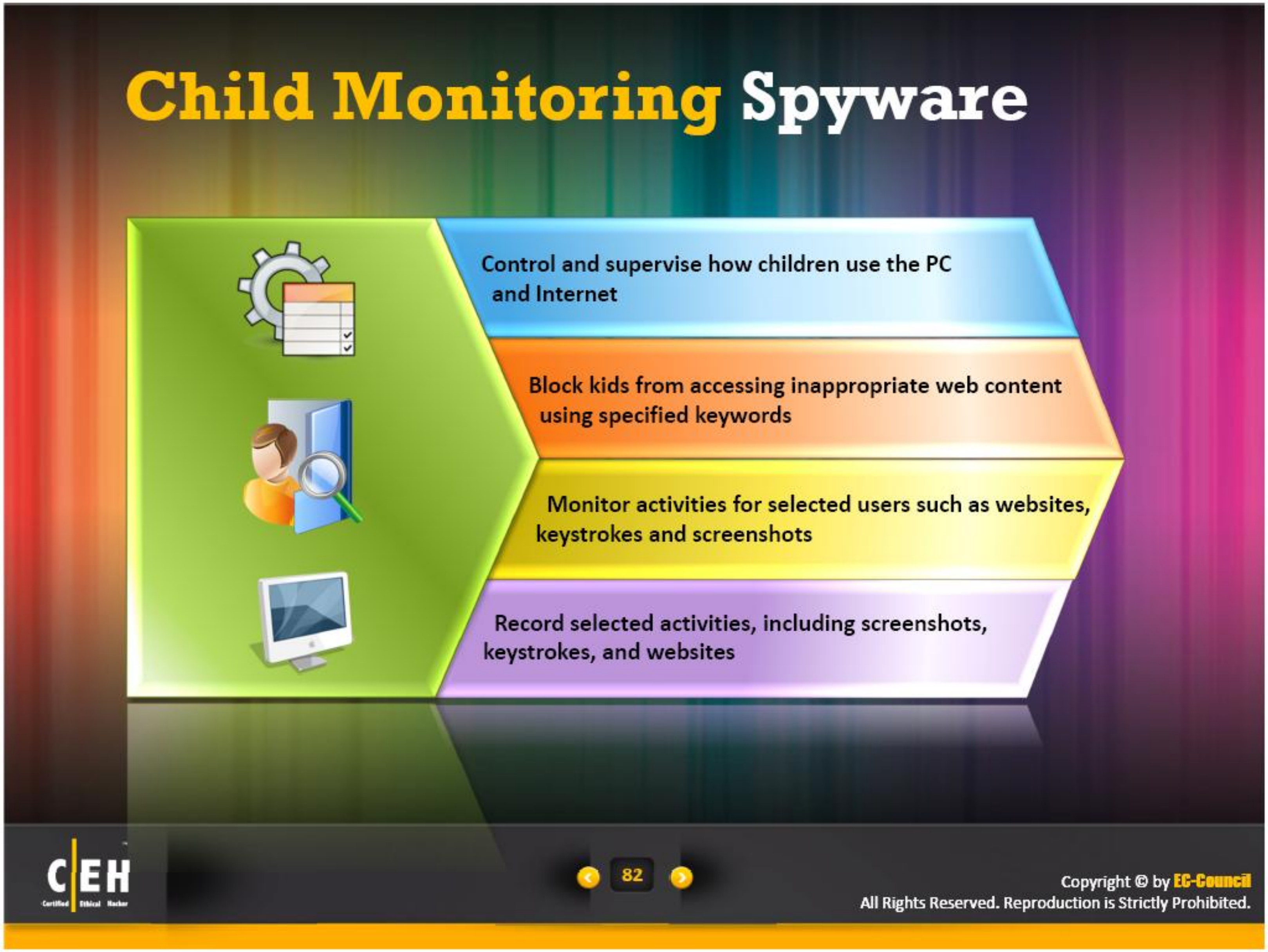
Forward Keyword Alerts: ● On ○ Off

http://www.spectorsoft.com



Internet and E-mail Spyware

- **Imonitor Employee Activity**
  http://www.employee-monitoring-software.cc
- **Employee Monitoring**
  http://www.employeemonitoring.net
- **OsMonitor**
  http://www.os-monitor.com
- **Ascendant NFM**
  http://www.ascendant-security.com
- **Wiretap Professional**
  http://www.wiretappro.com
- **Spy Software XP**
  http://www.softbe.com
- **Spylab WebSpy**
  http://www.spylab.org
- **Personal Inspector**
  http://www.spyarsenal.com

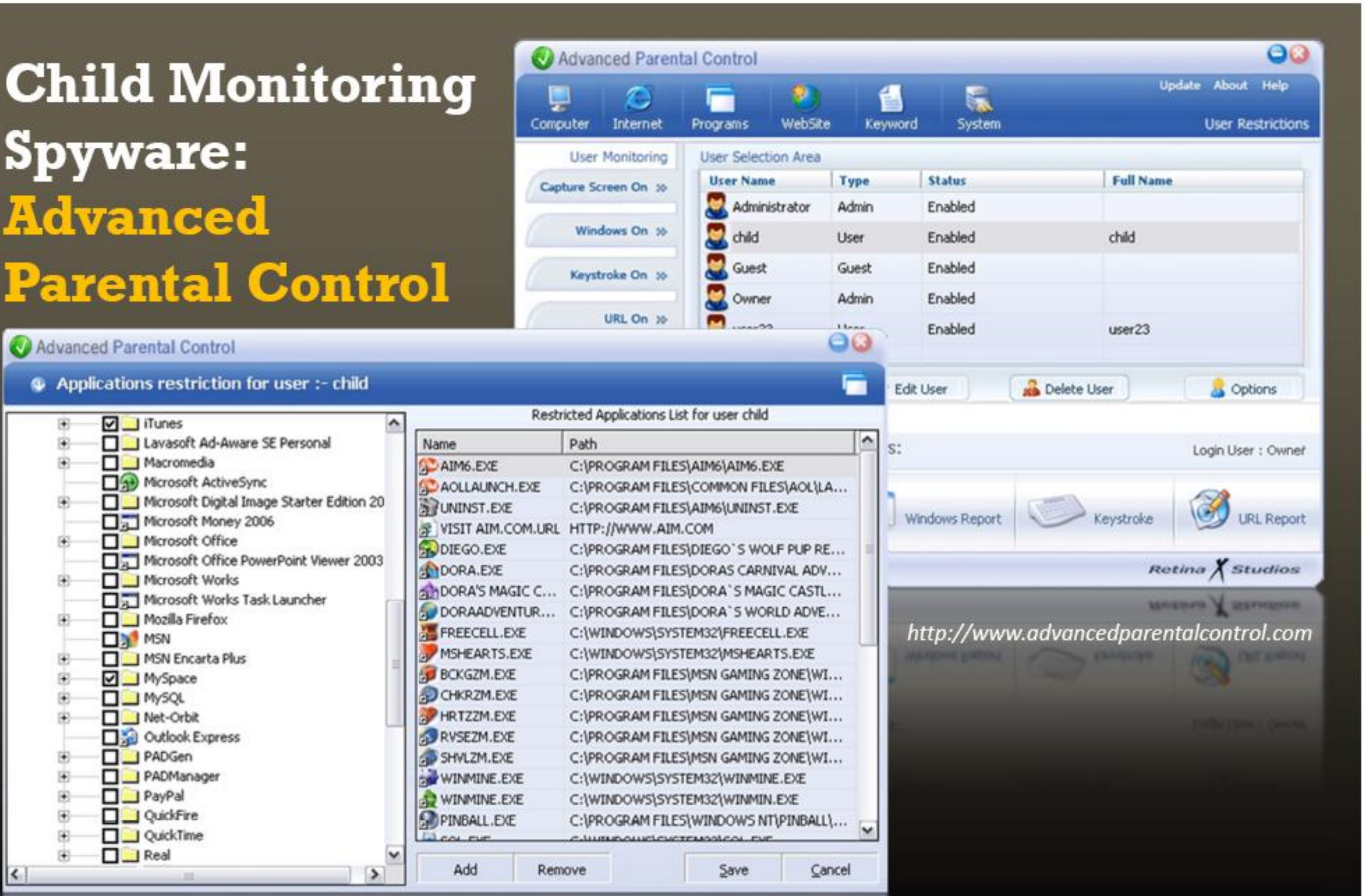


Child Monitoring Spyware

- Control and supervise how children use the PC and Internet
- Block kids from accessing inappropriate web content using specified keywords
- Monitor activities for selected users such as websites, keystrokes and screenshots
- Record selected activities, including screenshots, keystrokes, and websites

C|EH Certified Ethical Hacker

Child Monitoring Spyware: Advanced Parental Control



Advanced Parental Control

User Monitoring

- Capture Screen On »
- Windows On »
- Keystroke On »
- URL On »

User Selection Area

User Name	Type	Status	Full Name
Administrator	Admin	Enabled	
child	User	Enabled	child
Guest	Guest	Enabled	
Owner	Admin	Enabled	
user23	User	Enabled	user23

Login User : Owner

Advanced Parental Control

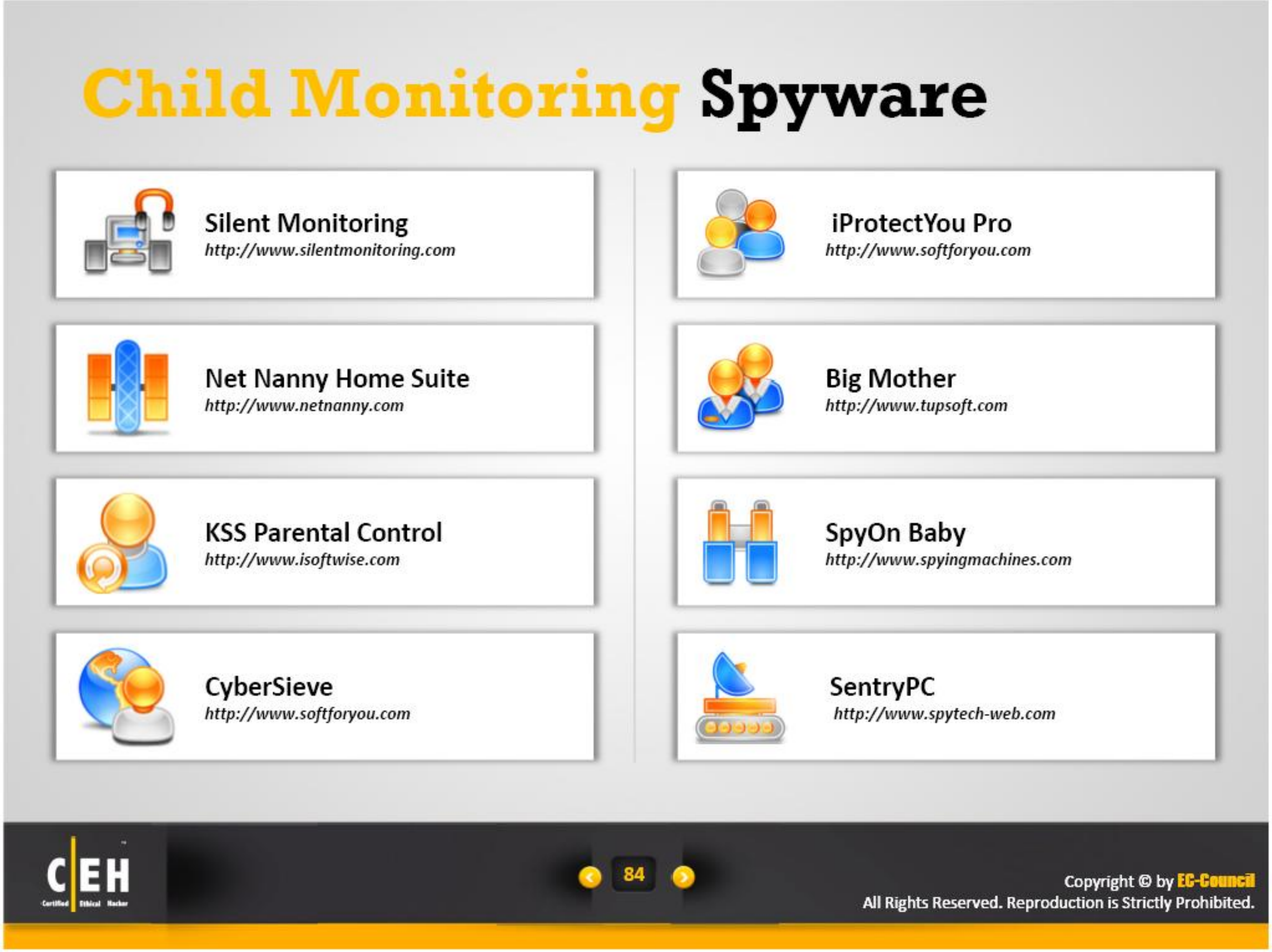
Applications restriction for user :- child

- ☑ iTunes
- □ Lavasoft Ad-Aware SE Personal
- □ Macromedia
- □ Microsoft ActiveSync
- □ Microsoft Digital Image Starter Edition 20
- □ Microsoft Money 2006
- □ Microsoft Office
- □ Microsoft Office PowerPoint Viewer 2003
- □ Microsoft Works
- □ Microsoft Works Task Launcher
- □ Mozilla Firefox
- □ MSN
- □ MSN Encarta Plus
- ☑ MySpace
- □ MySQL
- □ Net-Orbit
- □ Outlook Express
- □ PADGen
- □ PADManager
- □ PayPal
- □ QuickFire
- □ QuickTime
- □ Real

Restricted Applications List for user child

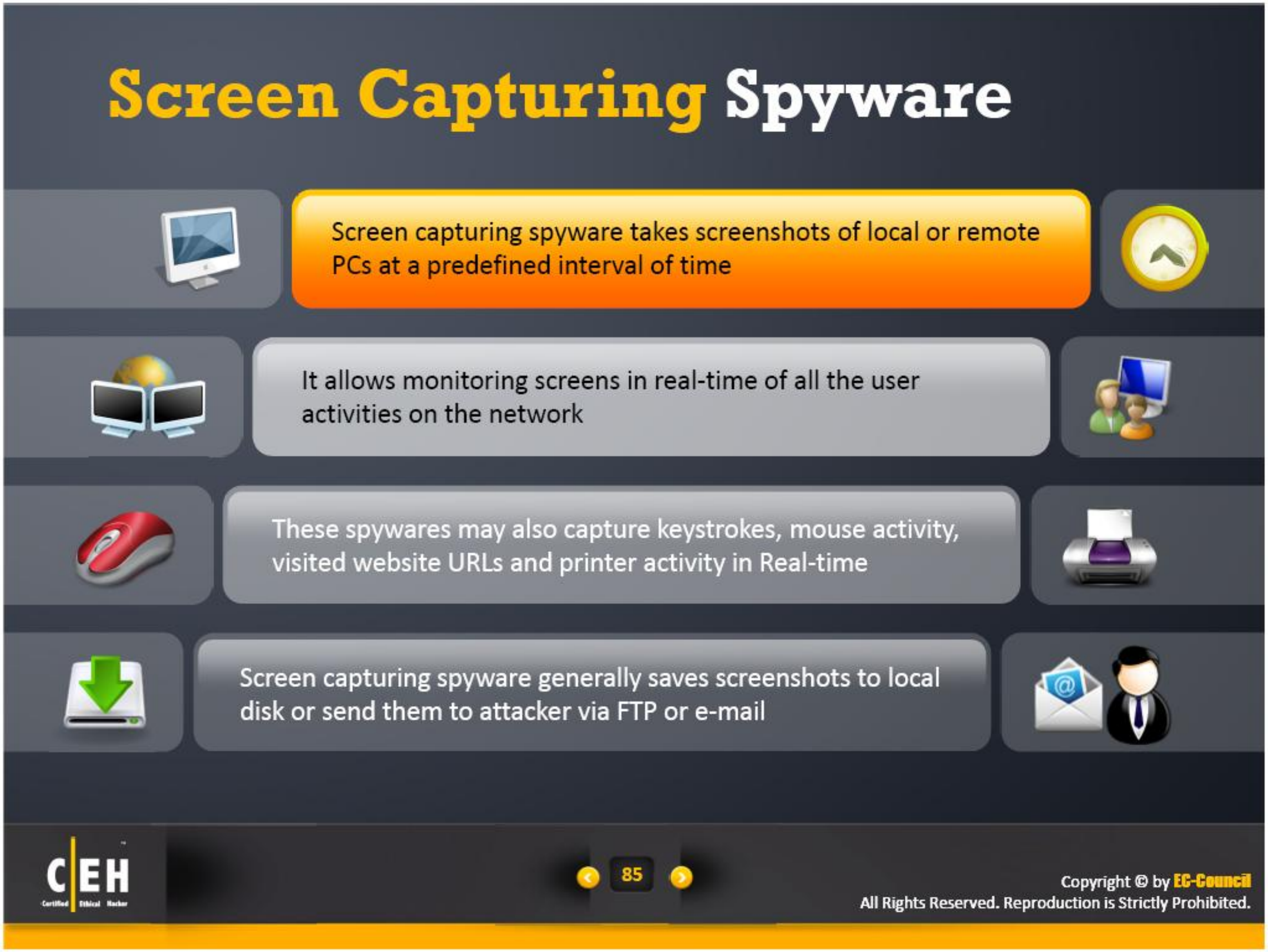
Name	Path
AIM6.EXE	C:\PROGRAM FILES\AIM6\AIM6.EXE
AOLLAUNCH.EXE	C:\PROGRAM FILES\COMMON FILES\AOL\LA...
UNINST.EXE	C:\PROGRAM FILES\AIM6\UNINST.EXE
VISIT AIM.COM.URL	HTTP://WWW.AIM.COM
DIEGO.EXE	C:\PROGRAM FILES\DIEGO`S WOLF PUP RE...
DORA.EXE	C:\PROGRAM FILES\DORAS CARNIVAL ADV...
DORA'S MAGIC C...	C:\PROGRAM FILES\DORA`S MAGIC CASTL...
DORAADVENTUR...	C:\PROGRAM FILES\DORA`S WORLD ADVE...
FREECELL.EXE	C:\WINDOWS\SYSTEM32\FREECELL.EXE
MSHEARTS.EXE	C:\WINDOWS\SYSTEM32\MSHEARTS.EXE
BCKGZM.EXE	C:\PROGRAM FILES\MSN GAMING ZONE\WI...
CHKRZM.EXE	C:\PROGRAM FILES\MSN GAMING ZONE\WI...
HRTZZM.EXE	C:\PROGRAM FILES\MSN GAMING ZONE\WI...
RVSEZM.EXE	C:\PROGRAM FILES\MSN GAMING ZONE\WI...
SHVLZM.EXE	C:\PROGRAM FILES\MSN GAMING ZONE\WI...
WINMINE.EXE	C:\WINDOWS\SYSTEM32\WINMINE.EXE
WINMINE.EXE	C:\WINDOWS\SYSTEM32\WINMIN.EXE
PINBALL.EXE	C:\PROGRAM FILES\WINDOWS NT\PINBALL\...

http://www.advancedparentalcontrol.com



Child Monitoring Spyware

Silent Monitoring *http://www.silentmonitoring.com*	**iProtectYou Pro** *http://www.softforyou.com*
Net Nanny Home Suite *http://www.netnanny.com*	**Big Mother** *http://www.tupsoft.com*
KSS Parental Control *http://www.isoftwise.com*	**SpyOn Baby** *http://www.spyingmachines.com*
CyberSieve *http://www.softforyou.com*	**SentryPC** *http://www.spytech-web.com*



Screen Capturing Spyware

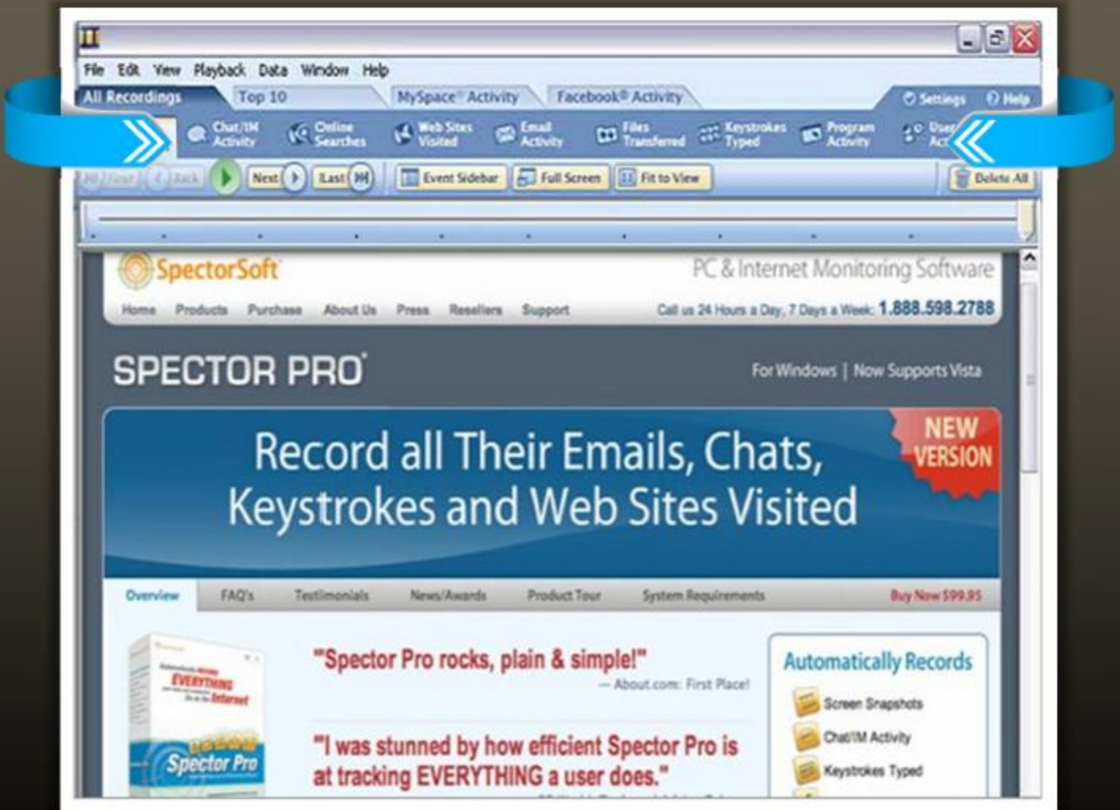
Screen capturing spyware takes screenshots of local or remote PCs at a predefined interval of time

It allows monitoring screens in real-time of all the user activities on the network

These spywares may also capture keystrokes, mouse activity, visited website URLs and printer activity in Real-time

Screen capturing spyware generally saves screenshots to local disk or send them to attacker via FTP or e-mail

Screen Capturing Spyware: Spector Pro



PC & Internet Monitoring Software

Call us 24 Hours a Day, 7 Days a Week: 1.888.598.2788

SPECTOR PRO®

For Windows | Now Supports Vista

Record all Their Emails, Chats, Keystrokes and Web Sites Visited

NEW VERSION

"Spector Pro rocks, plain & simple!"

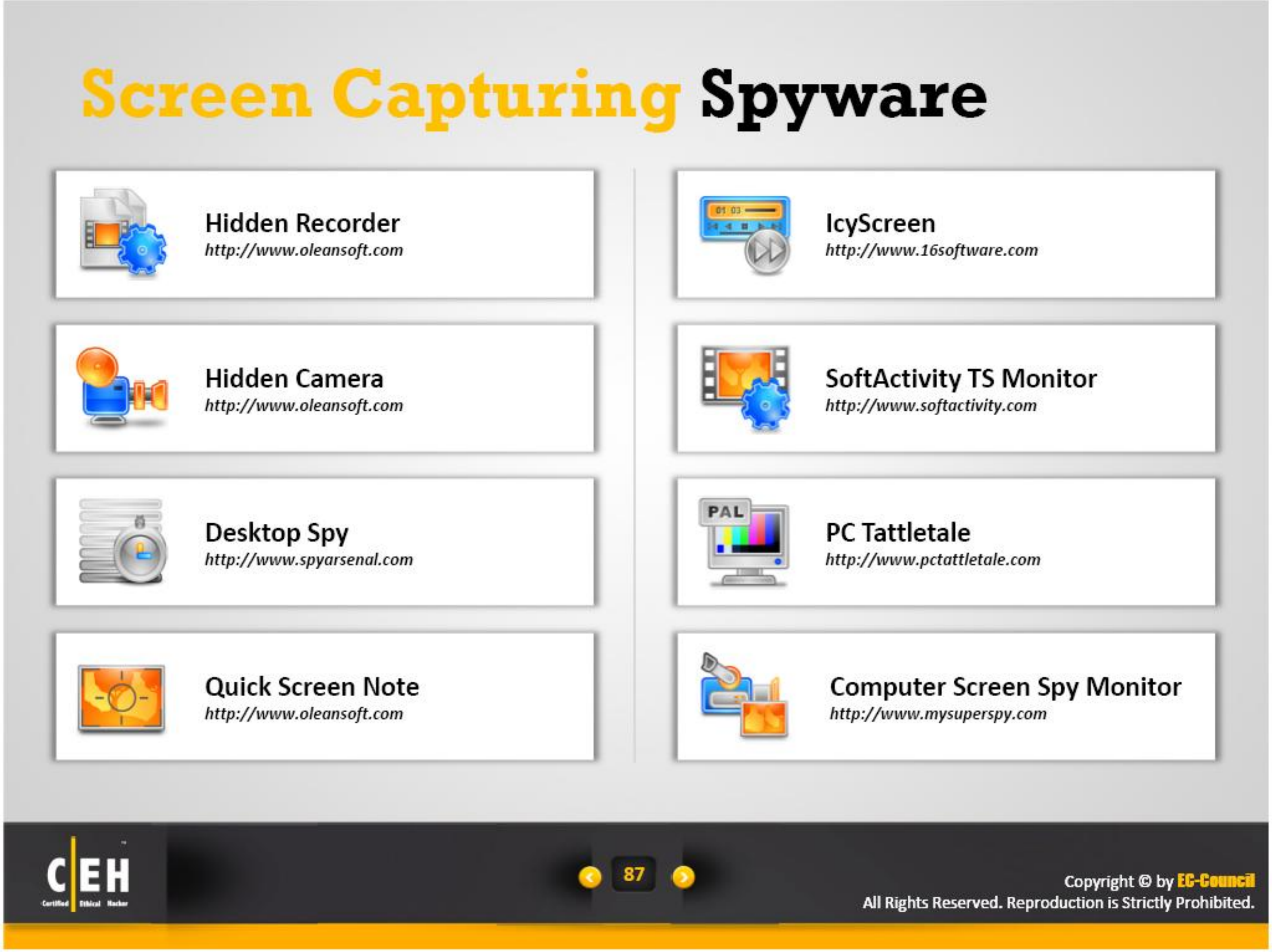
— About.com: First Place!

"I was stunned by how efficient Spector Pro is at tracking EVERYTHING a user does."

Automatically Records

- Screen Snapshots
- Chat/IM Activity
- Keystrokes Typed

http://www.spectorsoft.com



Screen Capturing Spyware

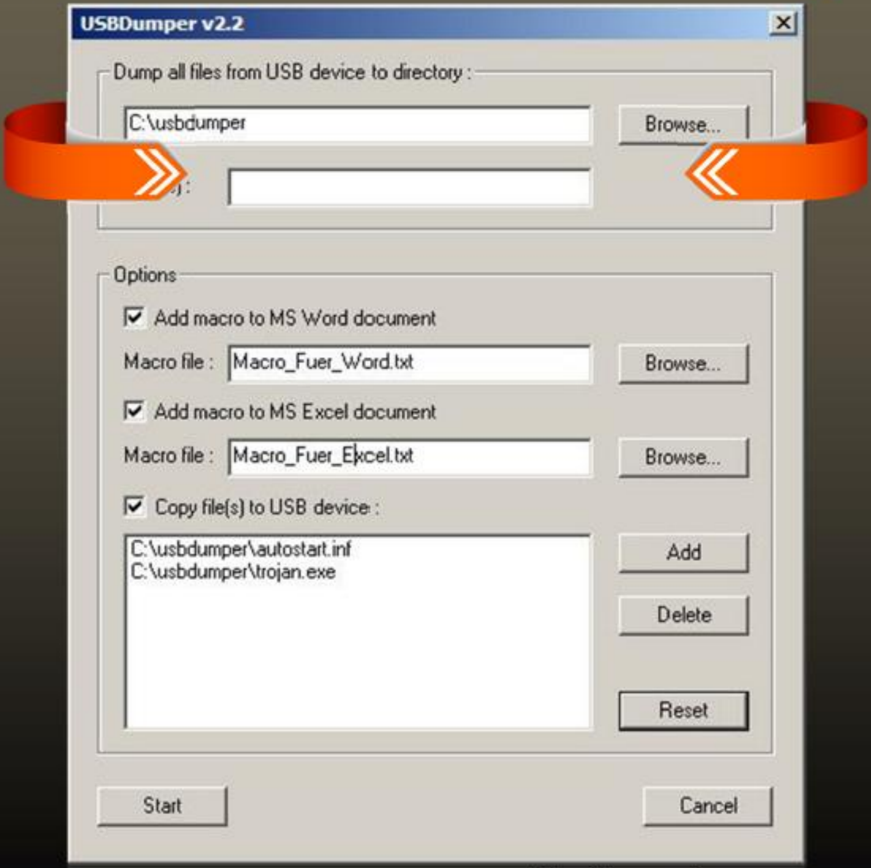
- **Hidden Recorder**
  http://www.oleansoft.com
- **Hidden Camera**
  http://www.oleansoft.com
- **Desktop Spy**
  http://www.spyarsenal.com
- **Quick Screen Note**
  http://www.oleansoft.com
- **IcyScreen**
  http://www.16software.com
- **SoftActivity TS Monitor**
  http://www.softactivity.com
- **PC Tattletale**
  http://www.pctattletale.com
- **Computer Screen Spy Monitor**
  http://www.mysuperspy.com

C|EH Certified Ethical Hacker

USB Spyware

- USB spyware **copies files** from USB devices to your hard disk in hidden mode without any request
- It may also capture, display, record and analyze **data transferred** between any USB device a connected to PC and applications

USB Spyware: USBDumper



USBDumper v2.2

Dump all files from USB device to directory : C:\usbdumper

Options

☑ Add macro to MS Word document

Macro file : Macro_Fuer_Word.txt

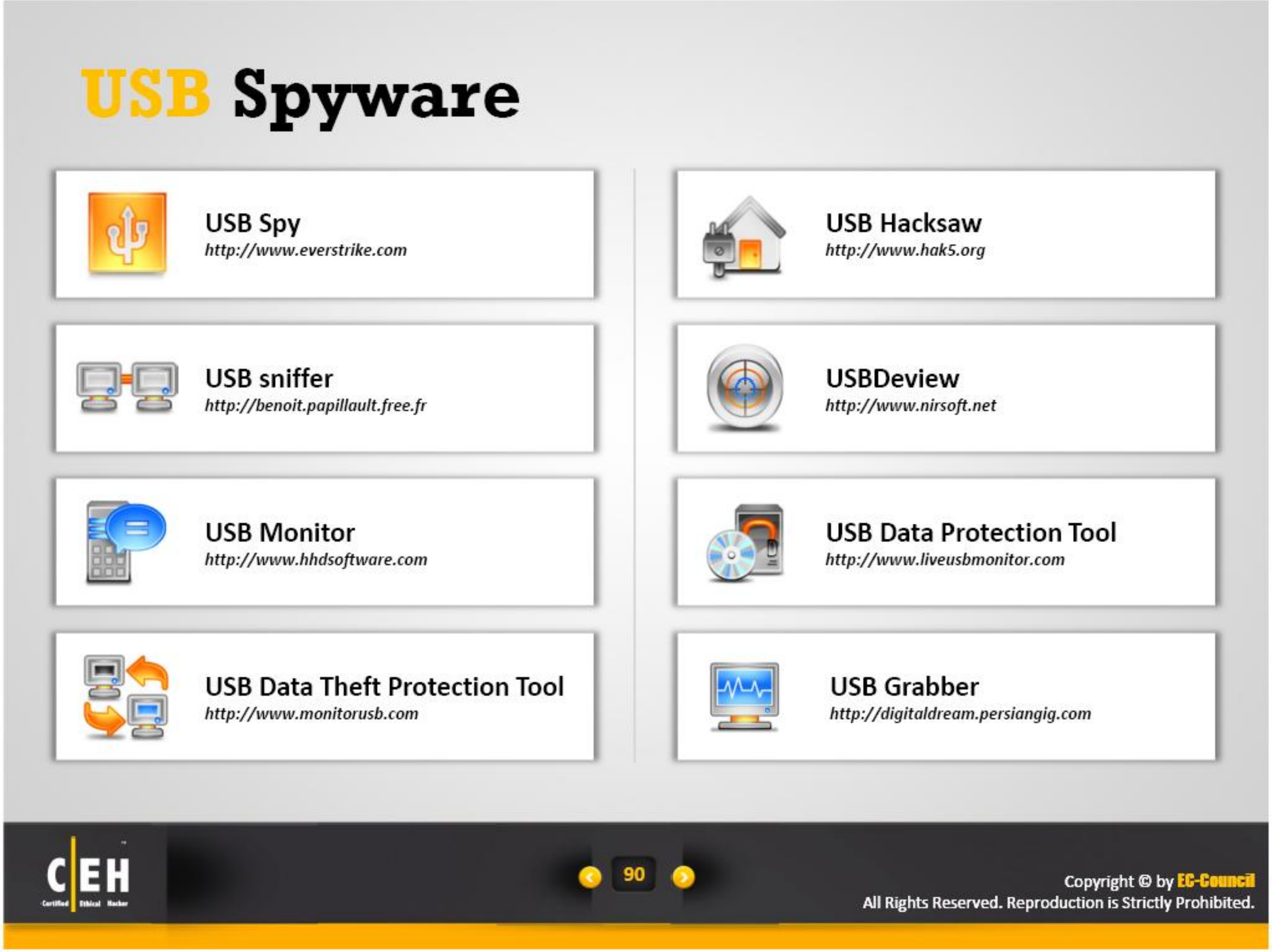
☑ Add macro to MS Excel document

Macro file : Macro_Fuer_Excel.txt

☑ Copy file(s) to USB device :

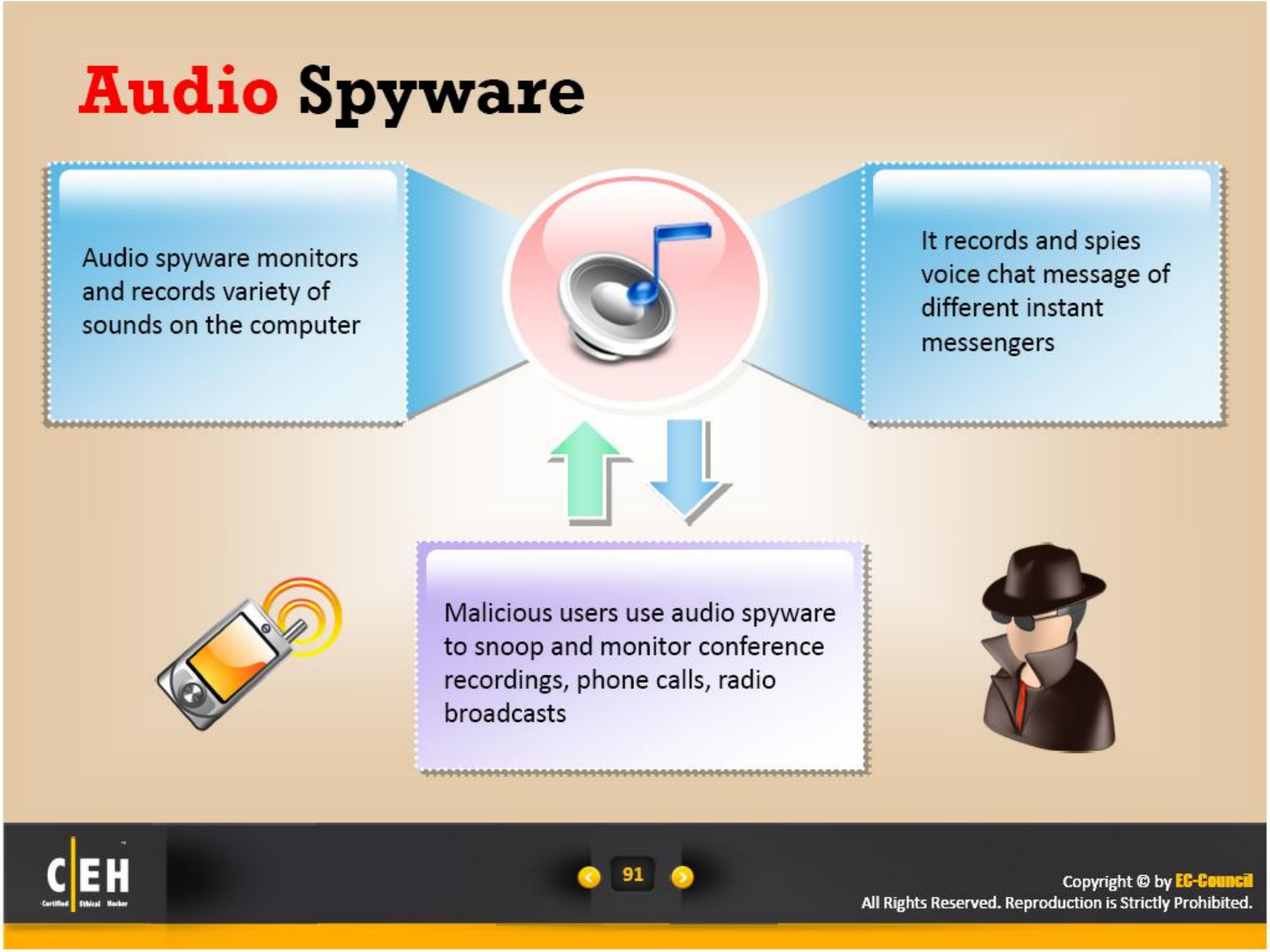
C:\usbdumper\autostart.inf
C:\usbdumper\trojan.exe

http://www.valgasu.org



USB Spyware

- USB Spy
  http://www.everstrike.com
- USB sniffer
  http://benoit.papillault.free.fr
- USB Monitor
  http://www.hhdsoftware.com
- USB Data Theft Protection Tool
  http://www.monitorusb.com
- USB Hacksaw
  http://www.hak5.org
- USBDeview
  http://www.nirsoft.net
- USB Data Protection Tool
  http://www.liveusbmonitor.com
- USB Grabber
  http://digitaldream.persiangig.com



Audio Spyware

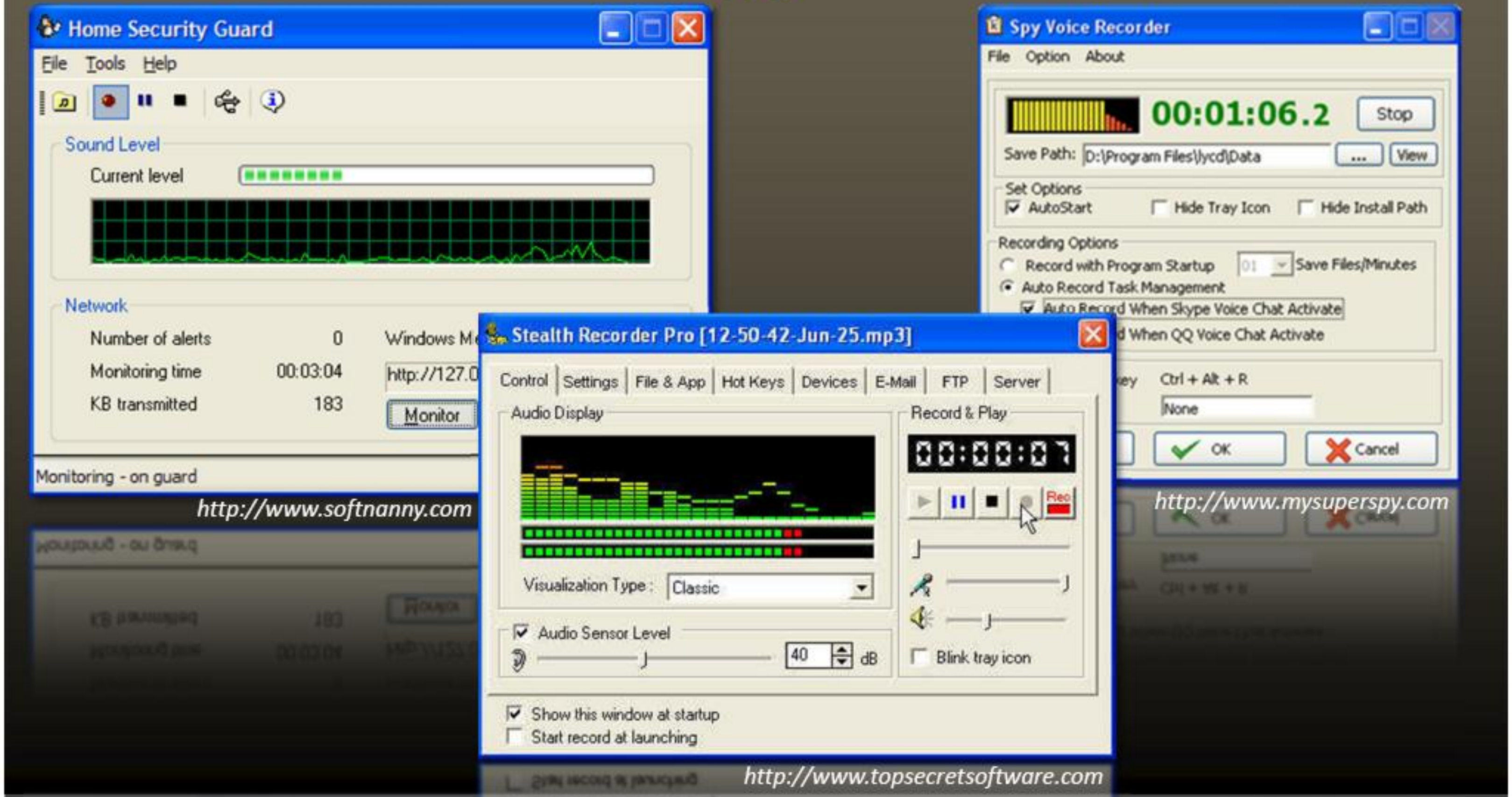
Audio spyware monitors and records variety of sounds on the computer

It records and spies voice chat message of different instant messengers

Malicious users use audio spyware to snoop and monitor conference recordings, phone calls, radio broadcasts

CEH
Certified Ethical Hacker

Audio Spyware: RoboNanny, Stealth Recorder Pro and Spy Voice Recorder



Home Security Guard

File Tools Help

Sound Level

Current level

Network

Number of alerts 0

Monitoring time 00:03:04

KB transmitted 183

Windows M

http://127.0

Monitor

Monitoring - on guard

http://www.softnanny.com

Spy Voice Recorder

File Option About

00:01:06.2 Stop

Save Path: D:\Program Files\lycd\Data ... View

Set Options

☑ AutoStart ☐ Hide Tray Icon ☐ Hide Install Path

Recording Options

○ Record with Program Startup 01 Save Files/Minutes

● Auto Record Task Management

☑ Auto Record When Skype Voice Chat Activate

d When QQ Voice Chat Activate

ey Ctrl + Alt + R

None

OK Cancel

http://www.mysuperspy.com

Stealth Recorder Pro [12-50-42-Jun-25.mp3]

Control | Settings | File & App | Hot Keys | Devices | E-Mail | FTP | Server

Audio Display

Visualization Type: Classic

☑ Audio Sensor Level 40 dB

Record & Play

00:00:07

☐ Blink tray icon

☑ Show this window at startup

☐ Start record at launching

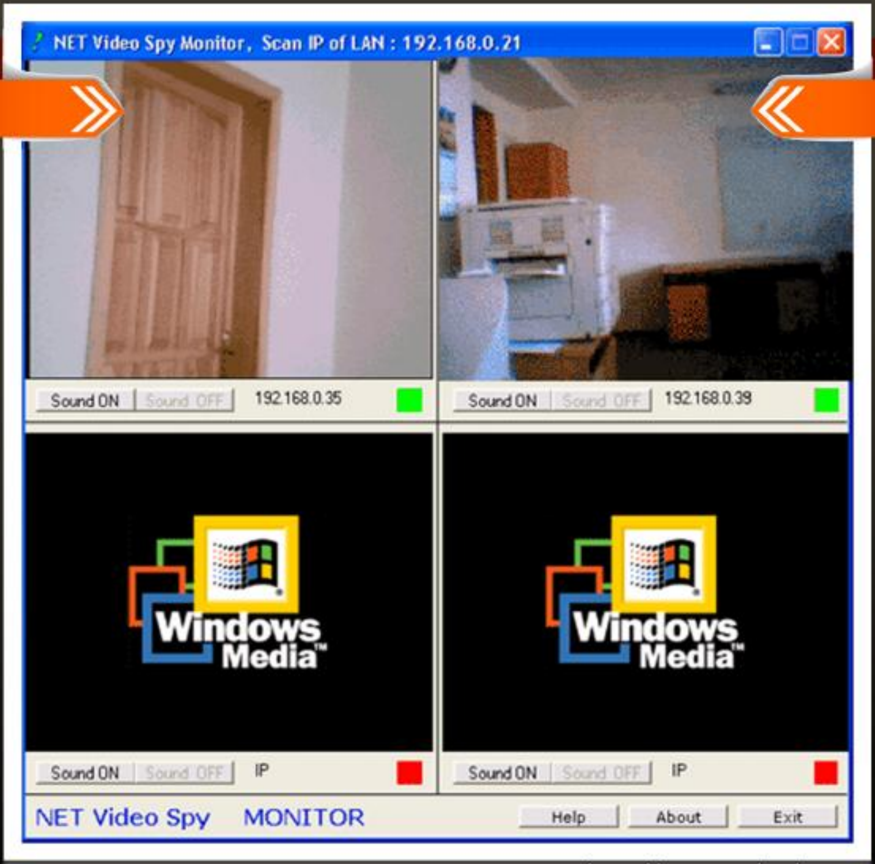
http://www.topsecretsoftware.com

Video Spyware

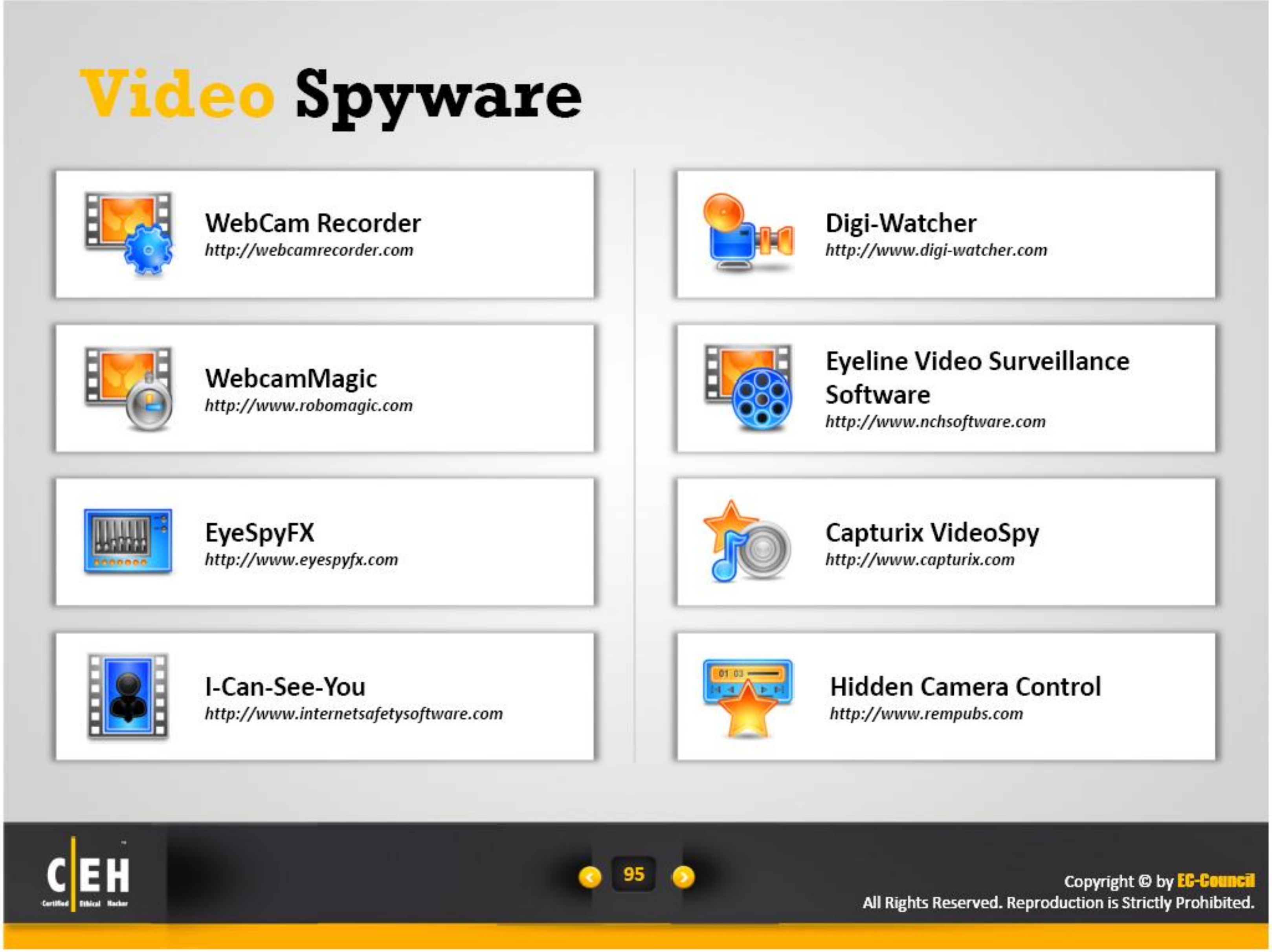
- Video spyware secretly **monitors** and **records** webcams and video IM conversions
- Attackers can remotely view webcams via the web or mobile phones
- Video spyware can be used for **video surveillance** of sensitive facilities

User
Hacker

Video Spyware: Net Video Spy



http://www.sarbash.com



Video Spyware

WebCam Recorder
http://webcamrecorder.com

WebcamMagic
http://www.robomagic.com

EyeSpyFX
http://www.eyespyfx.com

I-Can-See-You
http://www.internetsafetysoftware.com

Digi-Watcher
http://www.digi-watcher.com

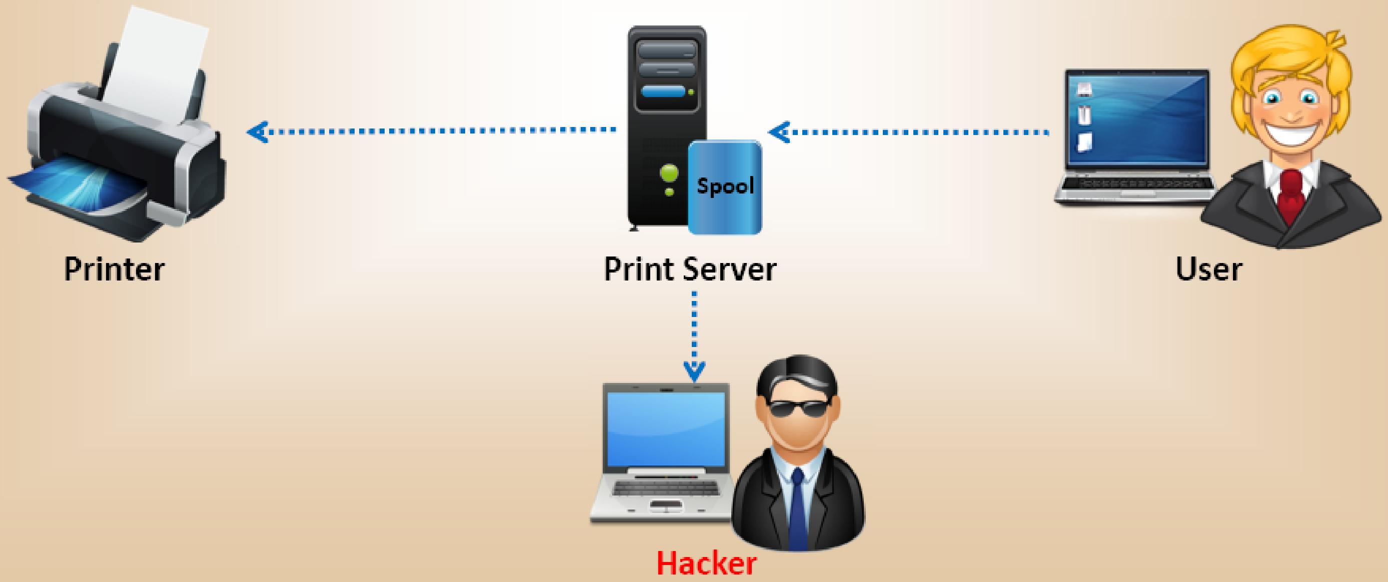
Eyeline Video Surveillance Software
http://www.nchsoftware.com

Capturix VideoSpy
http://www.capturix.com

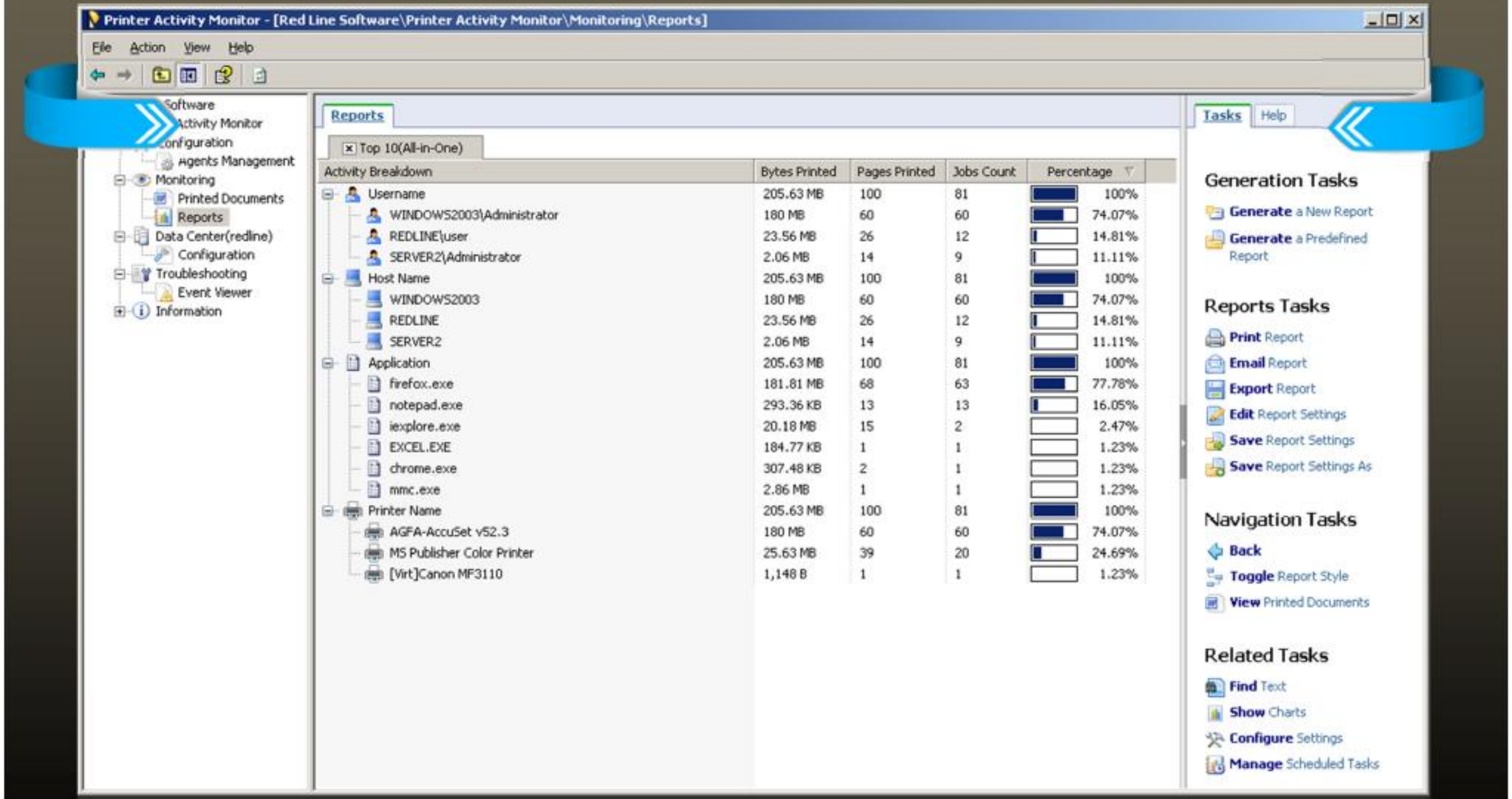
Hidden Camera Control
http://www.rempubs.com

Print Spyware

- Printer spyware facilitates remote printer usage monitoring
- It can be used to detect exact **print job properties** such as number of copies, number of printed pages, and content printed

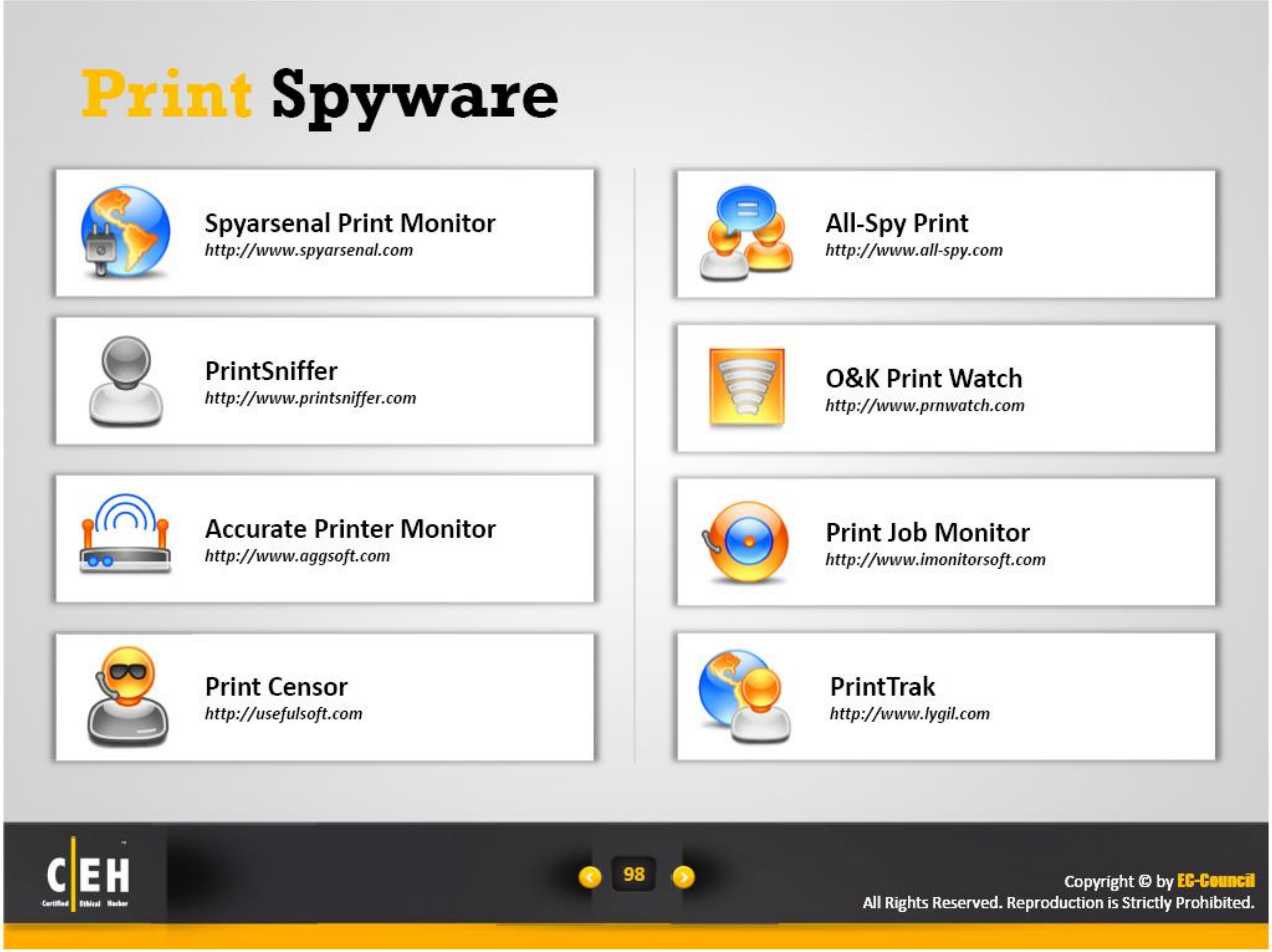


Print Spyware: Printer Activity Monitor



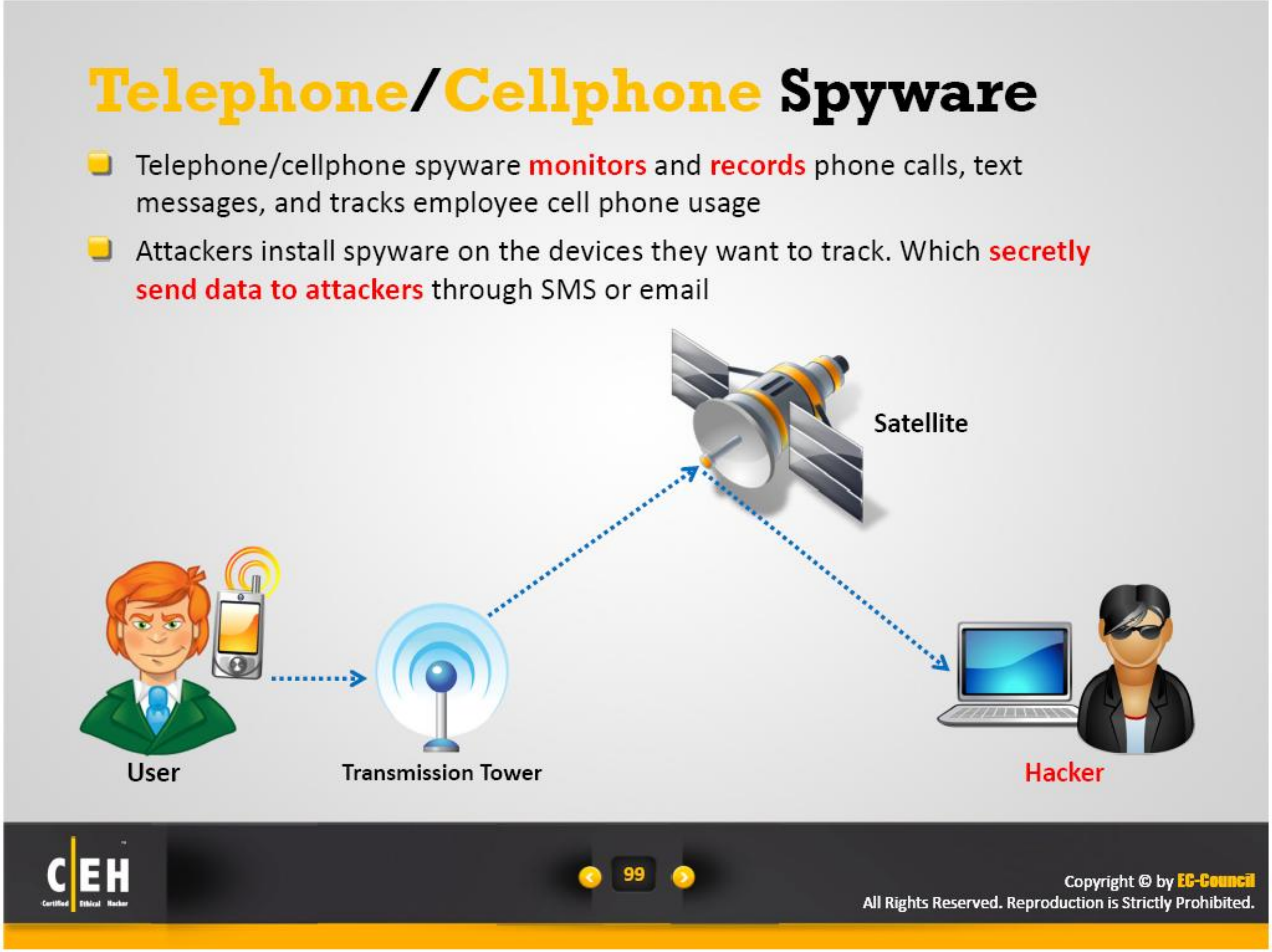
Activity Breakdown	Bytes Printed	Pages Printed	Jobs Count	Percentage
Username	205.63 MB	100	81	100%
WINDOWS2003\Administrator	180 MB	60	60	74.07%
REDLINE\user	23.56 MB	26	12	14.81%
SERVER2\Administrator	2.06 MB	14	9	11.11%
Host Name	205.63 MB	100	81	100%
WINDOWS2003	180 MB	60	60	74.07%
REDLINE	23.56 MB	26	12	14.81%
SERVER2	2.06 MB	14	9	11.11%
Application	205.63 MB	100	81	100%
firefox.exe	181.81 MB	68	63	77.78%
notepad.exe	293.36 KB	13	13	16.05%
iexplore.exe	20.18 MB	15	2	2.47%
EXCEL.EXE	184.77 KB	1	1	1.23%
chrome.exe	307.48 KB	2	1	1.23%
mmc.exe	2.86 MB	1	1	1.23%
Printer Name	205.63 MB	100	81	100%
AGFA-AccuSet v52.3	180 MB	60	60	74.07%
MS Publisher Color Printer	25.63 MB	39	20	24.69%
[Virt]Canon MF3110	1,148 B	1	1	1.23%

http://www.redline-software.com



Print Spyware

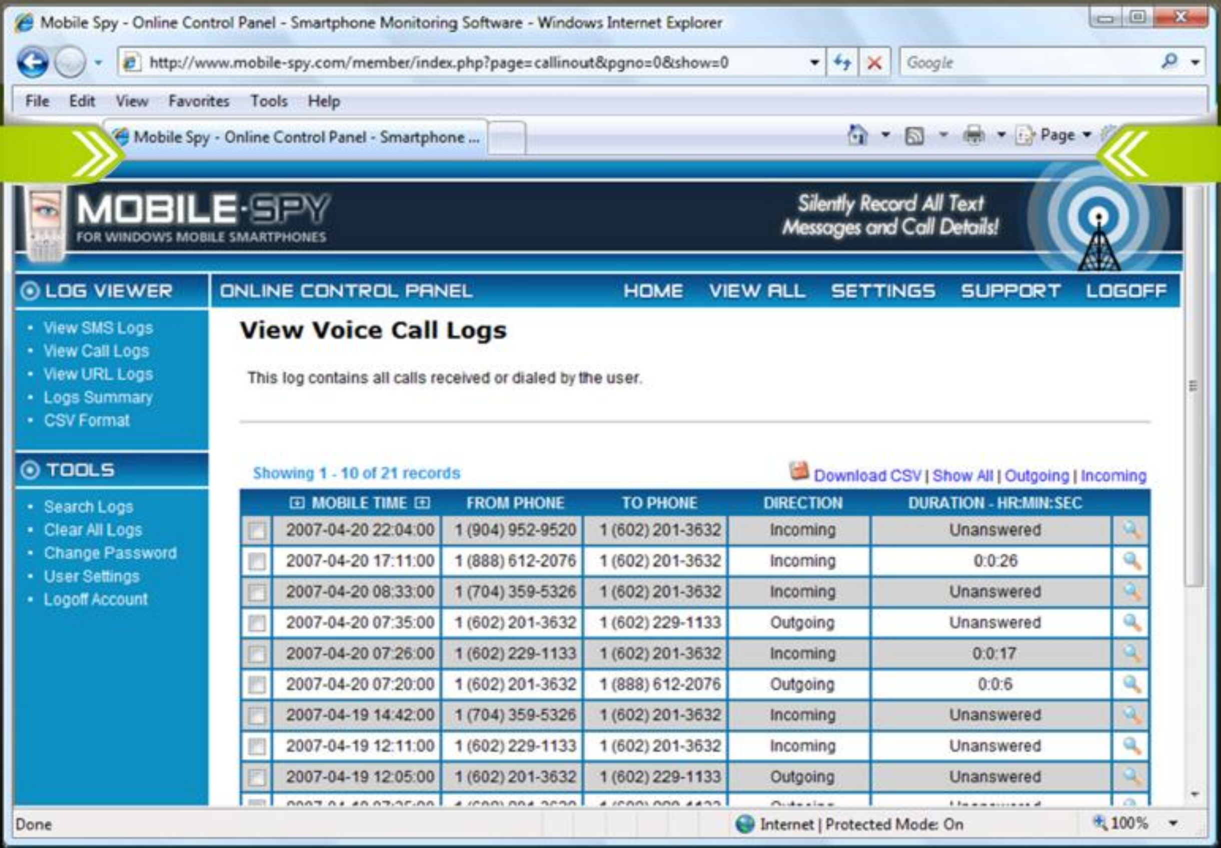
- Spyarsenal Print Monitor
  http://www.spyarsenal.com
- PrintSniffer
  http://www.printsniffer.com
- Accurate Printer Monitor
  http://www.aggsoft.com
- Print Censor
  http://usefulsoft.com
- All-Spy Print
  http://www.all-spy.com
- O&K Print Watch
  http://www.prnwatch.com
- Print Job Monitor
  http://www.imonitorsoft.com
- PrintTrak
  http://www.lygil.com



Telephone/Cellphone Spyware

- Telephone/cellphone spyware **monitors** and **records** phone calls, text messages, and tracks employee cell phone usage
- Attackers install spyware on the devices they want to track. Which **secretly send data to attackers** through SMS or email

Cellphone Spyware: Mobile Spy


Mobile Spy - Online Control Panel - Smartphone Monitoring Software - Windows Internet Explorer
http://www.mobile-spy.com/member/index.php?page=callinout&pgno=0&show=0
File Edit View Favorites Tools Help
Mobile Spy - Online Control Panel - Smartphone ...
MOBILE·SPY
FOR WINDOWS MOBILE SMARTPHONES
Silently Record All Text Messages and Call Details!
LOG VIEWER
ONLINE CONTROL PANEL
HOME
VIEW ALL
SETTINGS
SUPPORT
LOGOFF
View SMS Logs
View Call Logs
View URL Logs
Logs Summary
CSV Format
TOOLS
Search Logs
Clear All Logs
Change Password
User Settings
Logoff Account
Done
Internet | Protected Mode: On
100%

View Voice Call Logs

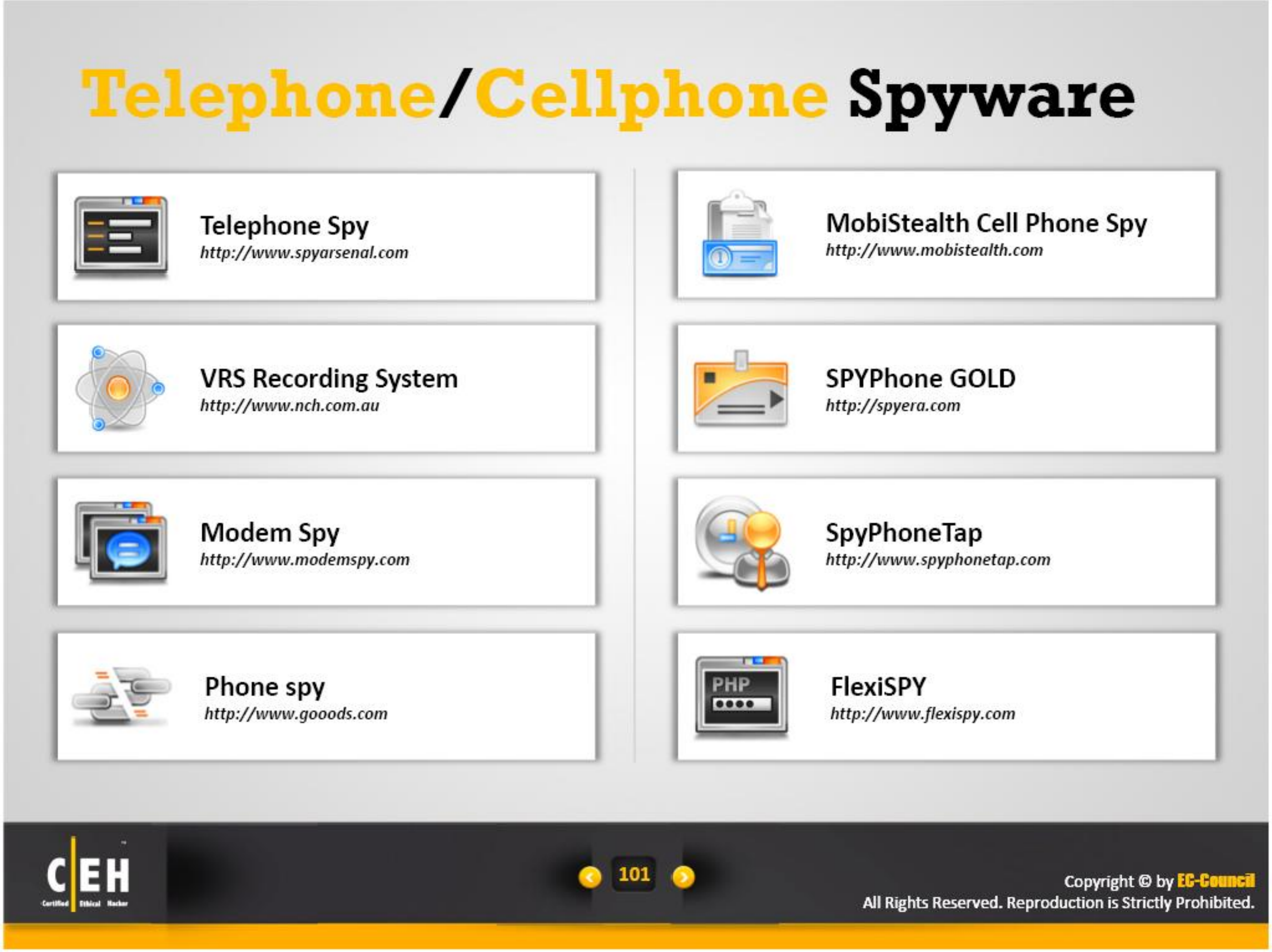
This log contains all calls received or dialed by the user.

Showing 1 - 10 of 21 records

Download CSV | Show All | Outgoing | Incoming

	MOBILE TIME	FROM PHONE	TO PHONE	DIRECTION	DURATION - HR:MIN:SEC	
□	2007-04-20 22:04:00	1 (904) 952-9520	1 (602) 201-3632	Incoming	Unanswered	🔍
□	2007-04-20 17:11:00	1 (888) 612-2076	1 (602) 201-3632	Incoming	0:0:26	🔍
□	2007-04-20 08:33:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered	🔍
□	2007-04-20 07:35:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	Unanswered	🔍
□	2007-04-20 07:26:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	0:0:17	🔍
□	2007-04-20 07:20:00	1 (602) 201-3632	1 (888) 612-2076	Outgoing	0:0:6	🔍
□	2007-04-19 14:42:00	1 (704) 359-5326	1 (602) 201-3632	Incoming	Unanswered	🔍
□	2007-04-19 12:11:00	1 (602) 229-1133	1 (602) 201-3632	Incoming	Unanswered	🔍
□	2007-04-19 12:05:00	1 (602) 201-3632	1 (602) 229-1133	Outgoing	Unanswered	🔍

http://www.phonespysoftware.com



Telephone/Cellphone Spyware

Telephone Spy
http://www.spyarsenal.com

VRS Recording System
http://www.nch.com.au

Modem Spy
http://www.modemspy.com

Phone spy
http://www.gooods.com

MobiStealth Cell Phone Spy
http://www.mobistealth.com

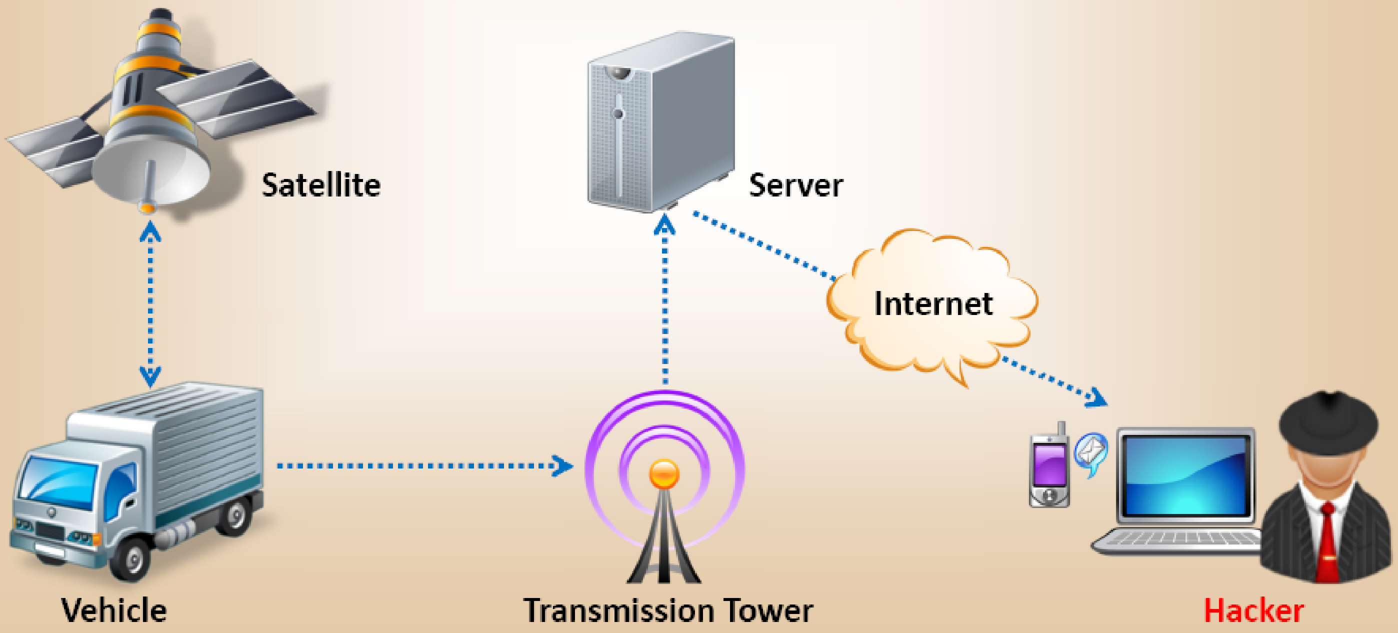
SPYPhone GOLD
http://spyera.com

SpyPhoneTap
http://www.spyphonetap.com

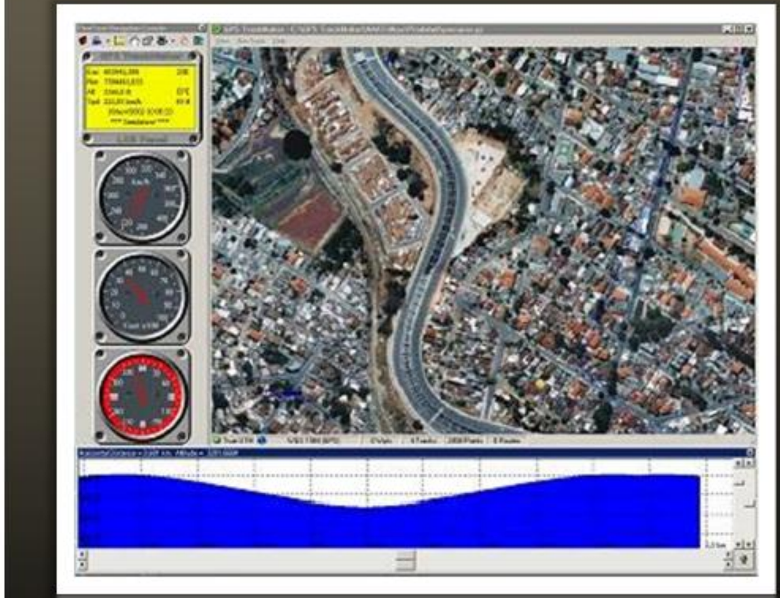
FlexiSPY
http://www.flexispy.com

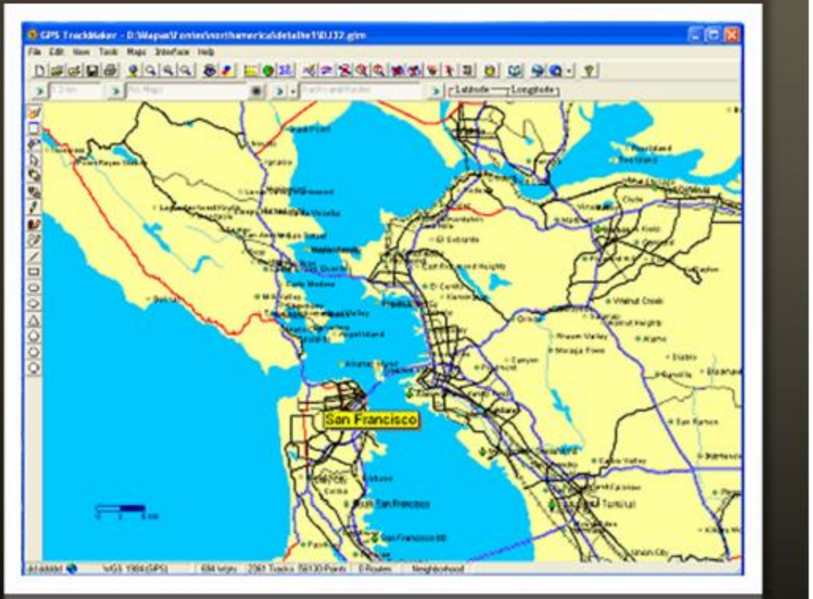
GPS Spyware

GPS spyware is a device or software application that uses the Global Positioning System to determine the location of a vehicle, person, or other asset to which it is attached or installed

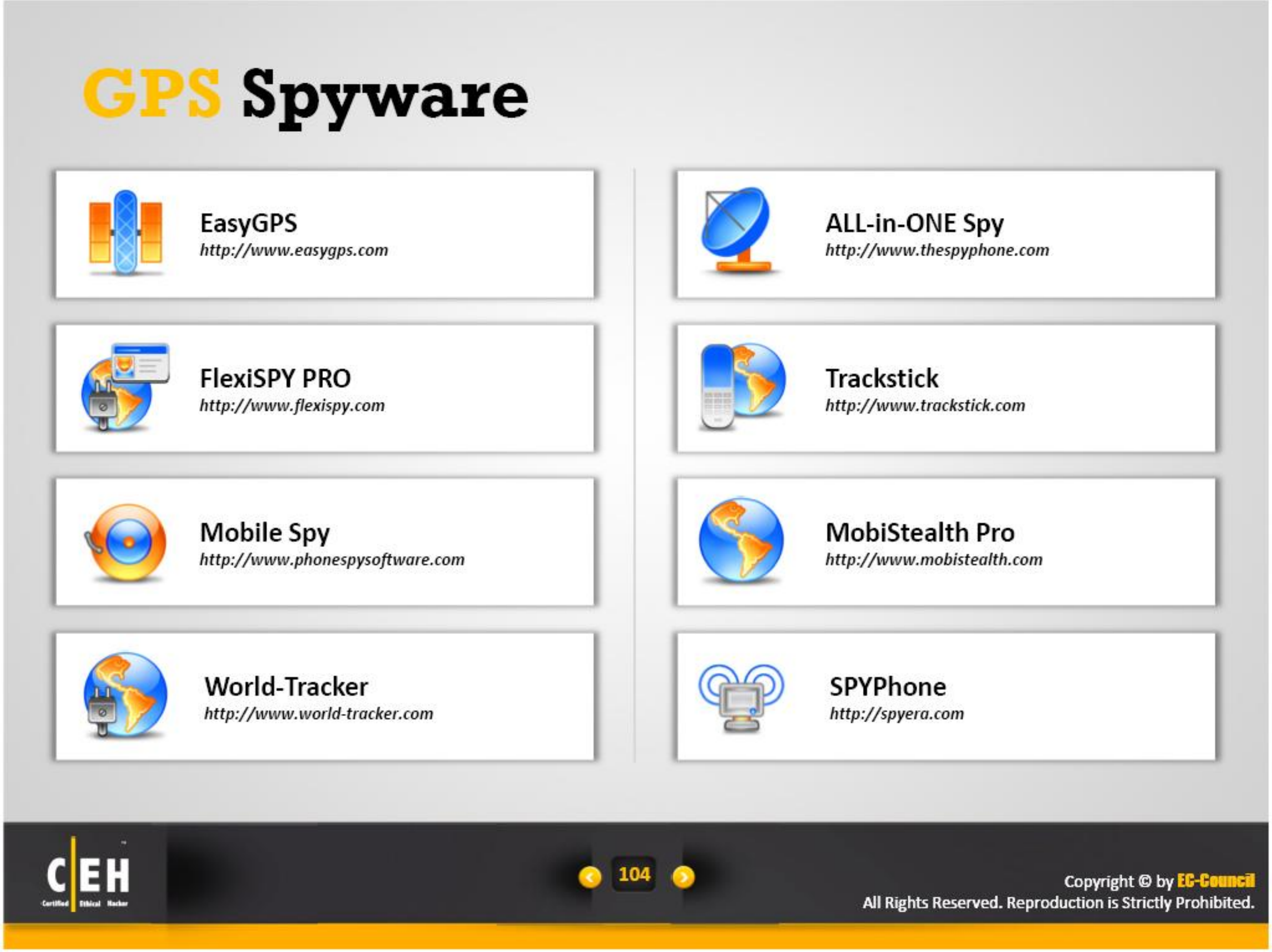


GPS Spyware: GPS TrackMaker





http://www.gpstm.com



GPS Spyware

EasyGPS
http://www.easygps.com

FlexiSPY PRO
http://www.flexispy.com

Mobile Spy
http://www.phonespysoftware.com

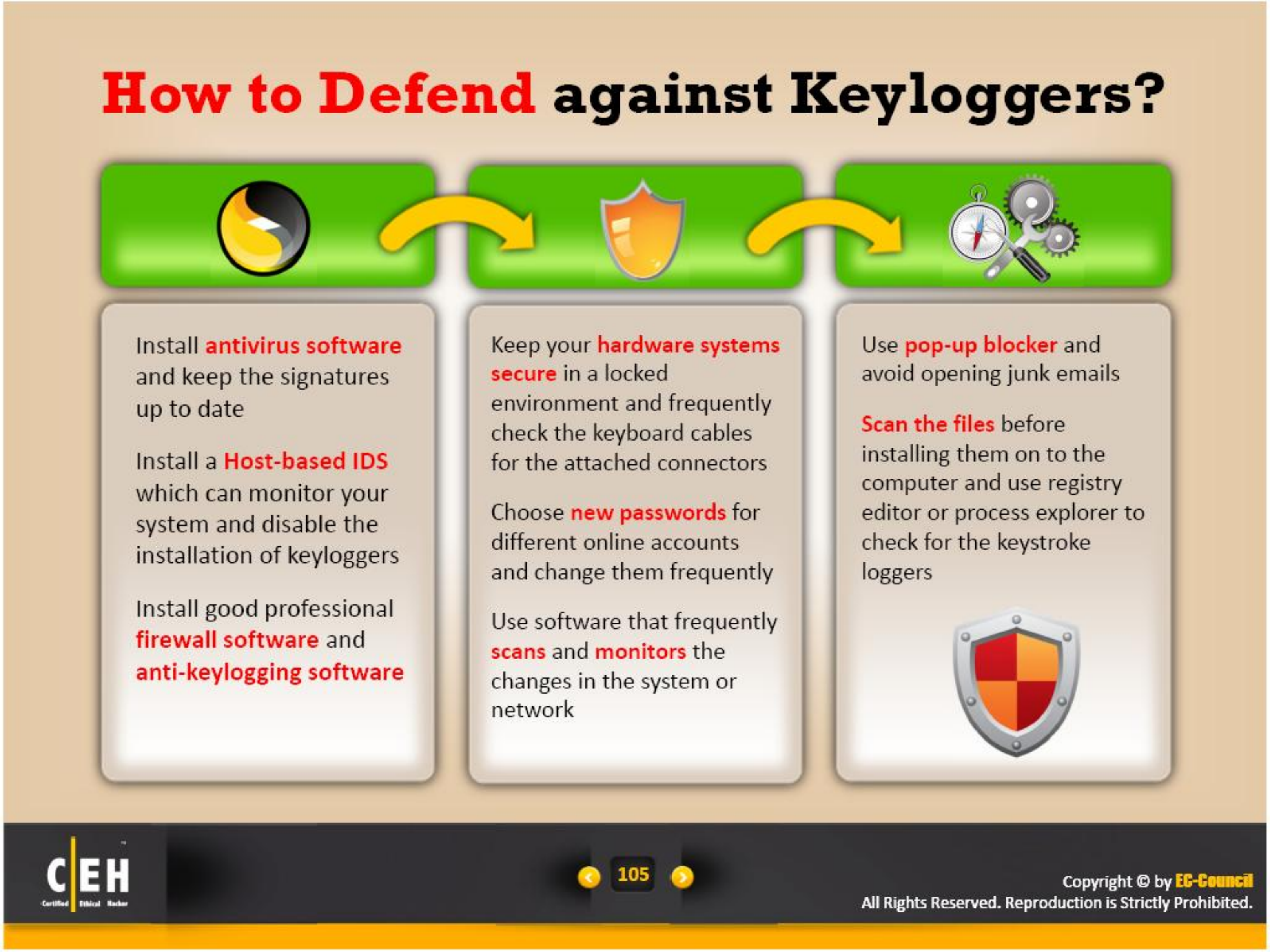
World-Tracker
http://www.world-tracker.com

ALL-in-ONE Spy
http://www.thespyphone.com

Trackstick
http://www.trackstick.com

MobiStealth Pro
http://www.mobistealth.com

SPYPhone
http://spyera.com



How to Defend against Keyloggers?

Install **antivirus software** and keep the signatures up to date

Install a **Host-based IDS** which can monitor your system and disable the installation of keyloggers

Install good professional **firewall software** and **anti-keylogging software**

Keep your **hardware systems secure** in a locked environment and frequently check the keyboard cables for the attached connectors

Choose **new passwords** for different online accounts and change them frequently

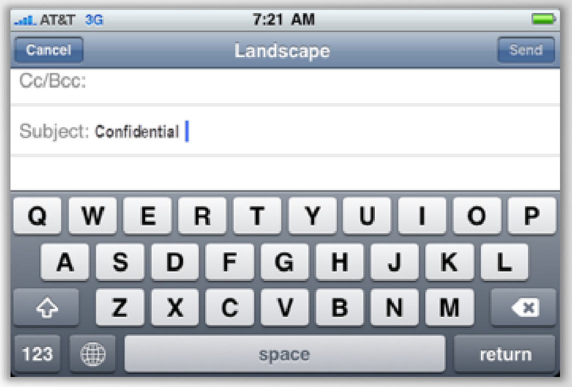
Use software that frequently **scans** and **monitors** the changes in the system or network

Use **pop-up blocker** and avoid opening junk emails

Scan the files before installing them on to the computer and use registry editor or process explorer to check for the keystroke loggers

Anti-Keylogger

- Anti keyloggers detect and disable software keyloggers
- Some of the anti-keyloggers work by matching **signatures of keylogger code** with a signature database while others protect keyboard drivers and kernels from manipulation by keyloggers
- Using a **virtual keyboard** or touch screen makes it difficult for malicious spyware and Trojan programs to capture keystrokes

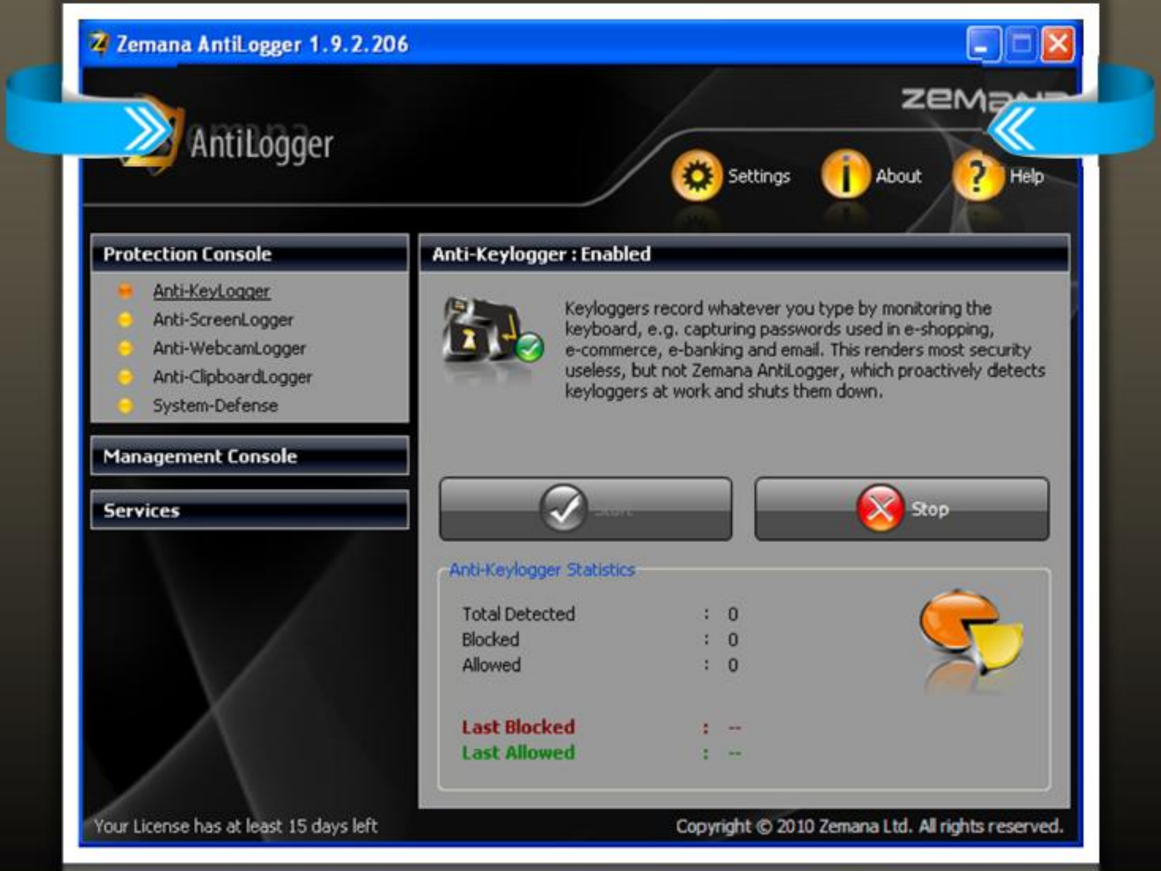


Cc/Bcc:

Subject: Confidential

Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 F13 F14 F15 F16 F17 F18 F19
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Delete
Fn Home Page Up Clear = / *
Tab Q W E R T Y U I O P { [}] | \
Delete End Page Down 7 8 9 –
Caps Lock A S D F G H J K L : ; " ' Enter
4 5 6 +
Shift Z X C V B N M < , > . ? / Shift
1 2 3
Control Alt Option Command Command Alt Option Control
0 . Enter

Anti-Keylogger: Zemana AntiLogger



Zemana AntiLogger 1.9.2.206

Protection Console

- Anti-KeyLogger
- Anti-ScreenLogger
- Anti-WebcamLogger
- Anti-ClipboardLogger
- System-Defense

Management Console

Services

Anti-Keylogger : Enabled

Keyloggers record whatever you type by monitoring the keyboard, e.g. capturing passwords used in e-shopping, e-commerce, e-banking and email. This renders most security useless, but not Zemana AntiLogger, which proactively detects keyloggers at work and shuts them down.

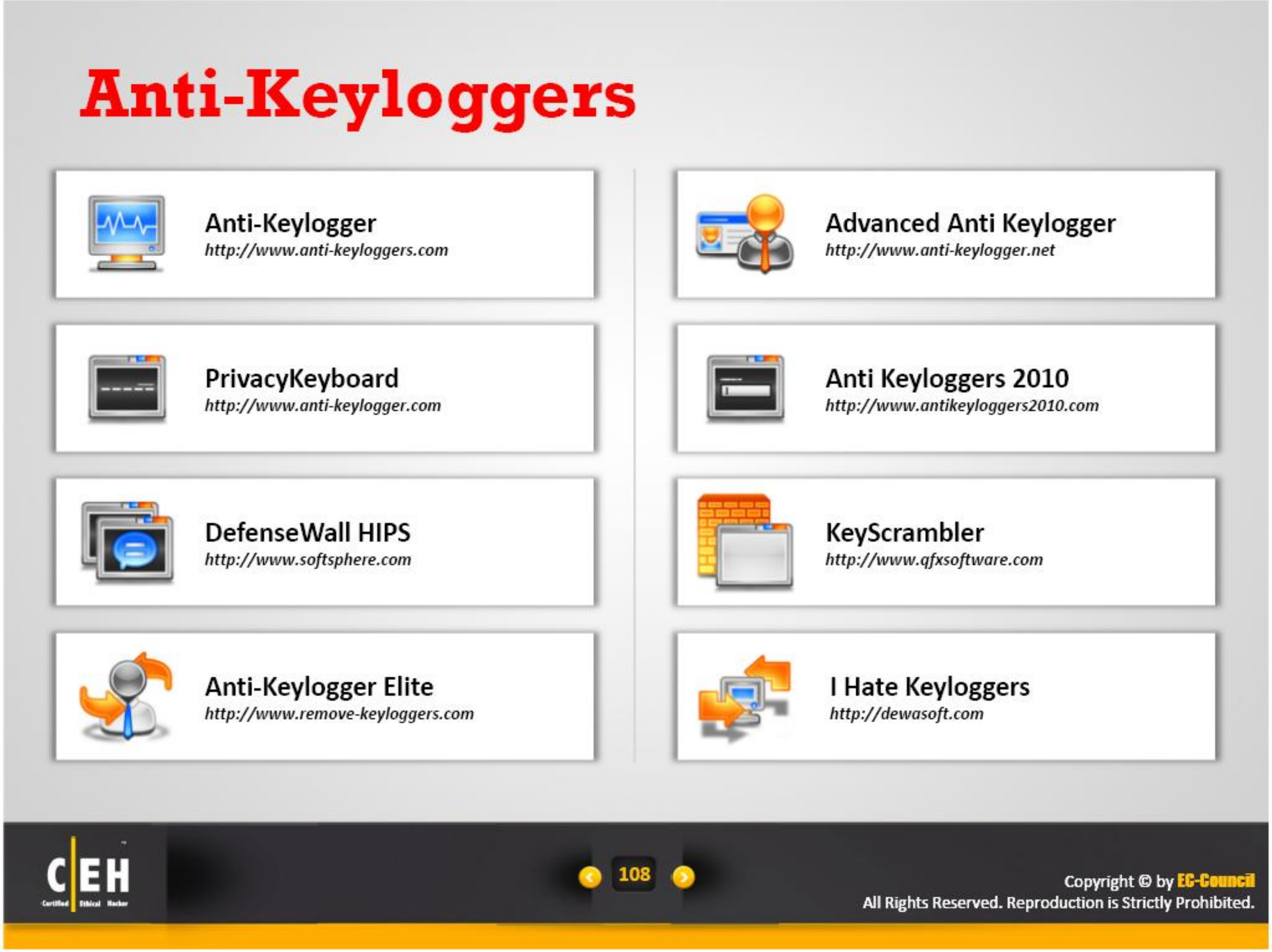
Anti-Keylogger Statistics

Total Detected	:	0
Blocked	:	0
Allowed	:	0
Last Blocked	:	--
Last Allowed	:	--

Your License has at least 15 days left

Copyright © 2010 Zemana Ltd. All rights reserved.

http://www.zemana.com



Anti-Keyloggers

Anti-Keylogger
http://www.anti-keyloggers.com

PrivacyKeyboard
http://www.anti-keylogger.com

DefenseWall HIPS
http://www.softsphere.com

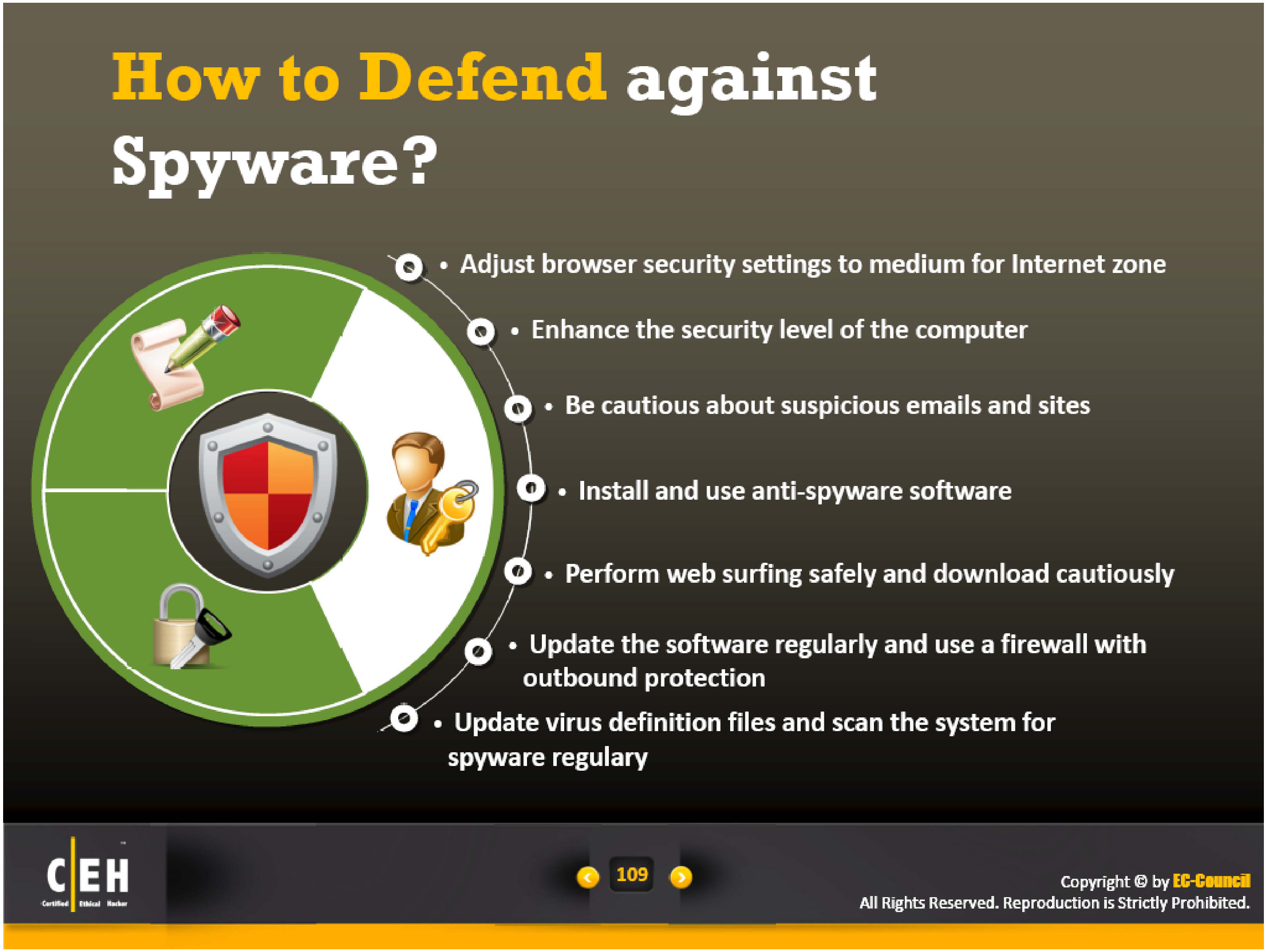
Anti-Keylogger Elite
http://www.remove-keyloggers.com

Advanced Anti Keylogger
http://www.anti-keylogger.net

Anti Keyloggers 2010
http://www.antikeyloggers2010.com

KeyScrambler
http://www.qfxsoftware.com

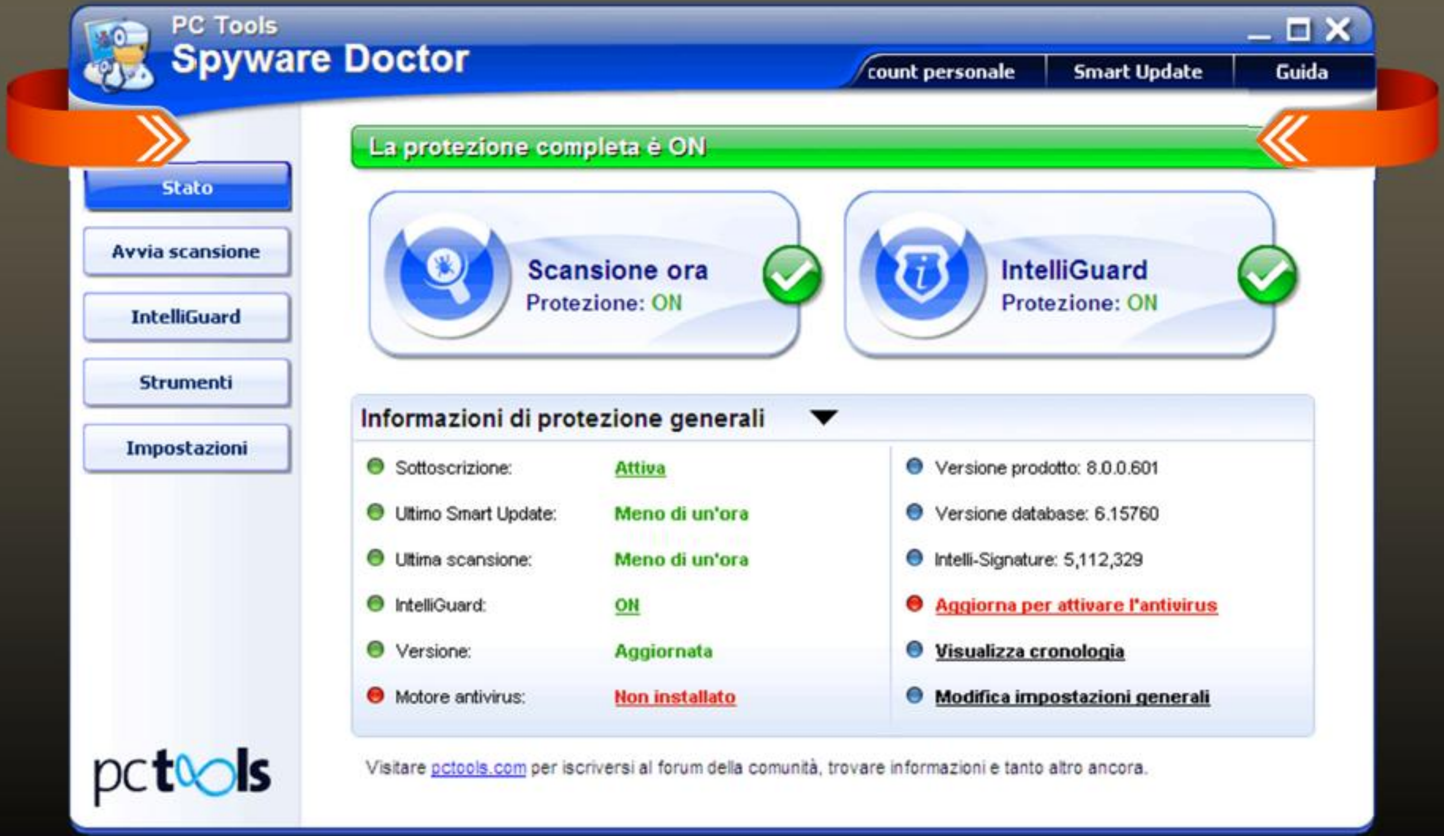
I Hate Keyloggers
http://dewasoft.com



How to Defend against Spyware?

- Adjust browser security settings to medium for Internet zone
- Enhance the security level of the computer
- Be cautious about suspicious emails and sites
- Install and use anti-spyware software
- Perform web surfing safely and download cautiously
- Update the software regularly and use a firewall with outbound protection
- Update virus definition files and scan the system for spyware regulary

Anti-Spyware: Spyware Doctor



La protezione completa è ON

Scansione ora
Protezione: ON

IntelliGuard
Protezione: ON

Informazioni di protezione generali

- Sottoscrizione: Attiva
- Ultimo Smart Update: Meno di un'ora
- Ultima scansione: Meno di un'ora
- IntelliGuard: ON
- Versione: Aggiornata
- Motore antivirus: Non installato

- Versione prodotto: 8.0.0.601
- Versione database: 6.15760
- Intelli-Signature: 5,112,329
- Aggiorna per attivare l'antivirus
- Visualizza cronologia
- Modifica impostazioni generali

Visitare pctools.com per iscriversi al forum della comunità, trovare informazioni e tanto altro ancora.

http://www.pctools.com

Anti-Spywares

CounterSpy
http://www.sunbeltsoftware.com

Norton Internet Security 2011
http://www.symantec.com

SpyHunter
http://www.enigmasoftware.com

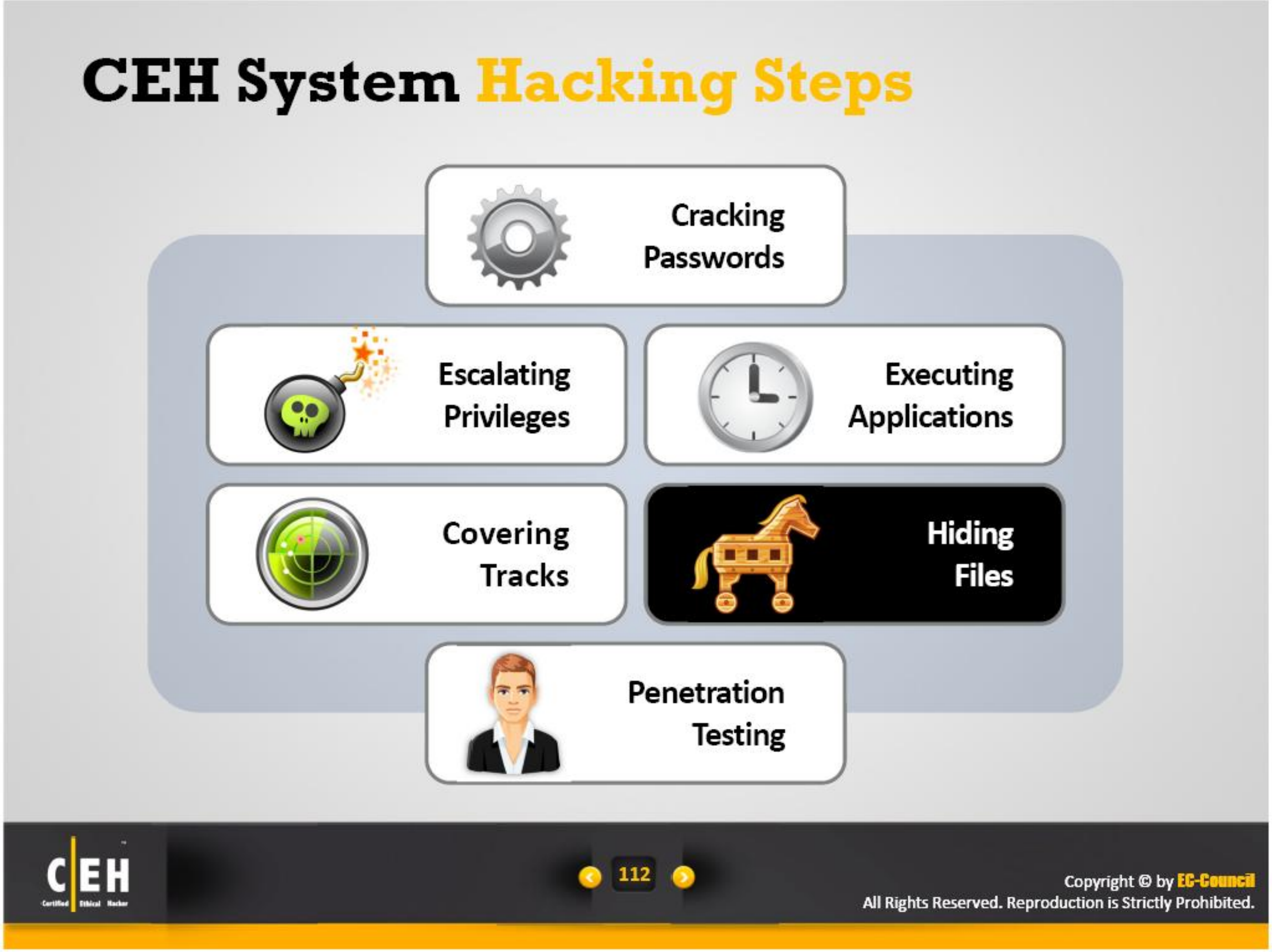
Spyware Terminator
http://www.spywareterminator.com

Kaspersky Internet Security 2011
http://www.kaspersky.com

Ad-Aware
http://www.lavasoft.com

Spy Sweeper
http://www.webroot.com

MacScan (for MAC OS X)
http://macscan.securemac.com



CEH System Hacking Steps

Cracking Passwords

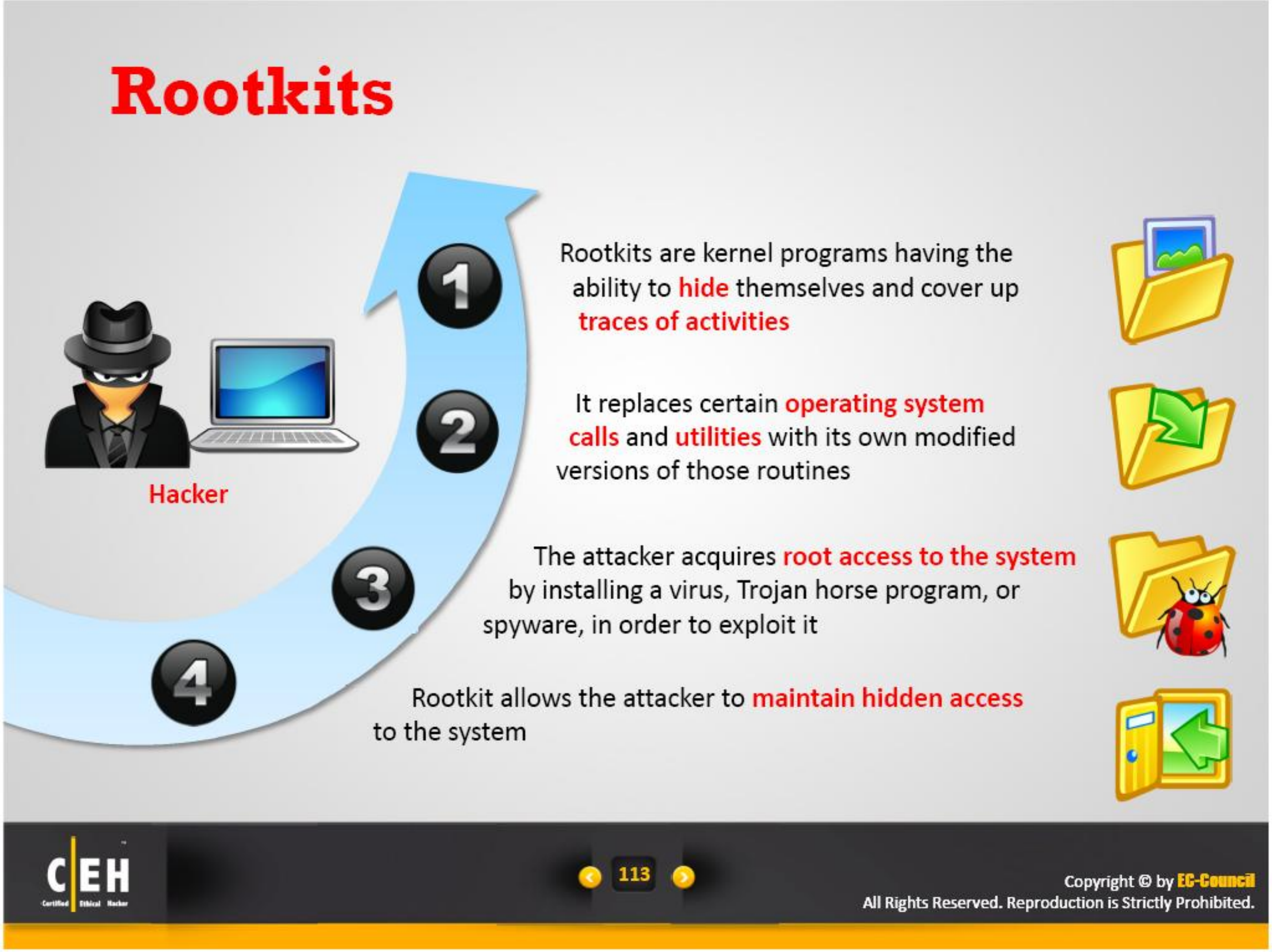
Escalating Privileges

Executing Applications

Covering Tracks

Hiding Files

Penetration Testing



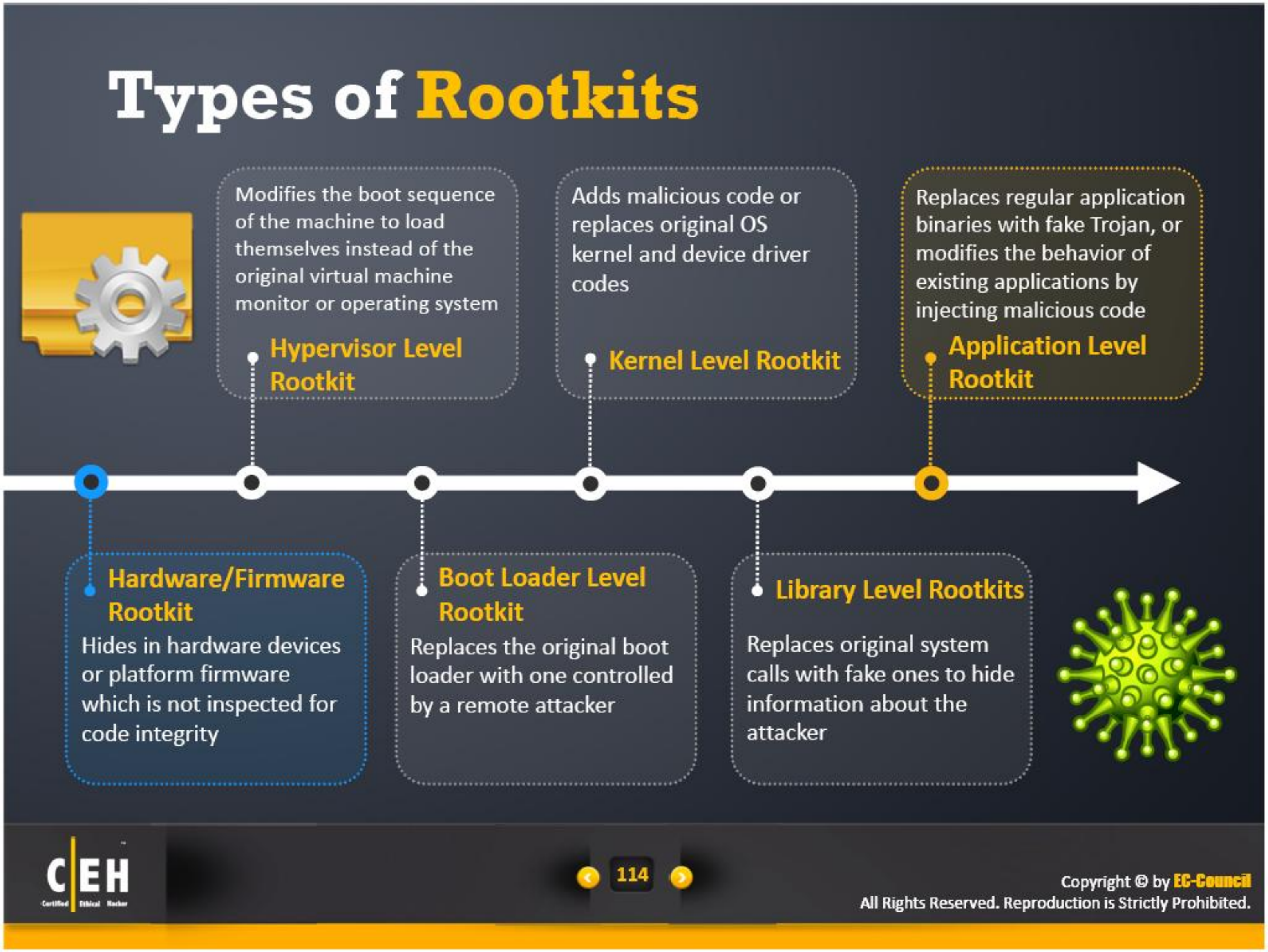
Rootkits

1. Rootkits are kernel programs having the ability to **hide** themselves and cover up **traces of activities**

2. It replaces certain **operating system calls** and **utilities** with its own modified versions of those routines

3. The attacker acquires **root access to the system** by installing a virus, Trojan horse program, or spyware, in order to exploit it

4. Rootkit allows the attacker to **maintain hidden access** to the system



Types of Rootkits

Hardware/Firmware Rootkit

Hides in hardware devices or platform firmware which is not inspected for code integrity

Hypervisor Level Rootkit

Modifies the boot sequence of the machine to load themselves instead of the original virtual machine monitor or operating system

Boot Loader Level Rootkit

Replaces the original boot loader with one controlled by a remote attacker

Kernel Level Rootkit

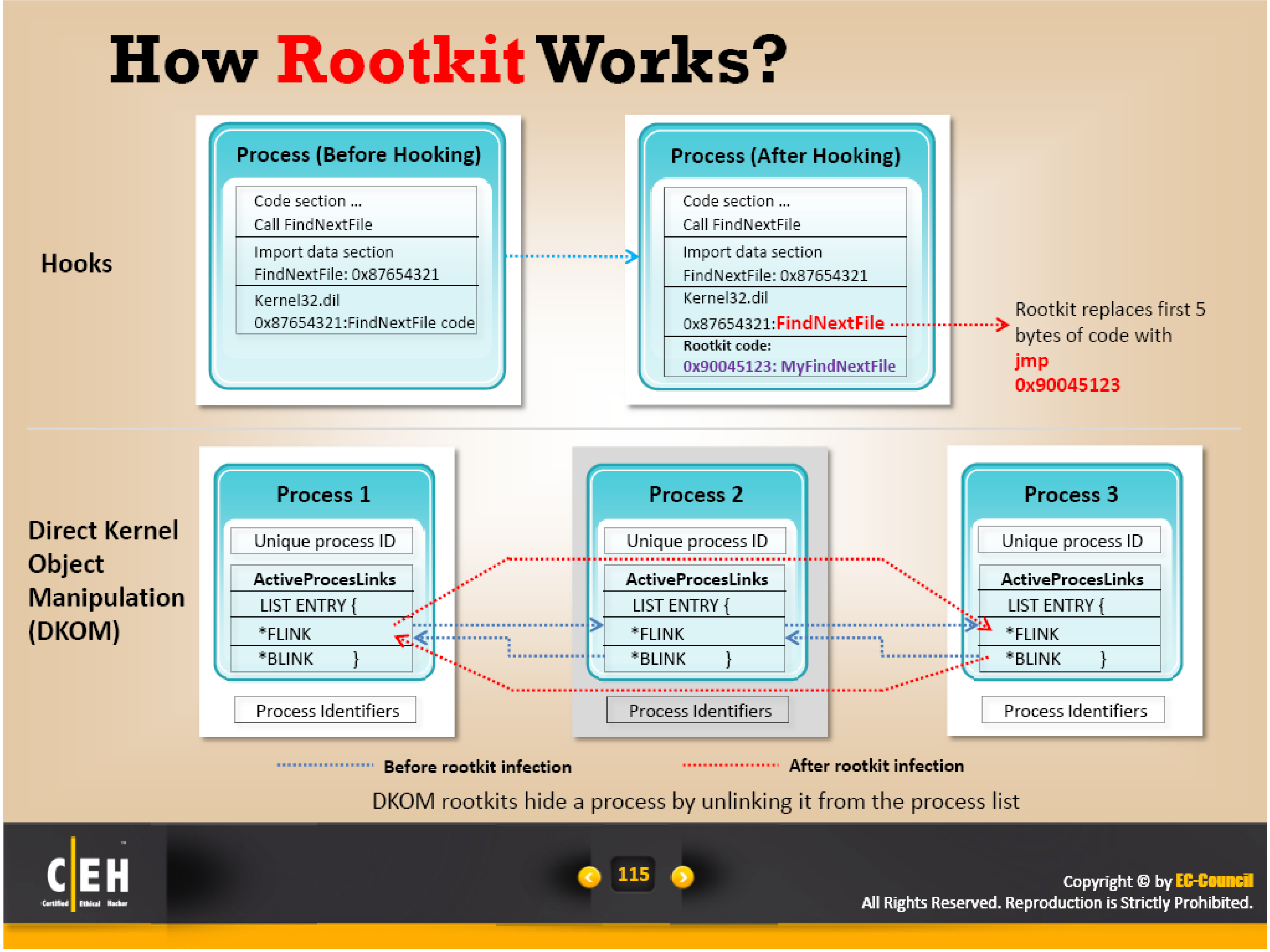
Adds malicious code or replaces original OS kernel and device driver codes

Library Level Rootkits

Replaces original system calls with fake ones to hide information about the attacker

Application Level Rootkit

Replaces regular application binaries with fake Trojan, or modifies the behavior of existing applications by injecting malicious code



How Rootkit Works?

Hooks

Process (Before Hooking)

Code section ...
Call FindNextFile

Import data section
FindNextFile: 0x87654321

Kernel32.dil
0x87654321:FindNextFile code

Process (After Hooking)

Code section ...
Call FindNextFile

Import data section
FindNextFile: 0x87654321

Kernel32.dil
0x87654321:FindNextFile

Rootkit code:
0x90045123: MyFindNextFile

Rootkit replaces first 5 bytes of code with **jmp 0x90045123**

Direct Kernel Object Manipulation (DKOM)

Process 1

Unique process ID

ActiveProcesLinks
LIST ENTRY {
*FLINK
*BLINK }

Process Identifiers

Process 2

Unique process ID

ActiveProcesLinks
LIST ENTRY {
*FLINK
*BLINK }

Process Identifiers

Process 3

Unique process ID

ActiveProcesLinks
LIST ENTRY {
*FLINK
*BLINK }

Process Identifiers

Before rootkit infection

After rootkit infection

DKOM rootkits hide a process by unlinking it from the process list

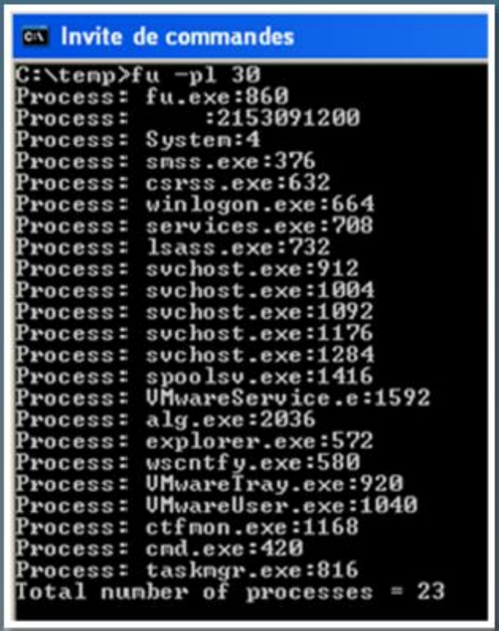
Rootkit: Fu

Fu operates using direct Kernel object manipulation

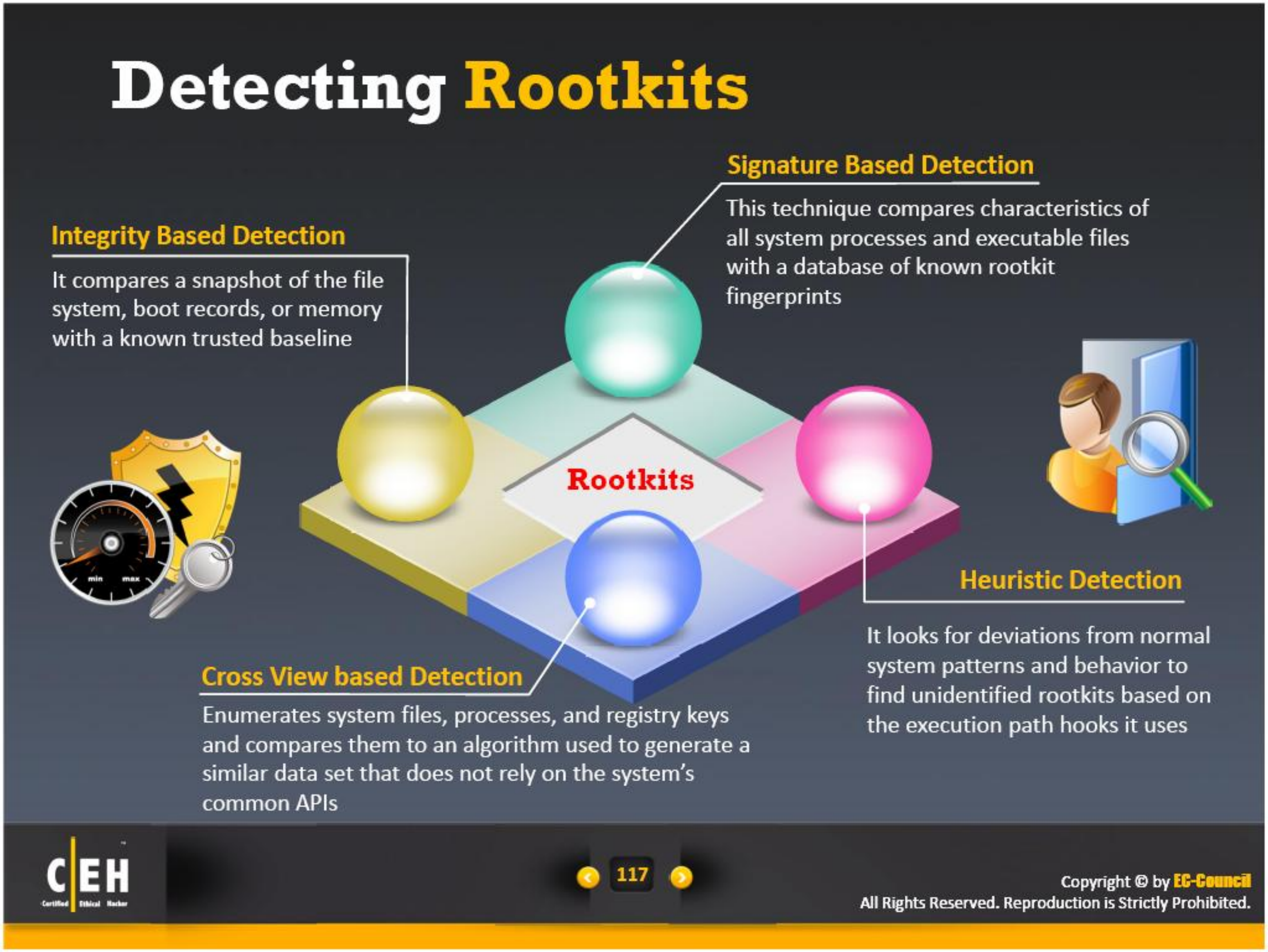
Components of Fu are dropper (fu.exe) and driver (msdirectx.sys)

It allows attacker to:

- Hide processes and drivers
- Hide information from user-mode applications and even from kernel-mode modules
- Add privileges to any process token
- Remove to-be-hidden entries from two linked lists with symbolic names



```
C:\temp>fu -pl 30
Process: fu.exe:860
Process:      :2153091200
Process: System:4
Process: smss.exe:376
Process: csrss.exe:632
Process: winlogon.exe:664
Process: services.exe:708
Process: lsass.exe:732
Process: svchost.exe:912
Process: svchost.exe:1004
Process: svchost.exe:1092
Process: svchost.exe:1176
Process: svchost.exe:1284
Process: spoolsv.exe:1416
Process: VMwareService.e:1592
Process: alg.exe:2036
Process: explorer.exe:572
Process: wscntfy.exe:580
Process: VMwareTray.exe:920
Process: VMwareUser.exe:1040
Process: ctfmon.exe:1168
Process: cmd.exe:420
Process: taskmgr.exe:816
Total number of processes = 23
```



Detecting Rootkits

Rootkits

Integrity Based Detection

It compares a snapshot of the file system, boot records, or memory with a known trusted baseline

Signature Based Detection

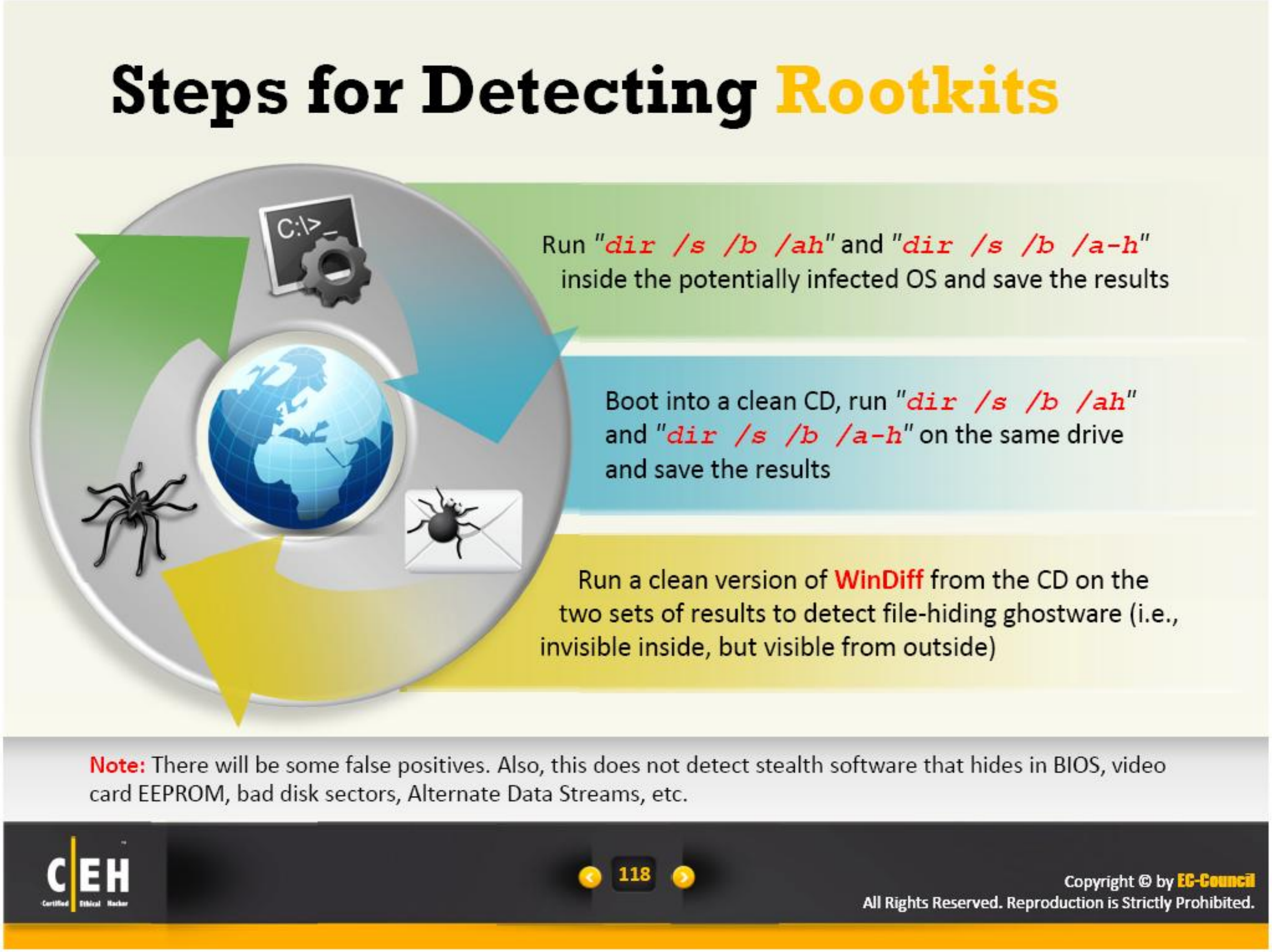
This technique compares characteristics of all system processes and executable files with a database of known rootkit fingerprints

Heuristic Detection

It looks for deviations from normal system patterns and behavior to find unidentified rootkits based on the execution path hooks it uses

Cross View based Detection

Enumerates system files, processes, and registry keys and compares them to an algorithm used to generate a similar data set that does not rely on the system's common APIs



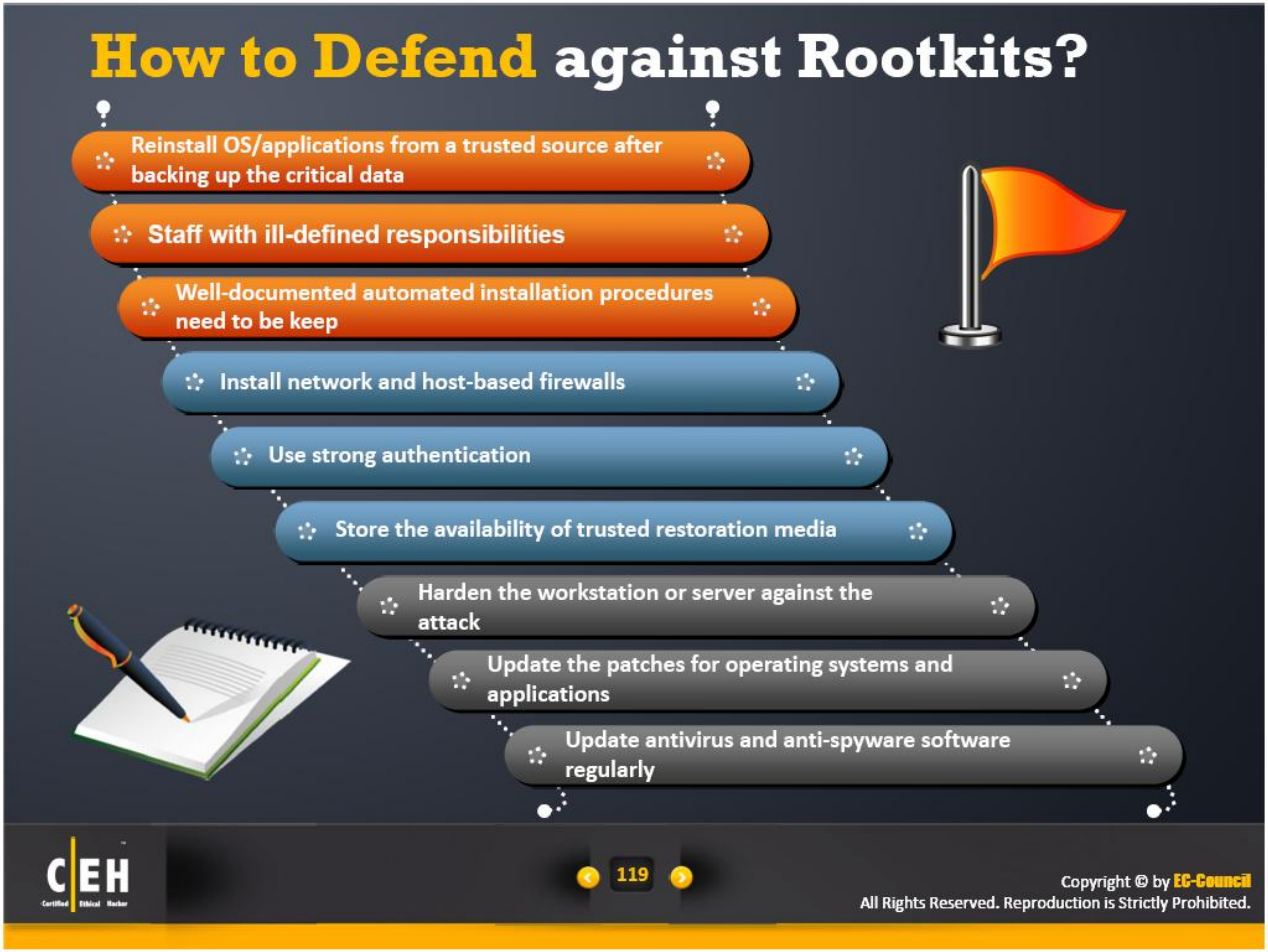
Steps for Detecting Rootkits

Run "`dir /s /b /ah`" and "`dir /s /b /a-h`" inside the potentially infected OS and save the results

Boot into a clean CD, run "`dir /s /b /ah`" and "`dir /s /b /a-h`" on the same drive and save the results

Run a clean version of **WinDiff** from the CD on the two sets of results to detect file-hiding ghostware (i.e., invisible inside, but visible from outside)

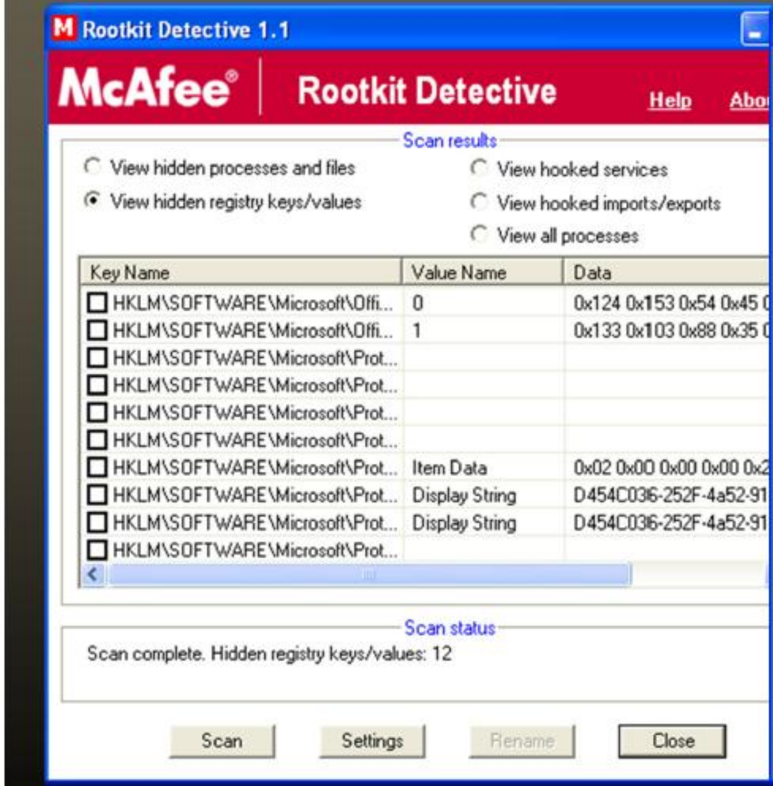
Note: There will be some false positives. Also, this does not detect stealth software that hides in BIOS, video card EEPROM, bad disk sectors, Alternate Data Streams, etc.



How to Defend against Rootkits?

- Reinstall OS/applications from a trusted source after backing up the critical data
- Staff with ill-defined responsibilities
- Well-documented automated installation procedures need to be keep
- Install network and host-based firewalls
- Use strong authentication
- Store the availability of trusted restoration media
- Harden the workstation or server against the attack
- Update the patches for operating systems and applications
- Update antivirus and anti-spyware software regularly

Anti-Rootkit: RootkitRevealer and McAfee Rootkit Detective



Rootkit Detective 1.1

McAfee® Rootkit Detective Help Abo

Scan results

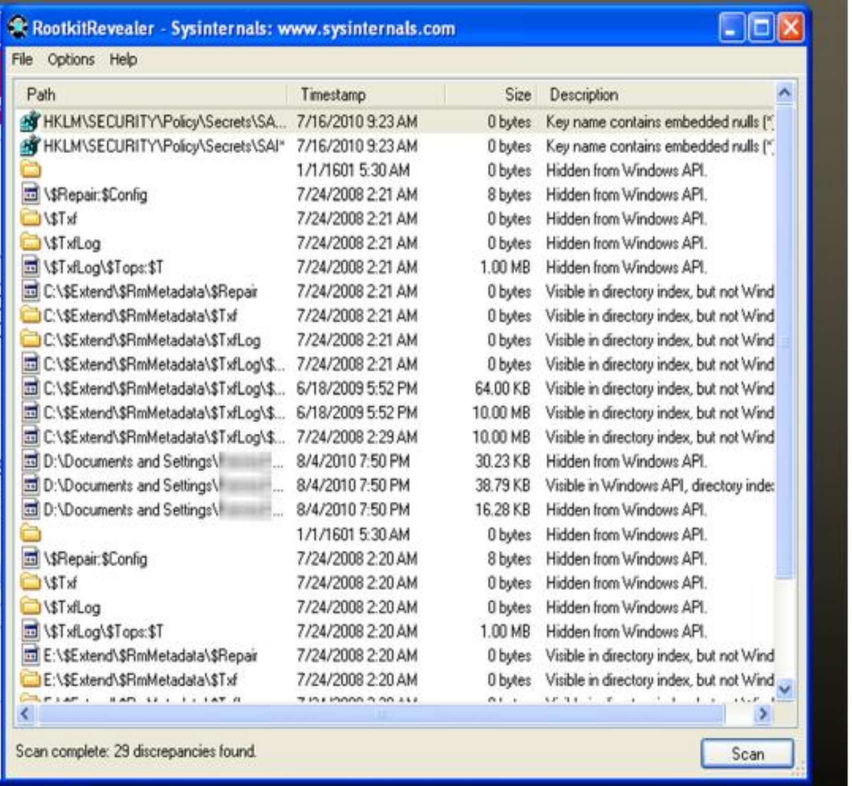
○ View hidden processes and files ○ View hooked services
● View hidden registry keys/values ○ View hooked imports/exports
○ View all processes

Key Name	Value Name	Data
□ HKLM\SOFTWARE\Microsoft\Offi...	0	0x124 0x153 0x54 0x45 0
□ HKLM\SOFTWARE\Microsoft\Offi...	1	0x133 0x103 0x88 0x35 0
□ HKLM\SOFTWARE\Microsoft\Prot...		
□ HKLM\SOFTWARE\Microsoft\Prot...		
□ HKLM\SOFTWARE\Microsoft\Prot...		
□ HKLM\SOFTWARE\Microsoft\Prot...		
□ HKLM\SOFTWARE\Microsoft\Prot...	Item Data	0x02 0x00 0x00 0x00 0x2
□ HKLM\SOFTWARE\Microsoft\Prot...	Display String	D454C036-252F-4a52-91
□ HKLM\SOFTWARE\Microsoft\Prot...	Display String	D454C036-252F-4a52-91
□ HKLM\SOFTWARE\Microsoft\Prot...		

Scan status

Scan complete. Hidden registry keys/values: 12

http://vil.nai.com

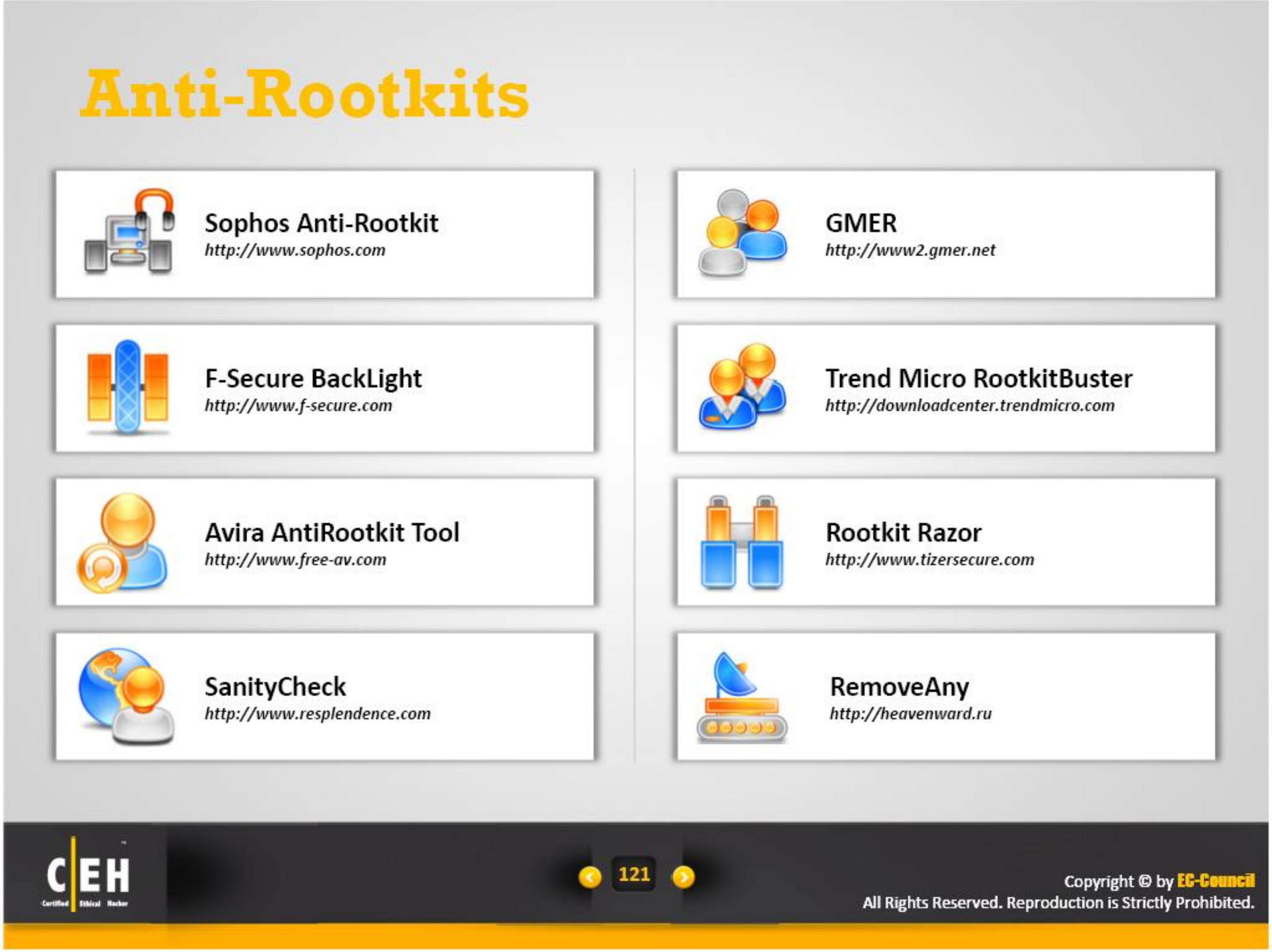


RootkitRevealer - Sysinternals: www.sysinternals.com

Path	Timestamp	Size	Description
HKLM\SECURITY\Policy\Secrets\SA...	7/16/2010 9:23 AM	0 bytes	Key name contains embedded nulls (*
HKLM\SECURITY\Policy\Secrets\SAI*	7/16/2010 9:23 AM	0 bytes	Key name contains embedded nulls (*
	1/1/1601 5:30 AM	0 bytes	Hidden from Windows API.
\$Repair:$Config	7/24/2008 2:21 AM	8 bytes	Hidden from Windows API.
\$Txf	7/24/2008 2:21 AM	0 bytes	Hidden from Windows API.
\$TxfLog	7/24/2008 2:21 AM	0 bytes	Hidden from Windows API.
\$TxfLog\$Tops:$T	7/24/2008 2:21 AM	1.00 MB	Hidden from Windows API.
C:\$Extend\$RmMetadata\$Repair	7/24/2008 2:21 AM	0 bytes	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$Txf	7/24/2008 2:21 AM	0 bytes	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$TxfLog	7/24/2008 2:21 AM	0 bytes	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$TxfLog\$...	7/24/2008 2:21 AM	0 bytes	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$TxfLog\$...	6/18/2009 5:52 PM	64.00 KB	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$TxfLog\$...	6/18/2009 5:52 PM	10.00 MB	Visible in directory index, but not Wind
C:\$Extend\$RmMetadata\$TxfLog\$...	7/24/2008 2:29 AM	10.00 MB	Visible in directory index, but not Wind
D:\Documents and Settings\[redacted]...	8/4/2010 7:50 PM	30.23 KB	Hidden from Windows API.
D:\Documents and Settings\[redacted]...	8/4/2010 7:50 PM	38.79 KB	Visible in Windows API, directory inde:
D:\Documents and Settings\[redacted]...	8/4/2010 7:50 PM	16.28 KB	Hidden from Windows API.
	1/1/1601 5:30 AM	0 bytes	Hidden from Windows API.
\$Repair:$Config	7/24/2008 2:20 AM	8 bytes	Hidden from Windows API.
\$Txf	7/24/2008 2:20 AM	0 bytes	Hidden from Windows API.
\$TxfLog	7/24/2008 2:20 AM	0 bytes	Hidden from Windows API.
\$TxfLog\$Tops:$T	7/24/2008 2:20 AM	1.00 MB	Hidden from Windows API.
E:\$Extend\$RmMetadata\$Repair	7/24/2008 2:20 AM	0 bytes	Visible in directory index, but not Wind
E:\$Extend\$RmMetadata\$Txf	7/24/2008 2:20 AM	0 bytes	Visible in directory index, but not Wind

Scan complete: 29 discrepancies found.

http://technet.microsoft.com

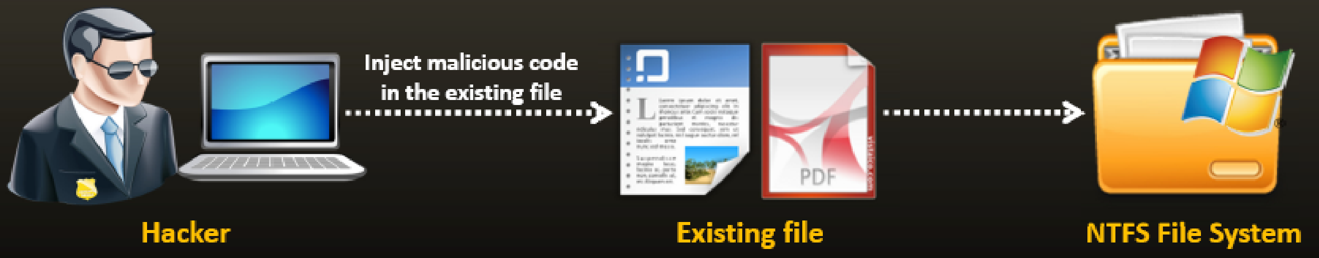


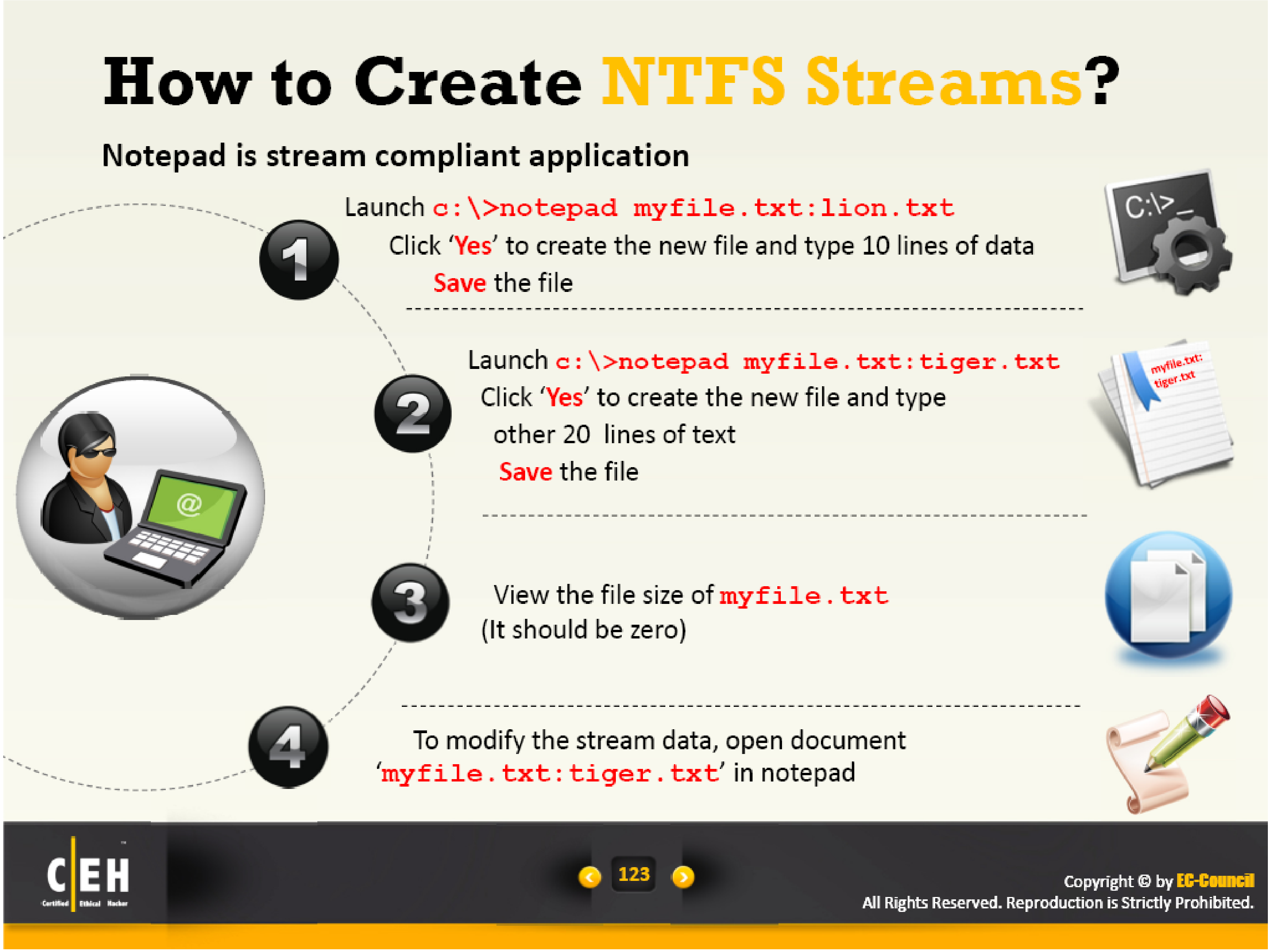
Anti-Rootkits

- **Sophos Anti-Rootkit**
  http://www.sophos.com
- **F-Secure BackLight**
  http://www.f-secure.com
- **Avira AntiRootkit Tool**
  http://www.free-av.com
- **SanityCheck**
  http://www.resplendence.com
- **GMER**
  http://www2.gmer.net
- **Trend Micro RootkitBuster**
  http://downloadcenter.trendmicro.com
- **Rootkit Razor**
  http://www.tizersecure.com
- **RemoveAny**
  http://heavenward.ru

NTFS Data Stream

- NTFS Alternate Data Stream (ADS) is a **Windows hidden stream** which contains metadata for the file such as attributes, word count, author name, and access and modification time of the files
- ADS is the ability to **fork data into existing files** without changing or altering their functionality, size, or display to file browsing utilities
- ADS allows an attacker to **inject malicious code** on a breached system and executes them without being detected by the user





How to Create NTFS Streams?

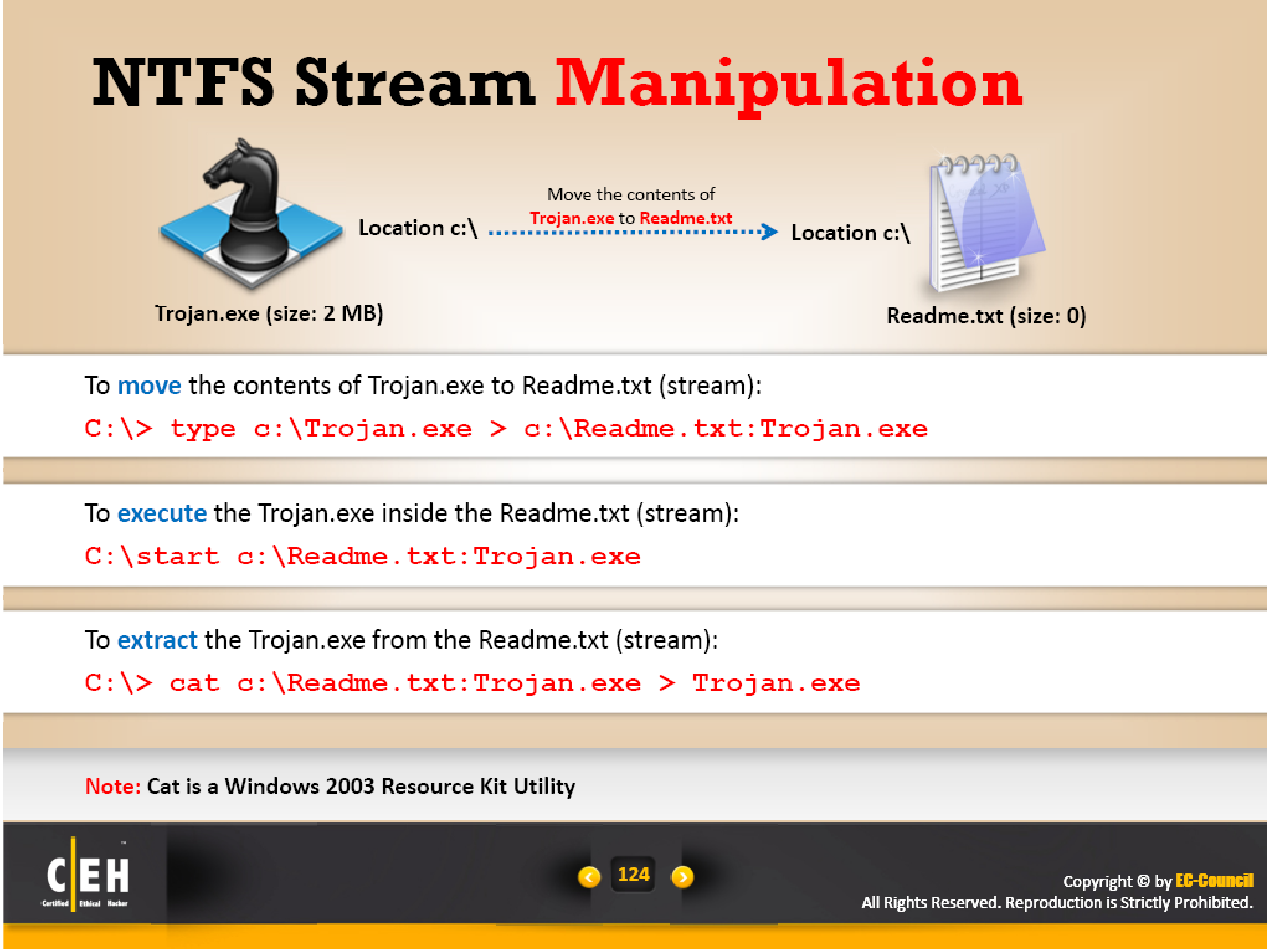
Notepad is stream compliant application

1. Launch `c:\>notepad myfile.txt:lion.txt`
   Click 'Yes' to create the new file and type 10 lines of data
   Save the file

2. Launch `c:\>notepad myfile.txt:tiger.txt`
   Click 'Yes' to create the new file and type other 20 lines of text
   Save the file

3. View the file size of `myfile.txt`
   (It should be zero)

4. To modify the stream data, open document '`myfile.txt:tiger.txt`' in notepad



NTFS Stream Manipulation

Move the contents of
Trojan.exe to Readme.txt
Location c:\
Location c:\
Trojan.exe (size: 2 MB)
Readme.txt (size: 0)

To move the contents of Trojan.exe to Readme.txt (stream):

```
C:\> type c:\Trojan.exe > c:\Readme.txt:Trojan.exe
```

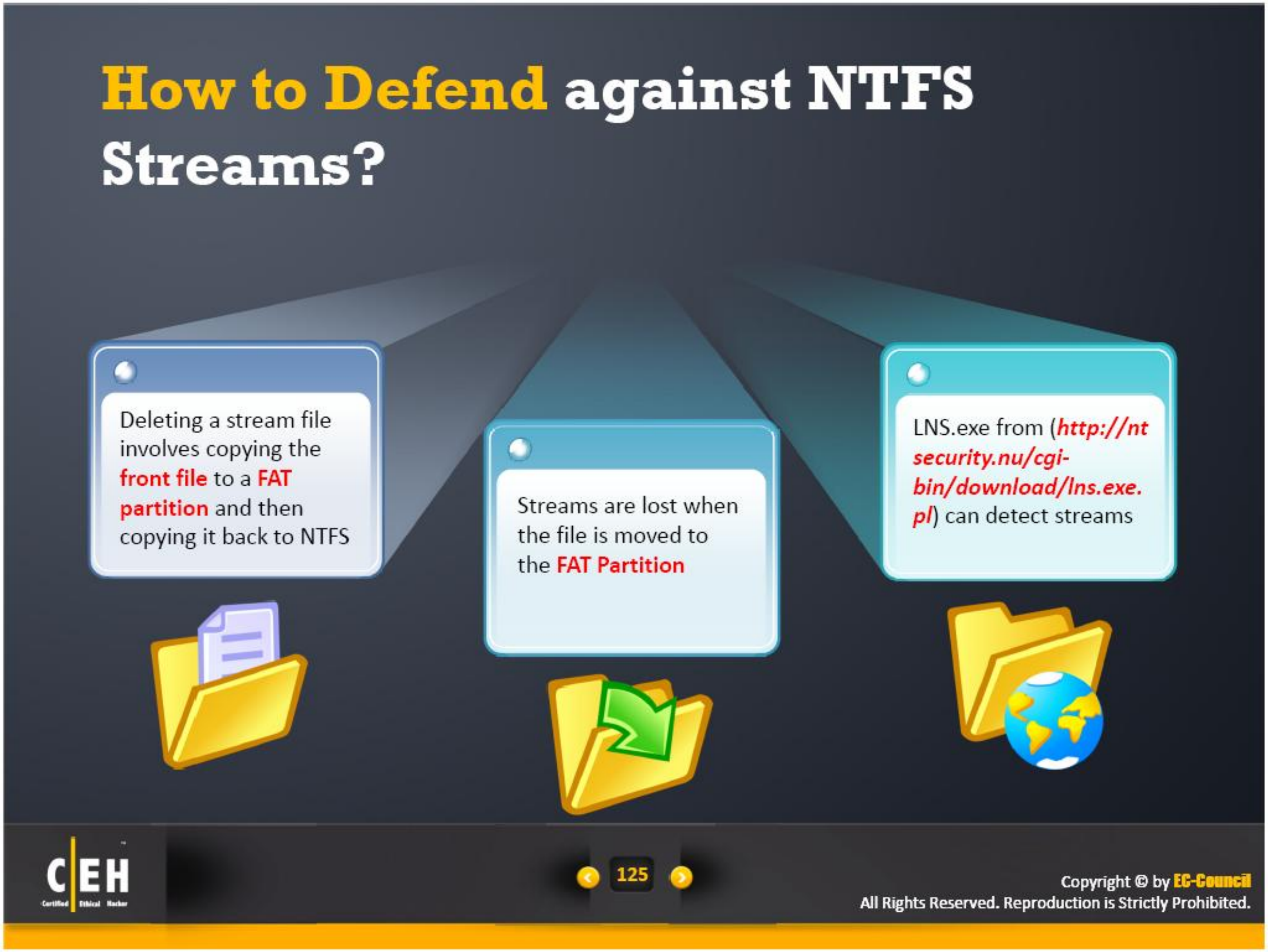
To execute the Trojan.exe inside the Readme.txt (stream):

```
C:\start c:\Readme.txt:Trojan.exe
```

To extract the Trojan.exe from the Readme.txt (stream):

```
C:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe
```

Note: Cat is a Windows 2003 Resource Kit Utility



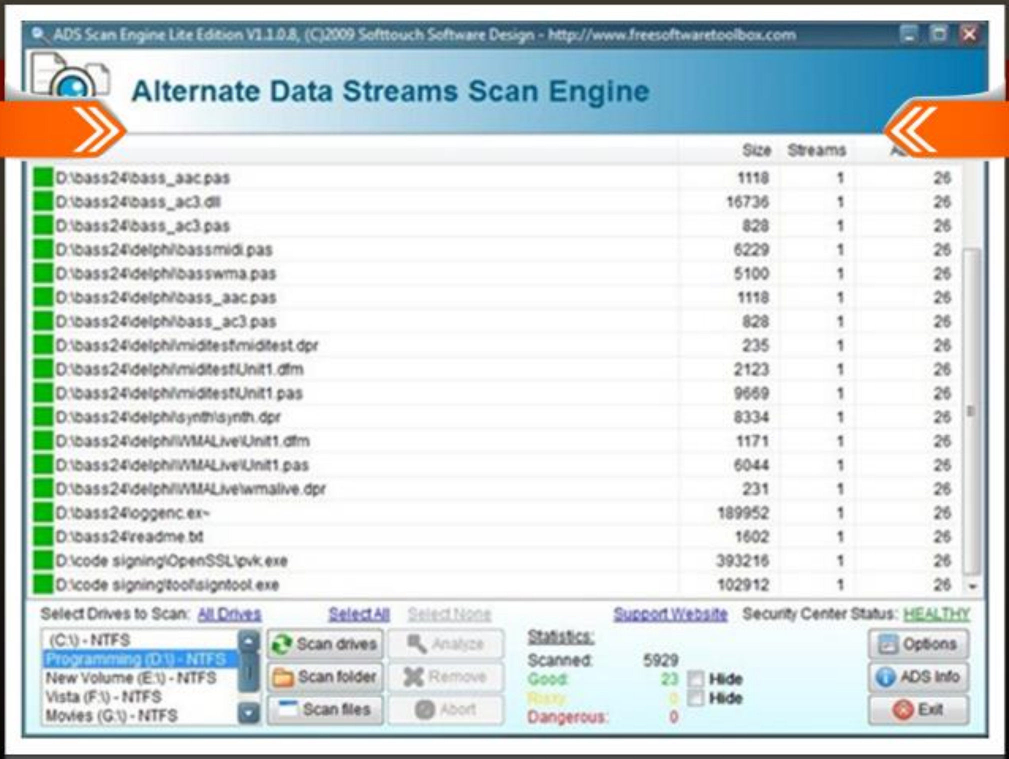
How to Defend against NTFS Streams?

Deleting a stream file involves copying the **front file** to a **FAT partition** and then copying it back to NTFS

Streams are lost when the file is moved to the **FAT Partition**

LNS.exe from (***http://ntsecurity.nu/cgi-bin/download/lns.exe.pl***) can detect streams

NTFS Stream Detector: ADS Scan Engine



ADS Scan Engine Lite Edition V1.1.0.8, (C)2009 Softtouch Software Design - http://www.freesoftwaretoolbox.com

Alternate Data Streams Scan Engine

	Size	Streams	A
🟩 D:\bass24\bass_aac.pas	1118	1	26
🟩 D:\bass24\bass_ac3.dll	16736	1	26
🟩 D:\bass24\bass_ac3.pas	828	1	26
🟩 D:\bass24\delphi\bassmidi.pas	6229	1	26
🟩 D:\bass24\delphi\basswma.pas	5100	1	26
🟩 D:\bass24\delphi\bass_aac.pas	1118	1	26
🟩 D:\bass24\delphi\bass_ac3.pas	828	1	26
🟩 D:\bass24\delphi\miditest\miditest.dpr	235	1	26
🟩 D:\bass24\delphi\miditest\Unit1.dfm	2123	1	26
🟩 D:\bass24\delphi\miditest\Unit1.pas	9669	1	26
🟩 D:\bass24\delphi\synth\synth.dpr	8334	1	26
🟩 D:\bass24\delphi\WMALive\Unit1.dfm	1171	1	26
🟩 D:\bass24\delphi\WMALive\Unit1.pas	6044	1	26
🟩 D:\bass24\delphi\WMALive\wmalive.dpr	231	1	26
🟩 D:\bass24\oggenc.ex~	189952	1	26
🟩 D:\bass24\readme.txt	1602	1	26
🟩 D:\code signing\OpenSSL\pvk.exe	393216	1	26
🟩 D:\code signing\tool\signtool.exe	102912	1	26

Select Drives to Scan: All Drives

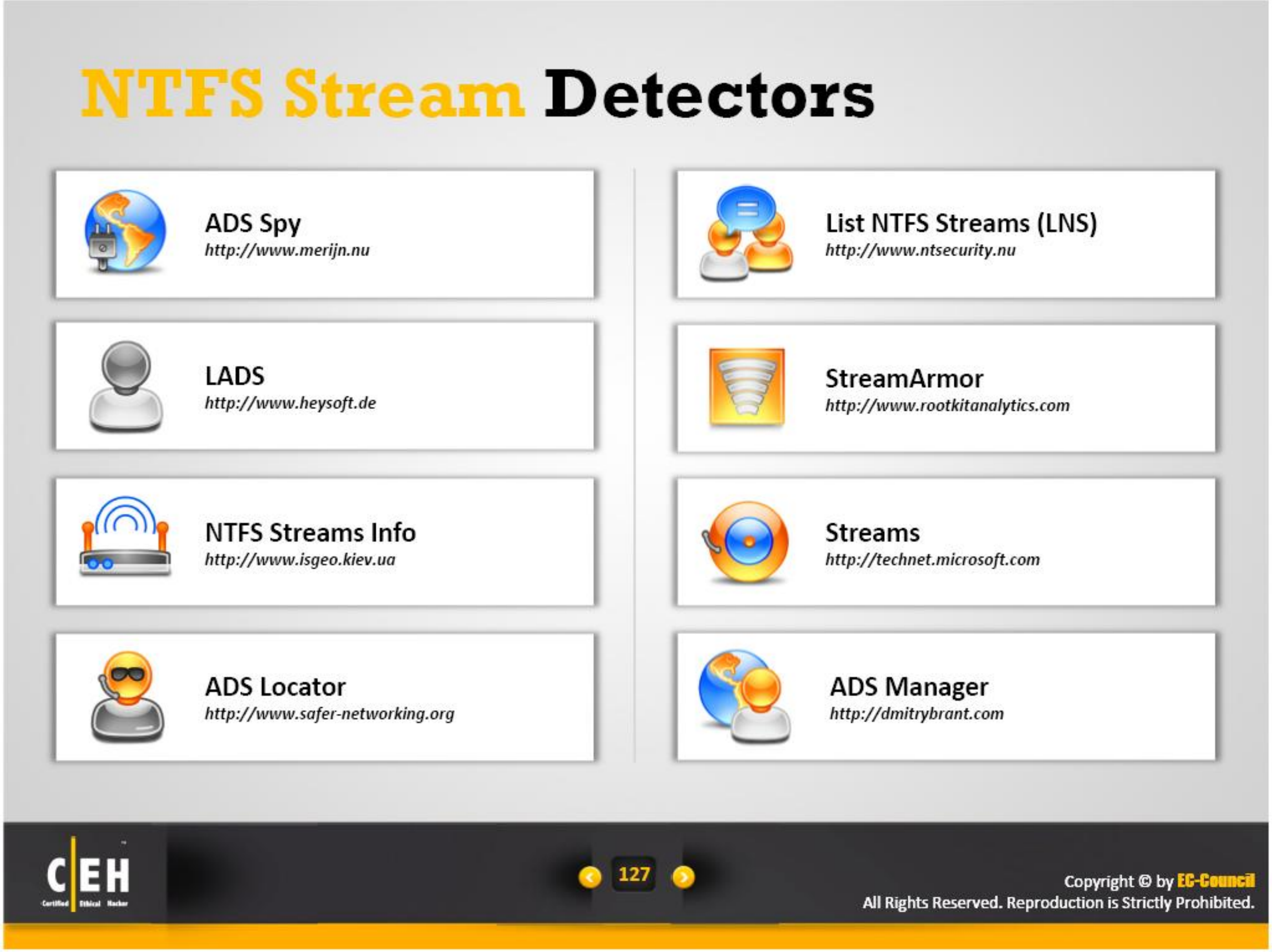
Select All Select None

Support Website Security Center Status: HEALTHY

(C:\) - NTFS
Programming (D:\) - NTFS
New Volume (E:\) - NTFS
Vista (F:\) - NTFS
Movies (G:\) - NTFS

Statistics:
Scanned: 5929
Good: 23 □ Hide
Risky: 0 □ Hide
Dangerous: 0

http://www.freesoftwaretoolbox.com



NTFS Stream Detectors

ADS Spy
http://www.merijn.nu

LADS
http://www.heysoft.de

NTFS Streams Info
http://www.isgeo.kiev.ua

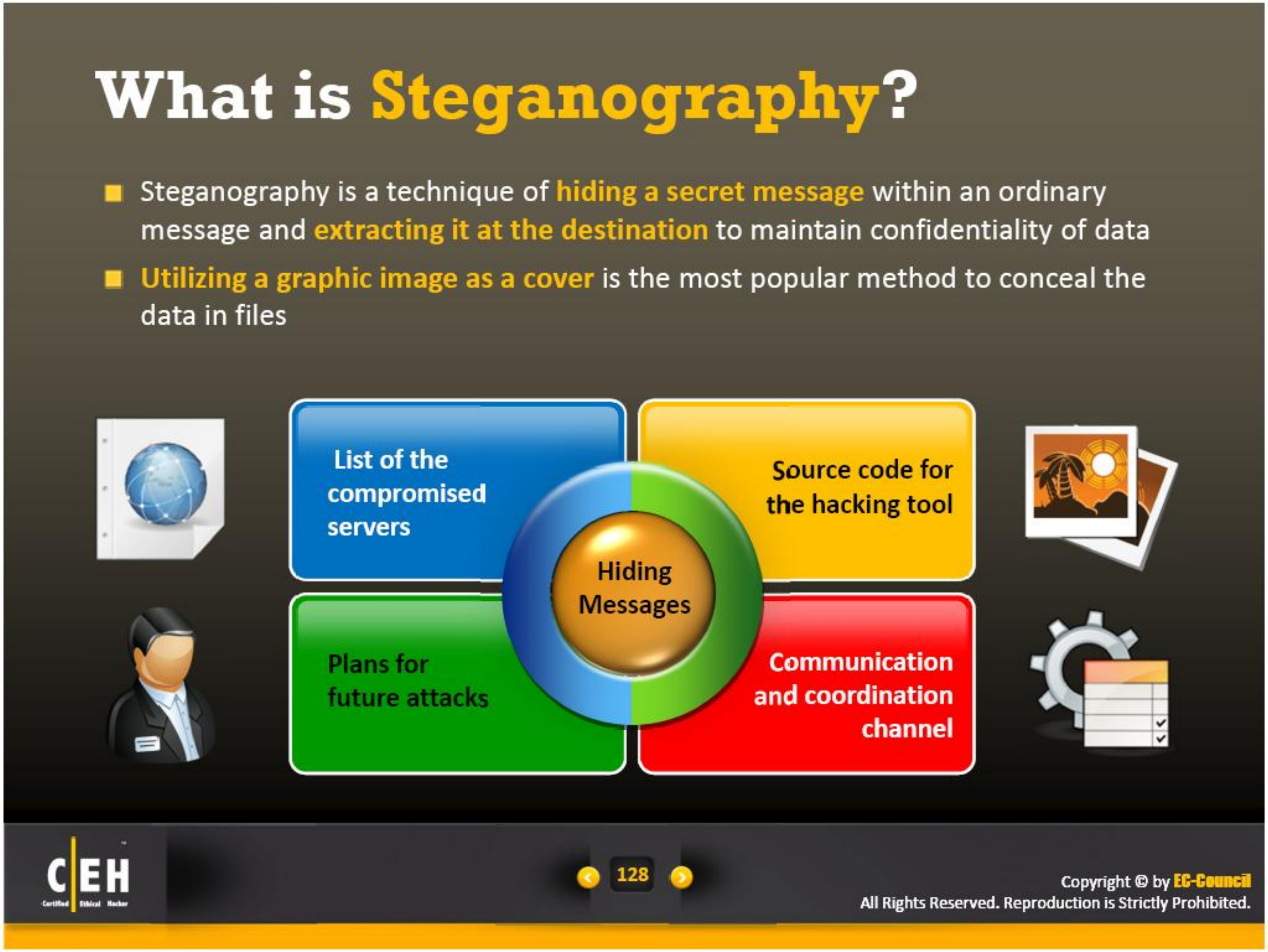
ADS Locator
http://www.safer-networking.org

List NTFS Streams (LNS)
http://www.ntsecurity.nu

StreamArmor
http://www.rootkitanalytics.com

Streams
http://technet.microsoft.com

ADS Manager
http://dmitrybrant.com



What is Steganography?

- Steganography is a technique of **hiding a secret message** within an ordinary message and **extracting it at the destination** to maintain confidentiality of data
- **Utilizing a graphic image as a cover** is the most popular method to conceal the data in files

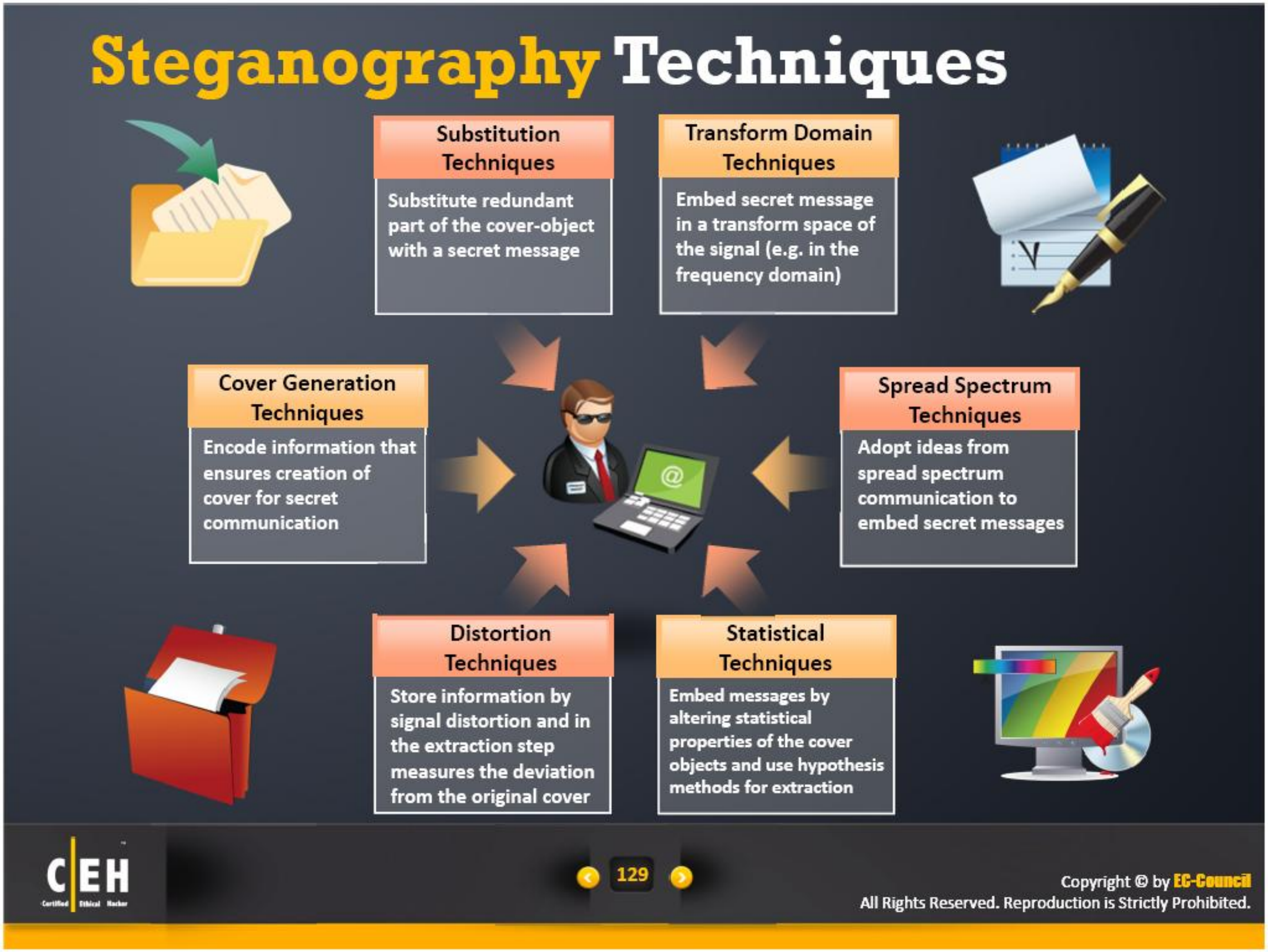
Hiding Messages

List of the compromised servers

Source code for the hacking tool

Plans for future attacks

Communication and coordination channel



Steganography Techniques

Substitution Techniques

Substitute redundant part of the cover-object with a secret message

Transform Domain Techniques

Embed secret message in a transform space of the signal (e.g. in the frequency domain)

Cover Generation Techniques

Encode information that ensures creation of cover for secret communication

Spread Spectrum Techniques

Adopt ideas from spread spectrum communication to embed secret messages

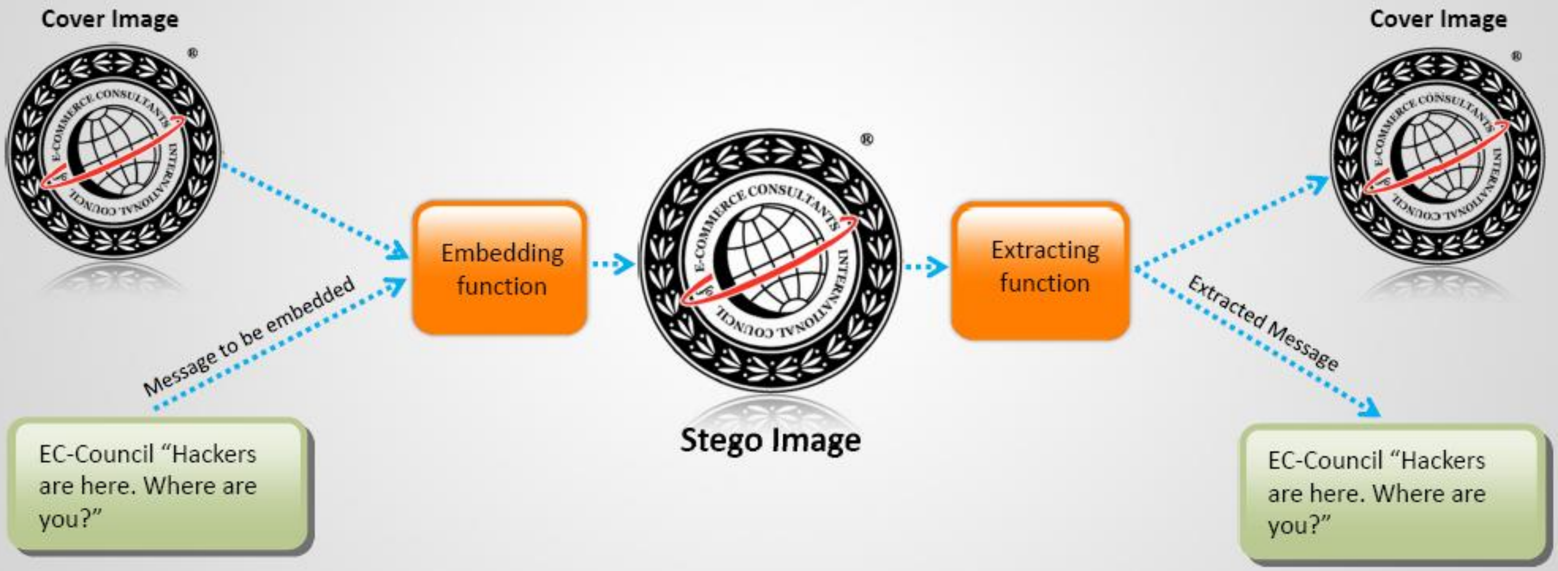
Distortion Techniques

Store information by signal distortion and in the extraction step measures the deviation from the original cover

Statistical Techniques

Embed messages by altering statistical properties of the cover objects and use hypothesis methods for extraction

How Steganography Works?



Cover Image

Embedding function

Message to be embedded

EC-Council “Hackers are here. Where are you?”

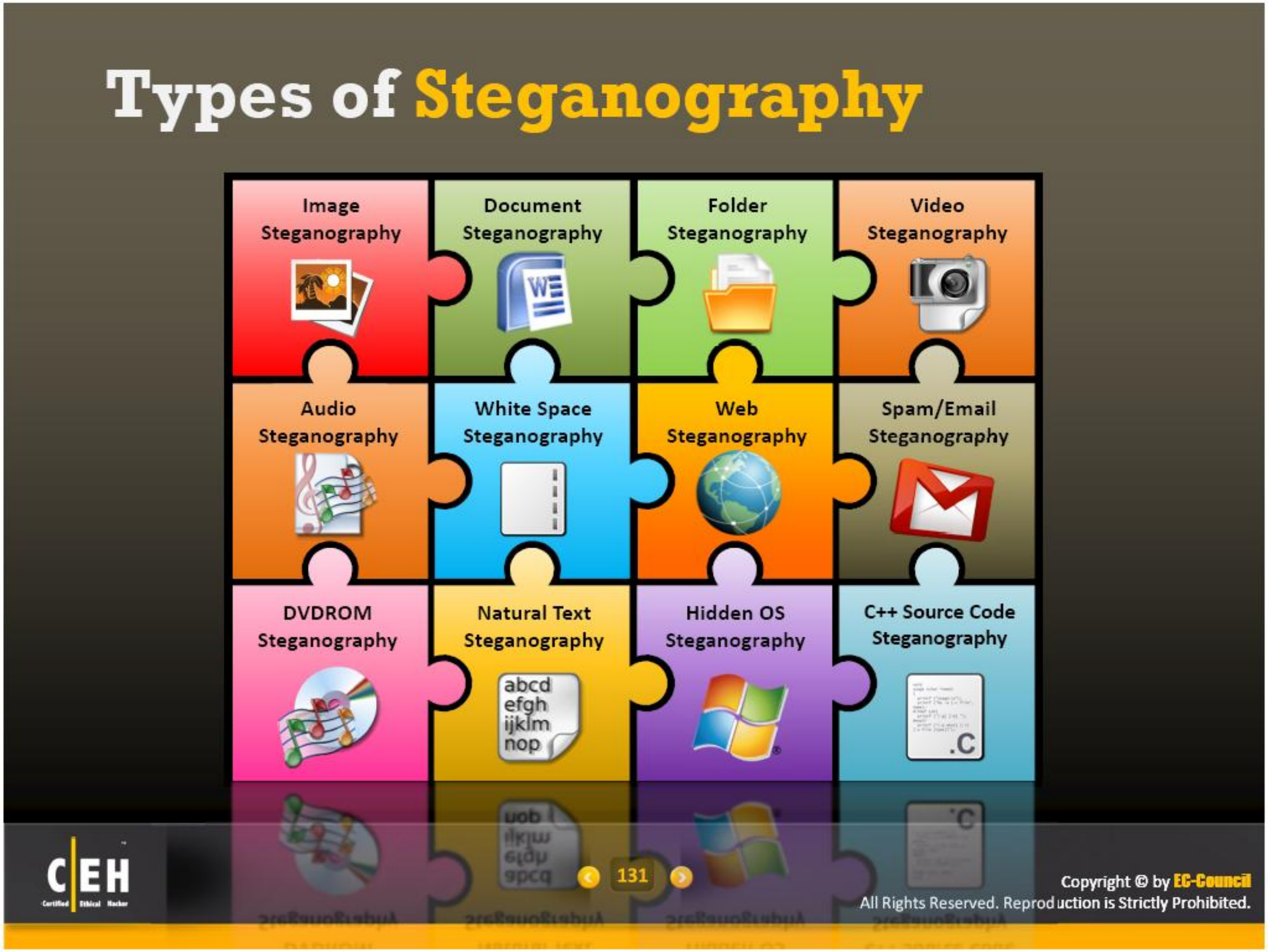
Stego Image

Extracting function

Cover Image

Extracted Message

EC-Council “Hackers are here. Where are you?”



Types of Steganography

Image Steganography

Document Steganography

Folder Steganography

Video Steganography

Audio Steganography

White Space Steganography

Web Steganography

Spam/Email Steganography

DVDROM Steganography

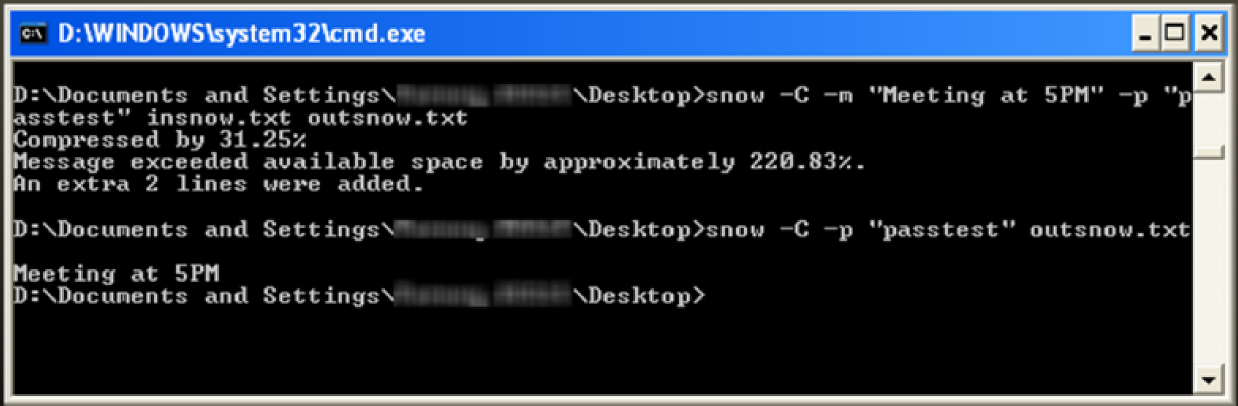
Natural Text Steganography

Hidden OS Steganography

C++ Source Code Steganography

Whitespace Steganography Tool: SNOW

1. The program snow is used to conceal messages in ASCII text by appending whitespace to the end of lines
2. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers
3. If the built-in encryption is used, the message cannot be read even if it is detected

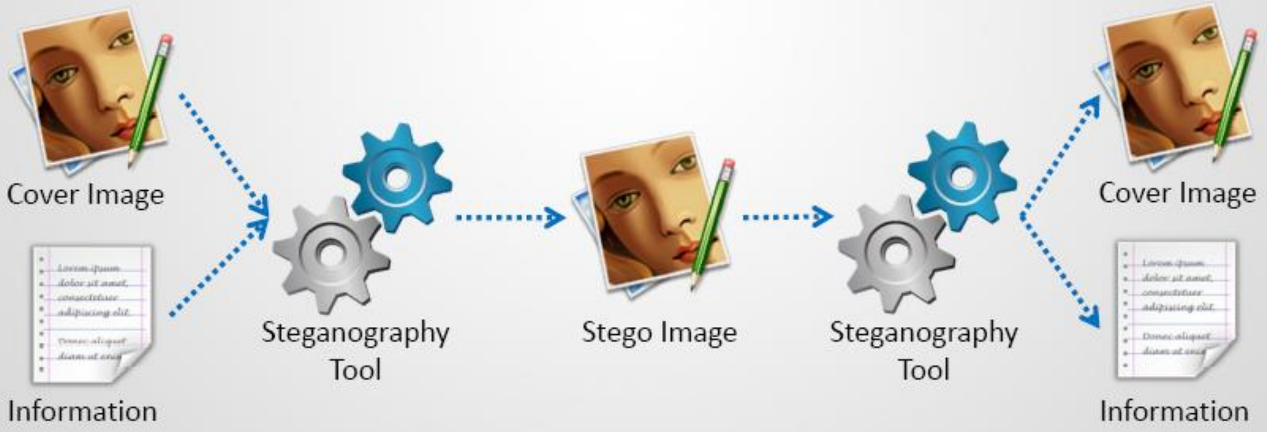


```
D:\Documents and Settings\[redacted]\Desktop>snow -C -m "Meeting at 5PM" -p "p
asstest" insnow.txt outsnow.txt
Compressed by 31.25%
Message exceeded available space by approximately 220.83%.
An extra 2 lines were added.

D:\Documents and Settings\[redacted]\Desktop>snow -C -p "passtest" outsnow.txt

Meeting at 5PM
D:\Documents and Settings\[redacted]\Desktop>
```

http://www.darkside.com.au

Image Steganography

- In image steganography, the **information is hidden in image** files of different formats such as .PNG, .JPG, .BMP, etc.
- Image steganography tools **replace redundant bits of image** data with the message in such a way that the effect can not be detected by human eyes



Cover Image

Information

Steganography Tool

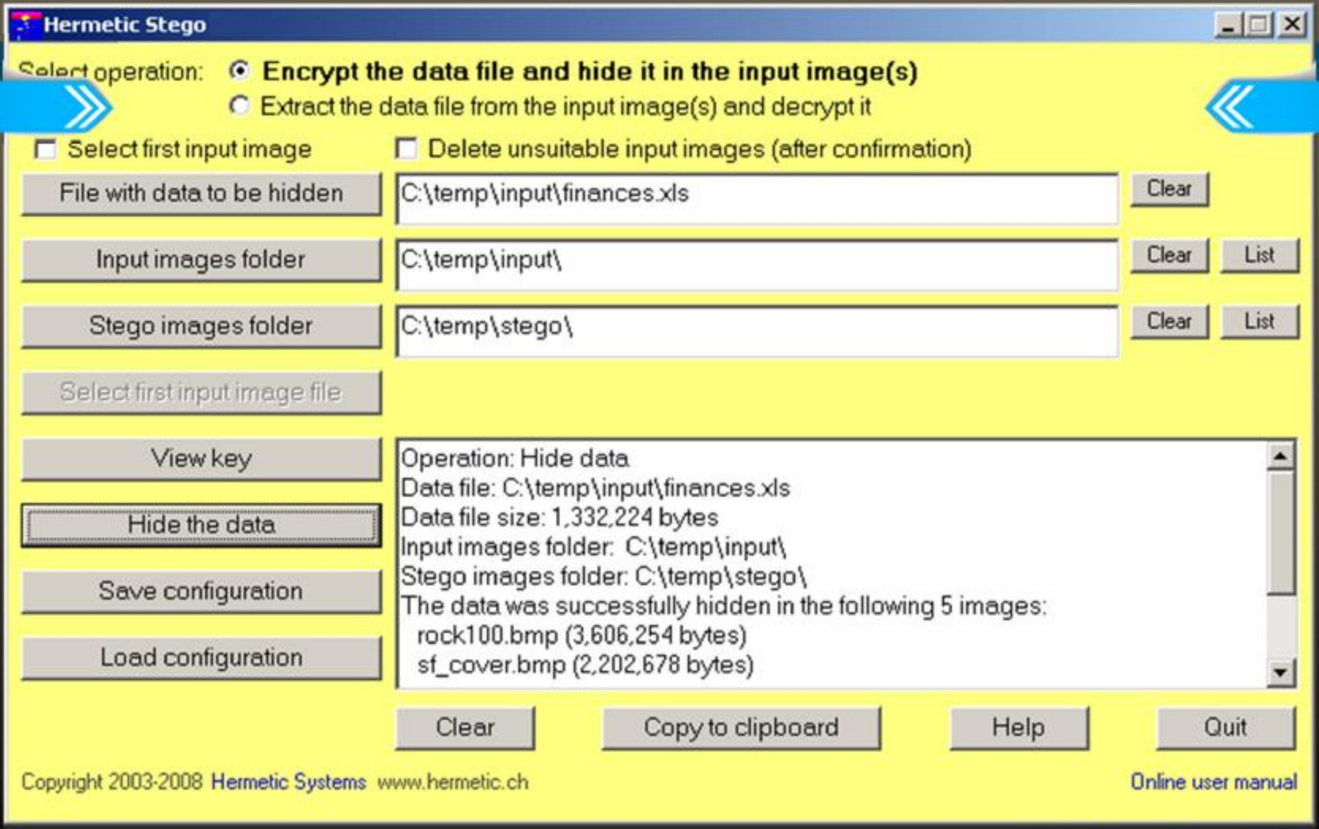
Stego Image

Steganography Tool

Cover Image

Information

Image Steganography: Hermetic Stego



Select operation: ● Encrypt the data file and hide it in the input image(s)
○ Extract the data file from the input image(s) and decrypt it

□ Select first input image □ Delete unsuitable input images (after confirmation)

File with data to be hidden: C:\temp\input\finances.xls

Input images folder: C:\temp\input\

Stego images folder: C:\temp\stego\

```
Operation: Hide data
Data file: C:\temp\input\finances.xls
Data file size: 1,332,224 bytes
Input images folder:  C:\temp\input\
Stego images folder: C:\temp\stego\
The data was successfully hidden in the following 5 images:
  rock100.bmp (3,606,254 bytes)
  sf_cover.bmp (2,202,678 bytes)
```

Copyright 2003-2008 Hermetic Systems www.hermetic.ch

http://www.hermetic.ch

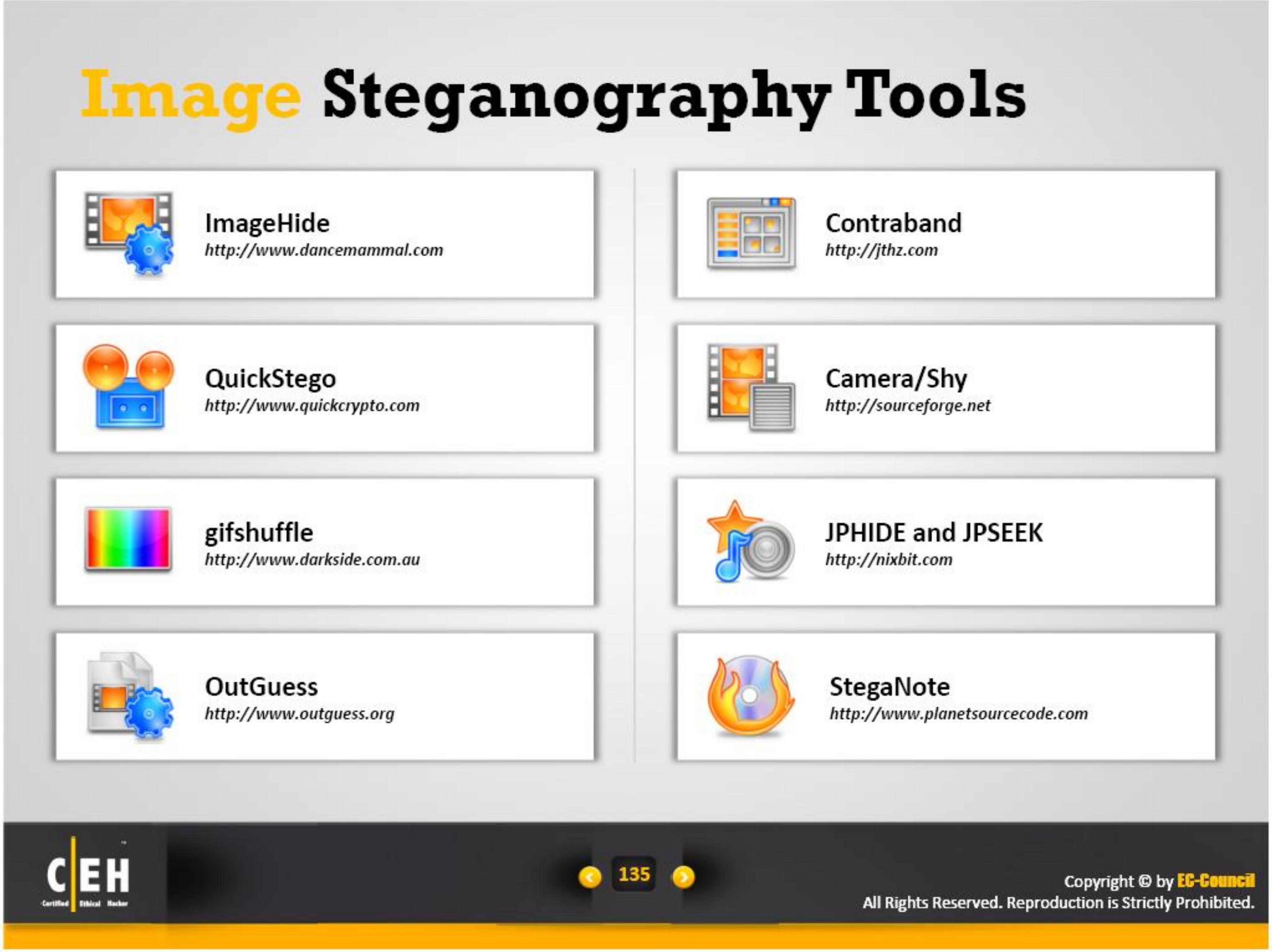
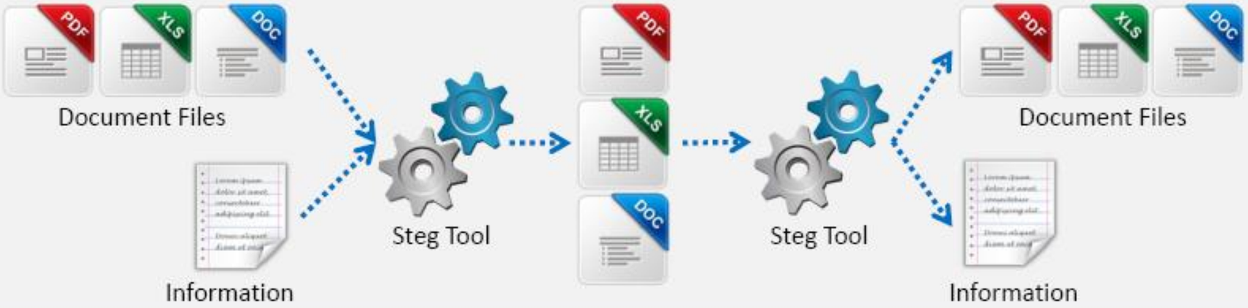
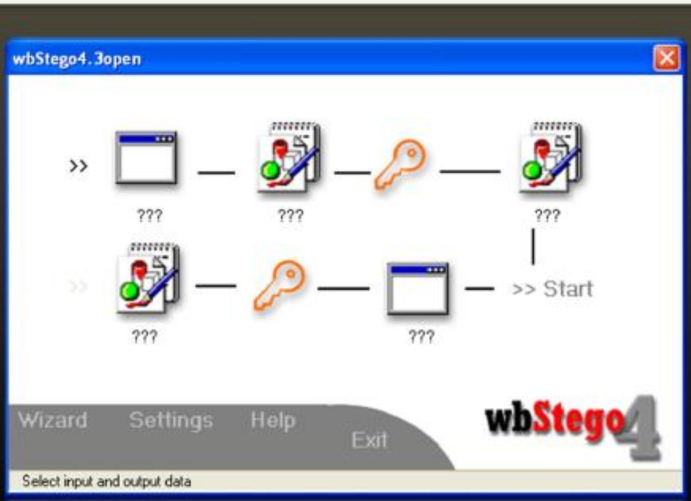


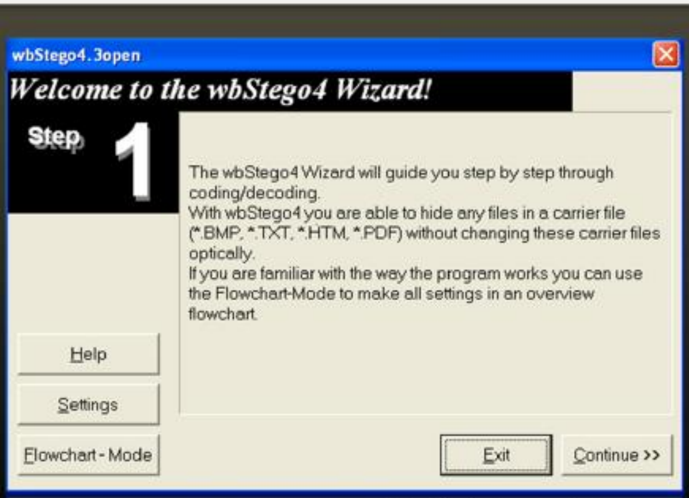
Image Steganography Tools

- ImageHide
  http://www.dancemammal.com
- QuickStego
  http://www.quickcrypto.com
- gifshuffle
  http://www.darkside.com.au
- OutGuess
  http://www.outguess.org
- Contraband
  http://jthz.com
- Camera/Shy
  http://sourceforge.net
- JPHIDE and JPSEEK
  http://nixbit.com
- StegaNote
  http://www.planetsourcecode.com

Document Steganography: wbStego





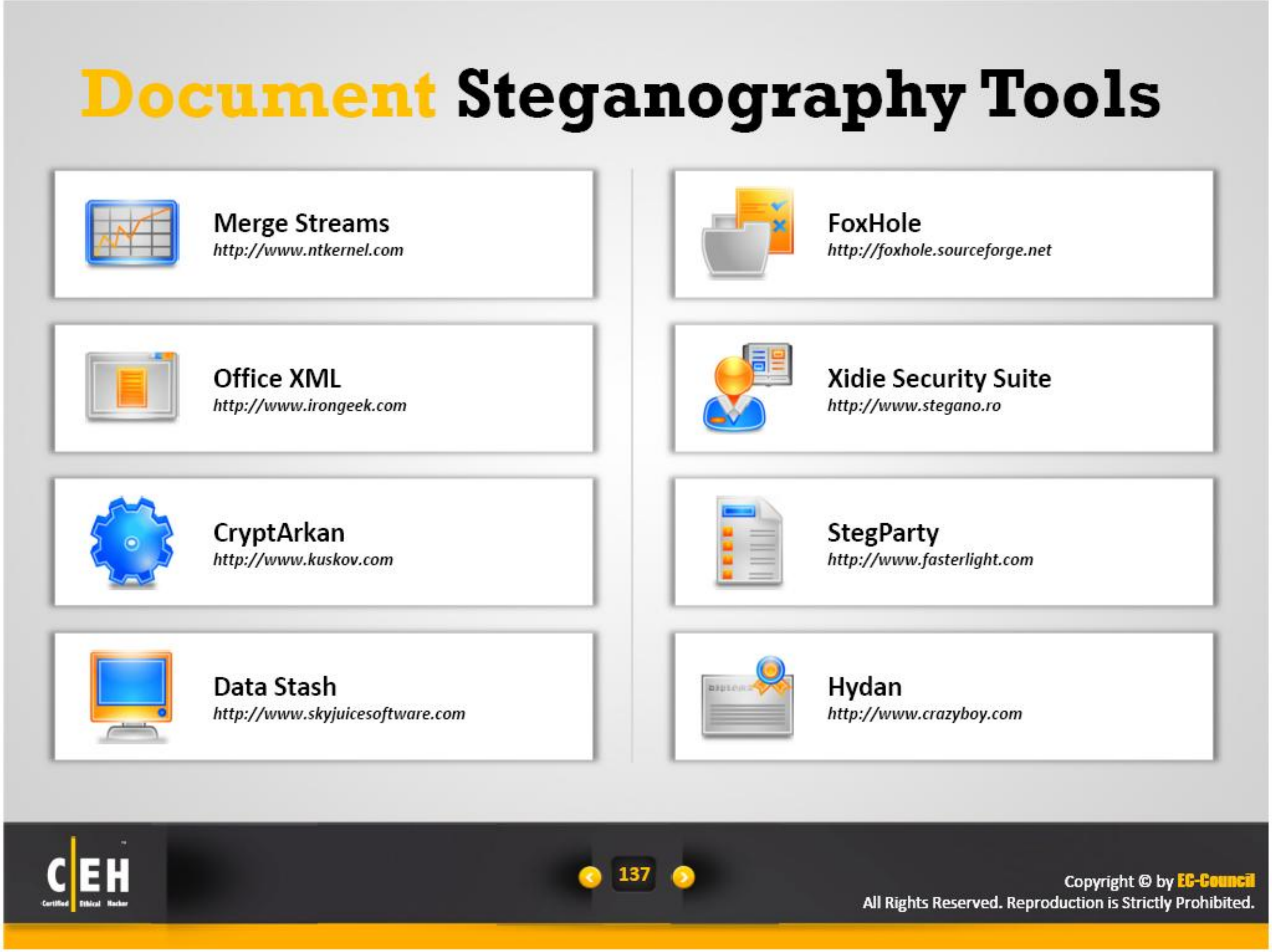

wbStego4.3open

Welcome to the wbStego4 Wizard!

Step 1

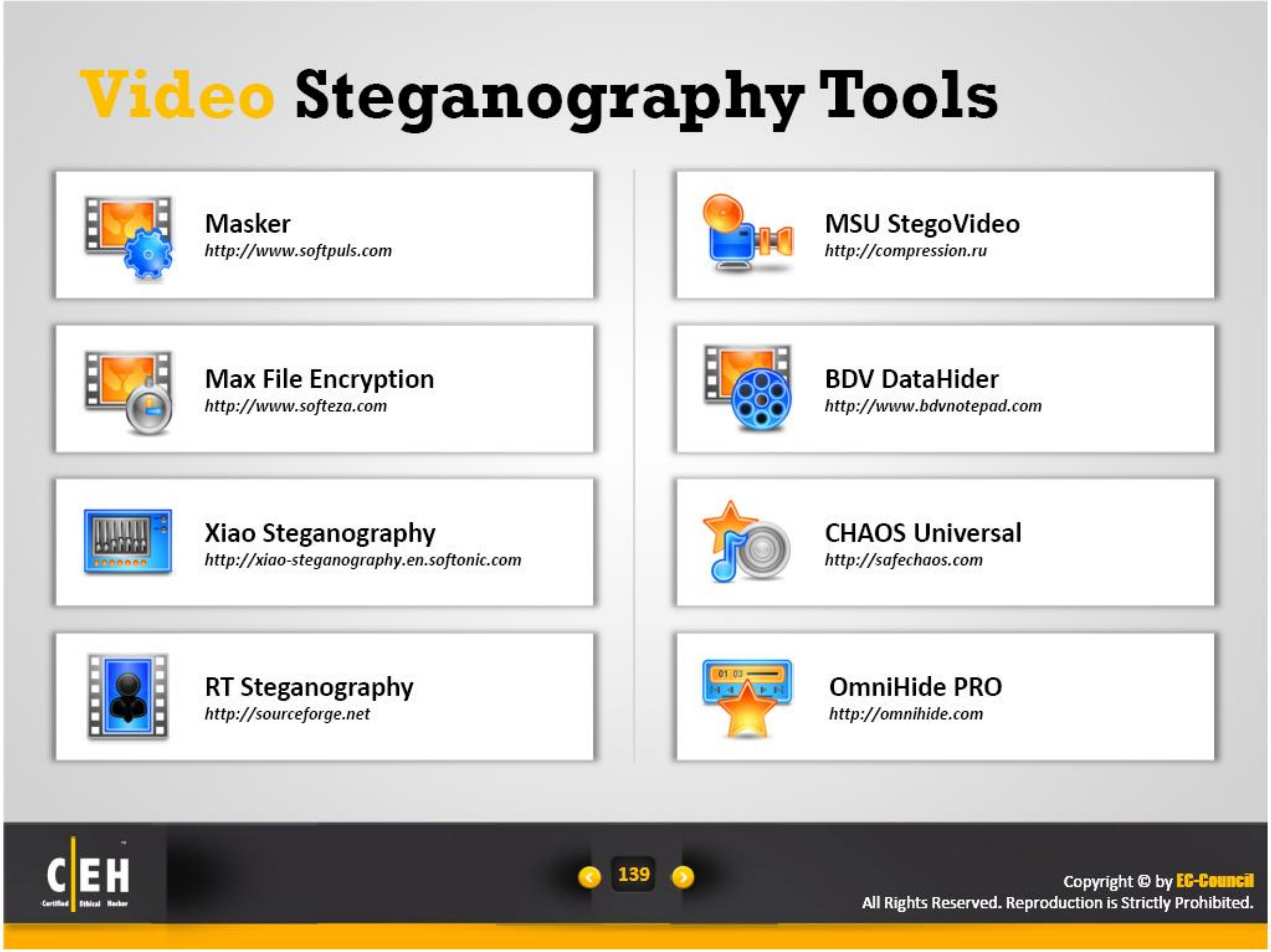
The wbStego4 Wizard will guide you step by step through coding/decoding.
With wbStego4 you are able to hide any files in a carrier file (*.BMP, *.TXT, *.HTM, *.PDF) without changing these carrier files optically.
If you are familiar with the way the program works you can use the Flowchart-Mode to make all settings in an overview flowchart.

http://wbstego.wbailer.com



Document Steganography Tools

- Merge Streams
  http://www.ntkernel.com
- Office XML
  http://www.irongeek.com
- CryptArkan
  http://www.kuskov.com
- Data Stash
  http://www.skyjuicesoftware.com
- FoxHole
  http://foxhole.sourceforge.net
- Xidie Security Suite
  http://www.stegano.ro
- StegParty
  http://www.fasterlight.com
- Hydan
  http://www.crazyboy.com

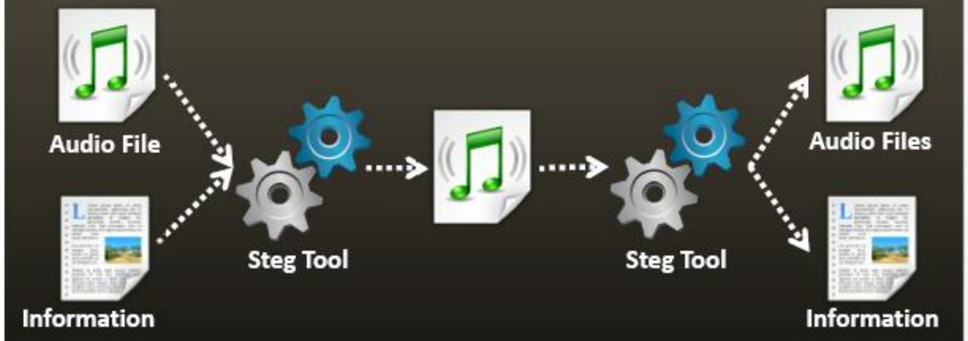


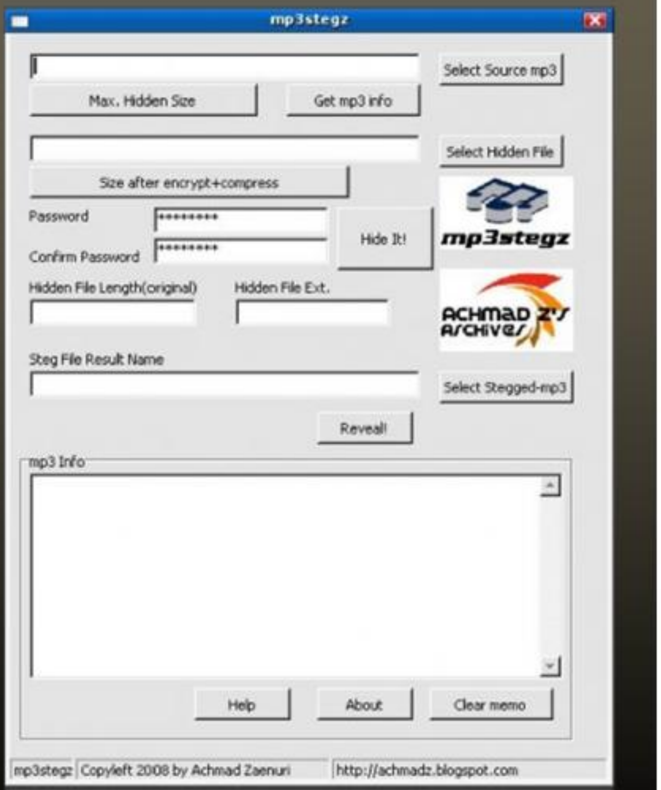
Video Steganography Tools

Masker *http://www.softpuls.com*	**MSU StegoVideo** *http://compression.ru*
Max File Encryption *http://www.softeza.com*	**BDV DataHider** *http://www.bdvnotepad.com*
Xiao Steganography *http://xiao-steganography.en.softonic.com*	**CHAOS Universal** *http://safechaos.com*
RT Steganography *http://sourceforge.net*	**OmniHide PRO** *http://omnihide.com*

Audio Steganography: Mp3stegz

Audio steganography refers to hiding a secret information in audio files such as .MP3, .RM, .WAV, etc.



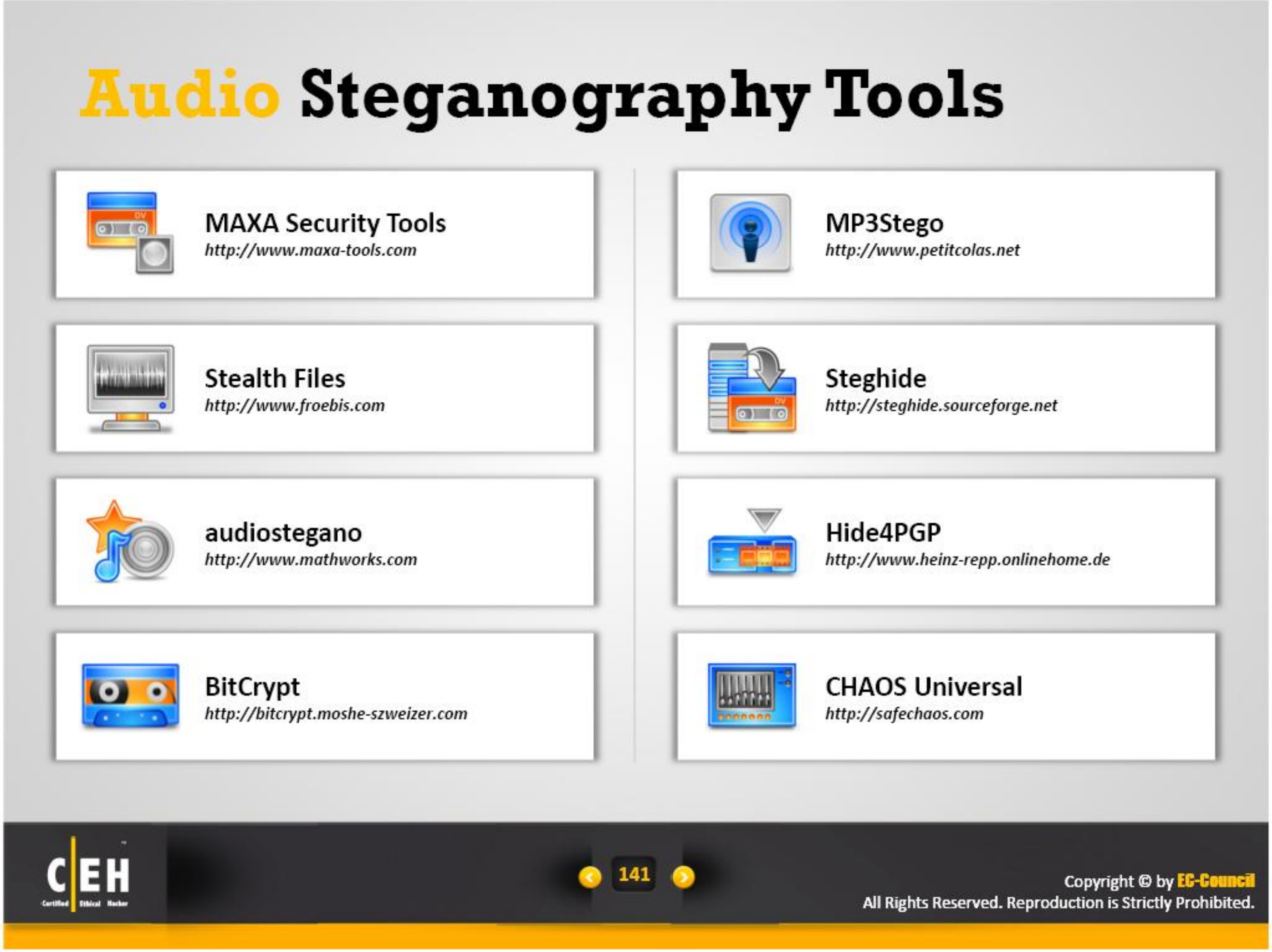


Password *********

Confirm Password *********

mp3stegz | Copyleft 2008 by Achmad Zaenuri | http://achmadz.blogspot.com

http://sourceforge.net



Audio Steganography Tools

MAXA Security Tools
http://www.maxa-tools.com

Stealth Files
http://www.froebis.com

audiostegano
http://www.mathworks.com

BitCrypt
http://bitcrypt.moshe-szweizer.com

MP3Stego
http://www.petitcolas.net

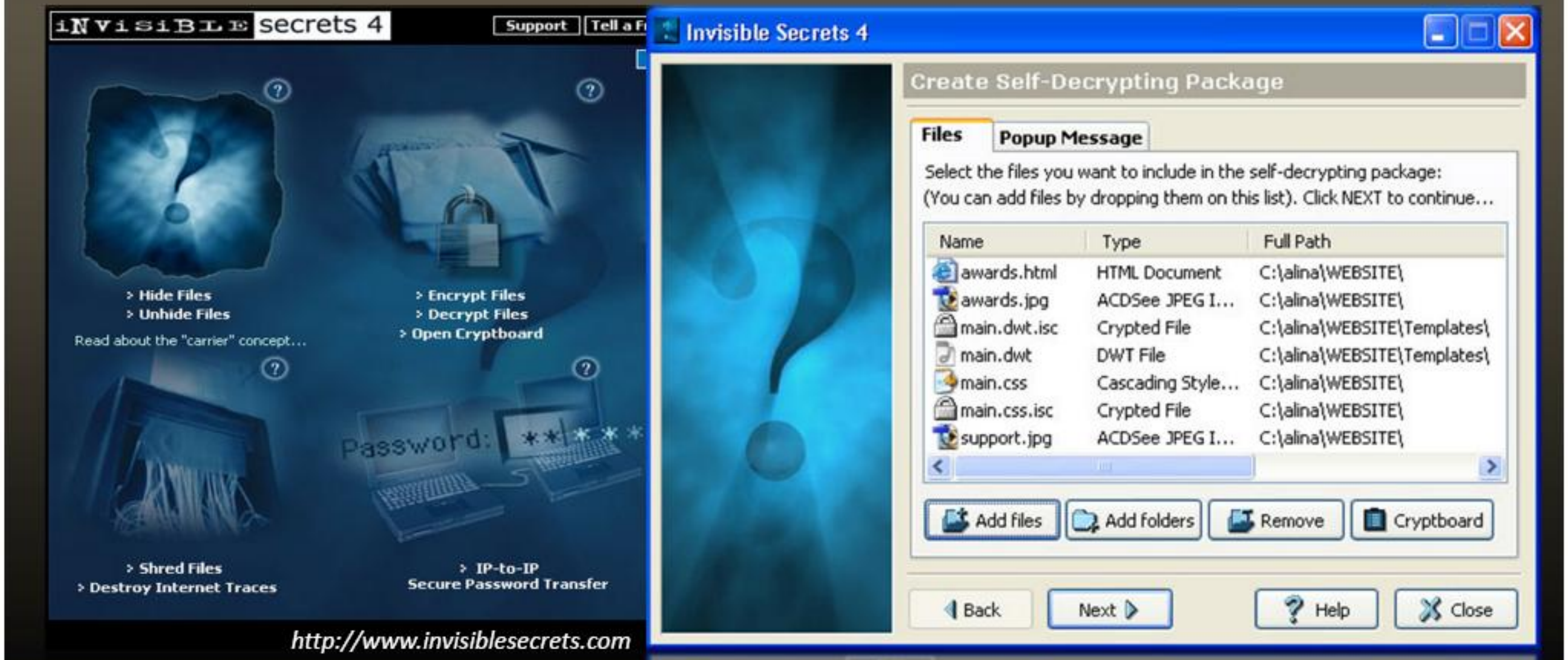
Steghide
http://steghide.sourceforge.net

Hide4PGP
http://www.heinz-repp.onlinehome.de

CHAOS Universal
http://safechaos.com

Folder Steganography: Invisible Secrets 4

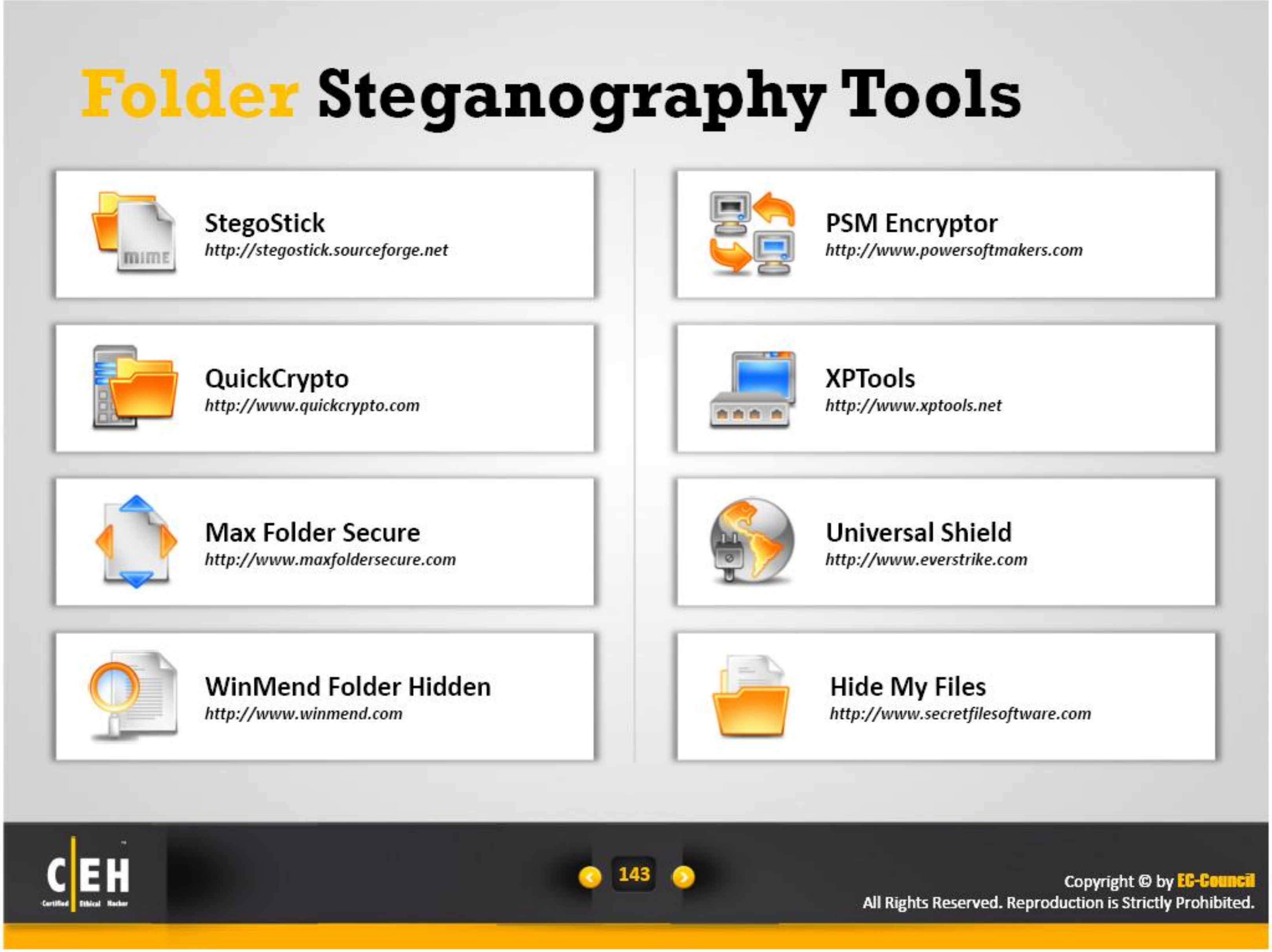
Folder steganography refers to hiding a secret information in folders



Create Self-Decrypting Package

Select the files you want to include in the self-decrypting package:
(You can add files by dropping them on this list). Click NEXT to continue...

Name	Type	Full Path
awards.html	HTML Document	C:\alina\WEBSITE\
awards.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\
main.dwt.isc	Crypted File	C:\alina\WEBSITE\Templates\
main.dwt	DWT File	C:\alina\WEBSITE\Templates\
main.css	Cascading Style...	C:\alina\WEBSITE\
main.css.isc	Crypted File	C:\alina\WEBSITE\
support.jpg	ACDSee JPEG I...	C:\alina\WEBSITE\



Folder Steganography Tools

StegoStick
http://stegostick.sourceforge.net

PSM Encryptor
http://www.powersoftmakers.com

QuickCrypto
http://www.quickcrypto.com

XPTools
http://www.xptools.net

Max Folder Secure
http://www.maxfoldersecure.com

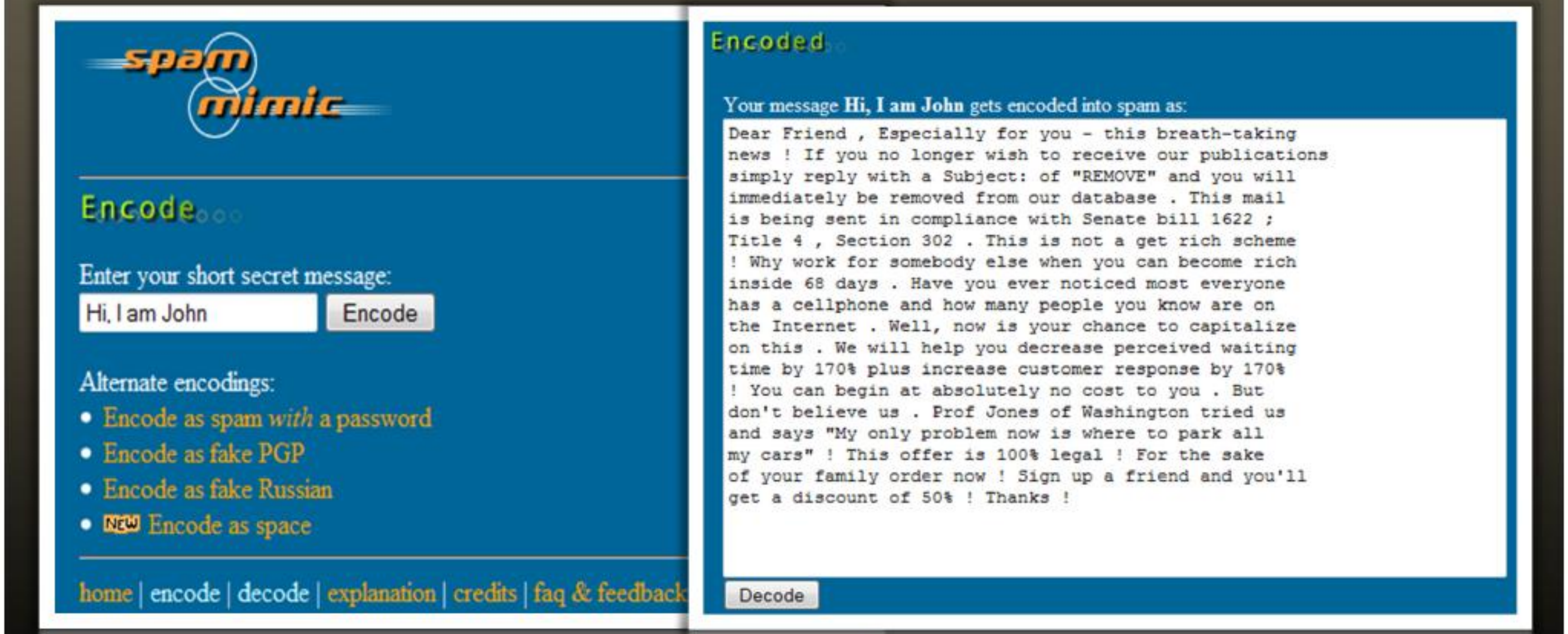
Universal Shield
http://www.everstrike.com

WinMend Folder Hidden
http://www.winmend.com

Hide My Files
http://www.secretfilesoftware.com

Spam/Email Steganography: Spam Mimic

Spam steganography refers to hiding information in spam messages



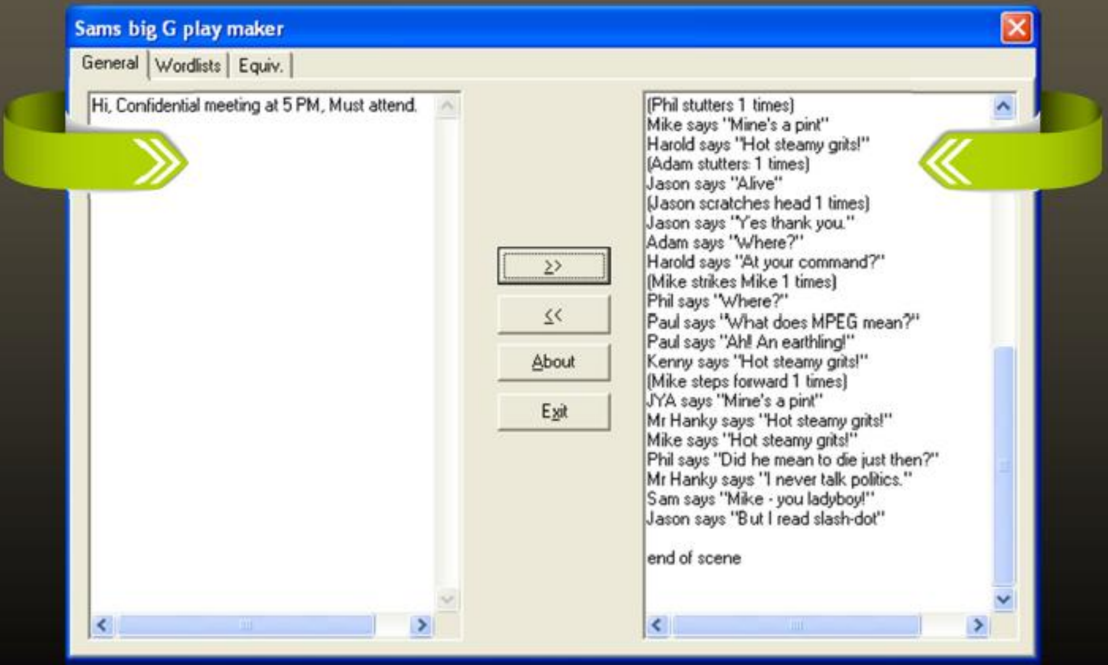
Your message **Hi, I am John** gets encoded into spam as:

```
Dear Friend , Especially for you - this breath-taking
news ! If you no longer wish to receive our publications
simply reply with a Subject: of "REMOVE" and you will
immediately be removed from our database . This mail
is being sent in compliance with Senate bill 1622 ;
Title 4 , Section 302 . This is not a get rich scheme
! Why work for somebody else when you can become rich
inside 68 days . Have you ever noticed most everyone
has a cellphone and how many people you know are on
the Internet . Well, now is your chance to capitalize
on this . We will help you decrease perceived waiting
time by 170% plus increase customer response by 170%
! You can begin at absolutely no cost to you . But
don't believe us . Prof Jones of Washington tried us
and says "My only problem now is where to park all
my cars" ! This offer is 100% legal ! For the sake
of your family order now ! Sign up a friend and you'll
get a discount of 50% ! Thanks !
```

http://www.spammimic.com

Natural Text Steganography: Sams Big G Play Maker

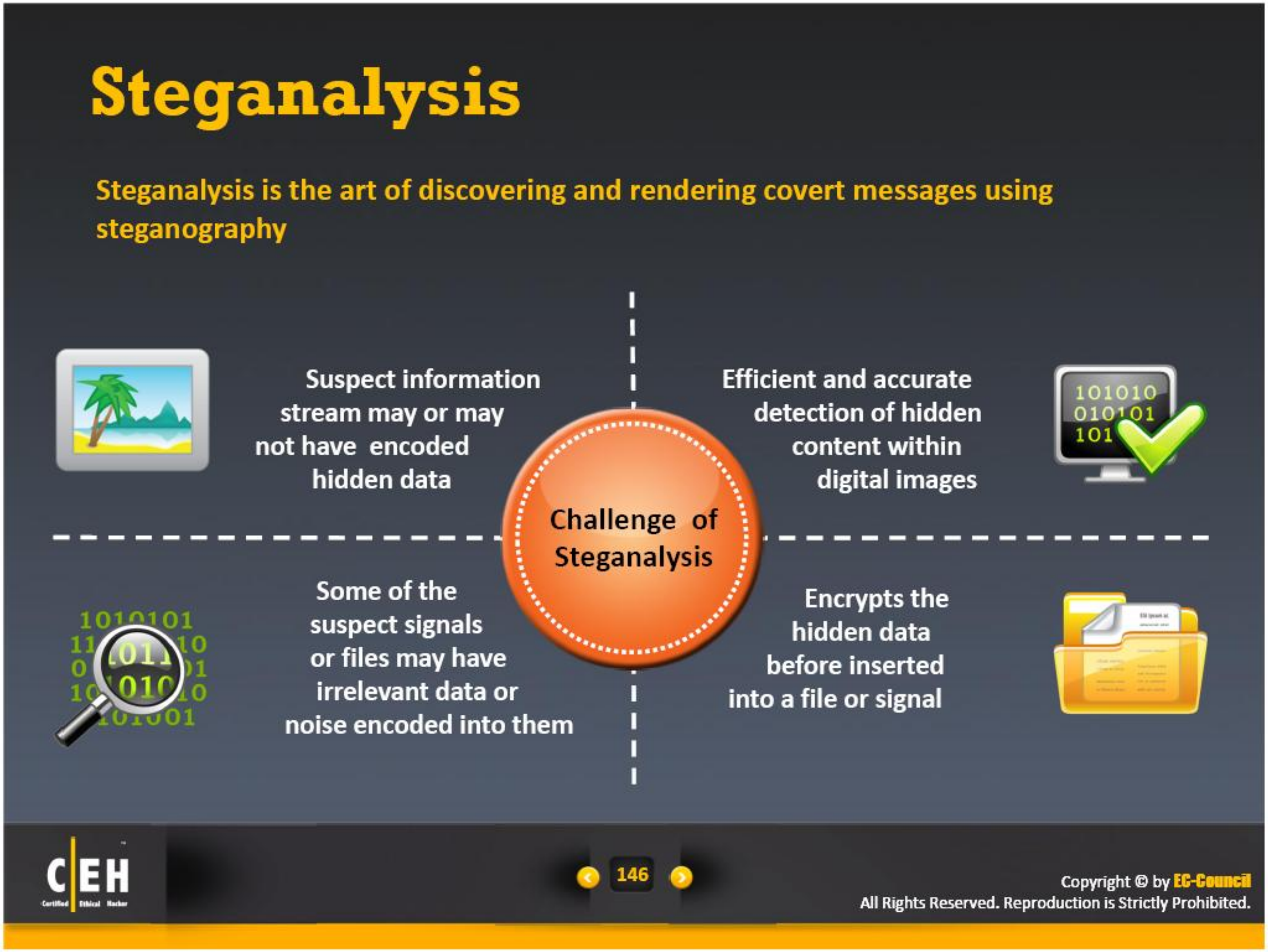
Natural text steganography programs convert sensitive information in to a **user-definable free speech** such as a play



Hi, Confidential meeting at 5 PM, Must attend.

```
(Phil stutters 1 times)
Mike says "Mine's a pint"
Harold says "Hot steamy grits!"
(Adam stutters 1 times)
Jason says "Alive"
(Jason scratches head 1 times)
Jason says "Yes thank you."
Adam says "Where?"
Harold says "At your command?"
(Mike strikes Mike 1 times)
Phil says "Where?"
Paul says "What does MPEG mean?"
Paul says "Ah! An earthling!"
Kenny says "Hot steamy grits!"
(Mike steps forward 1 times)
JYA says "Mine's a pint"
Mr Hanky says "Hot steamy grits!"
Mike says "Hot steamy grits!"
Phil says "Did he mean to die just then?"
Mr Hanky says "I never talk politics."
Sam says "Mike - you ladyboy!"
Jason says "But I read slash-dot"

end of scene
```

http://www.scramdisk.clara.net



Steganalysis

Steganalysis is the art of discovering and rendering covert messages using steganography

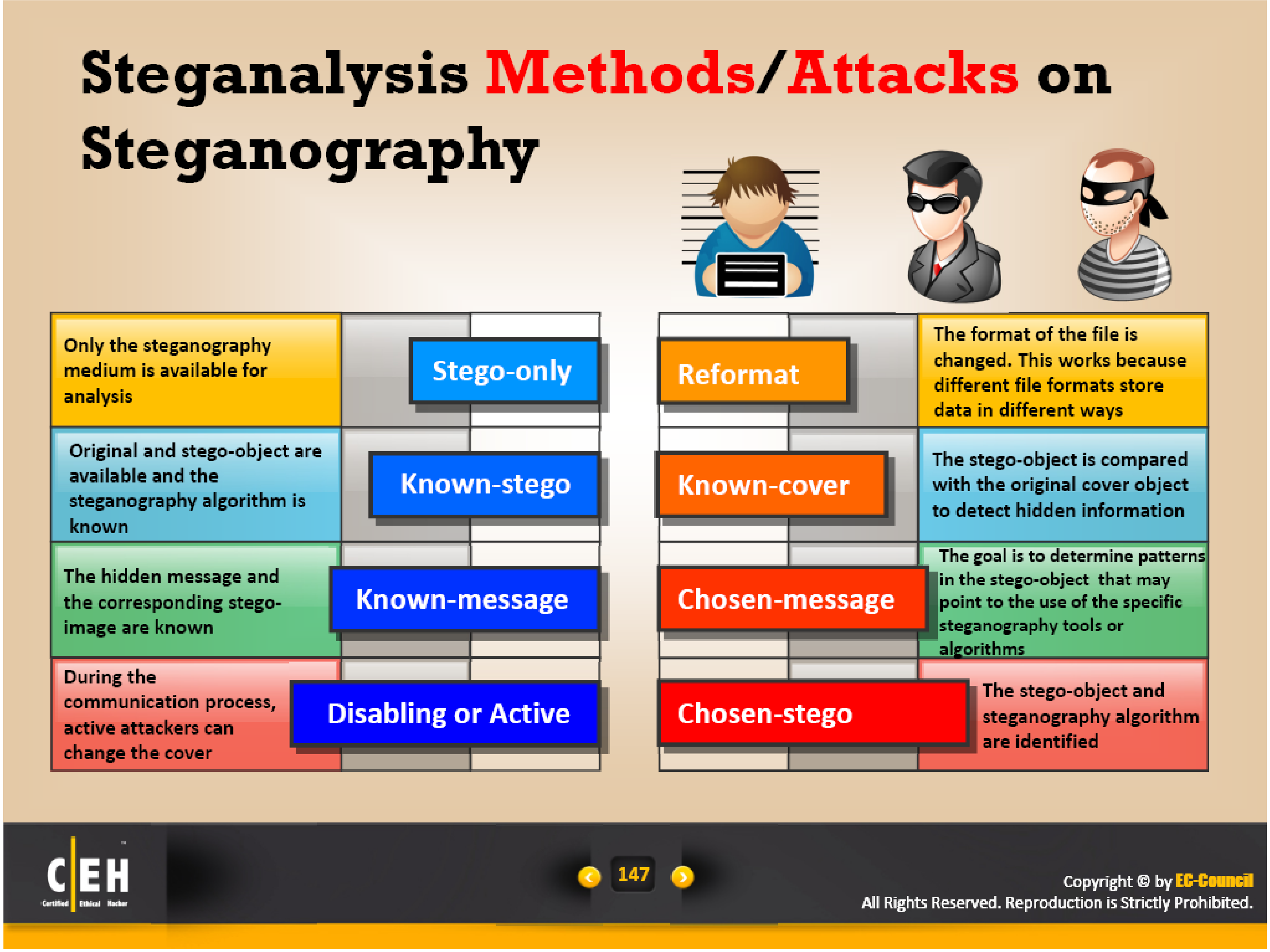
Challenge of Steganalysis

Suspect information stream may or may not have encoded hidden data

Efficient and accurate detection of hidden content within digital images

Some of the suspect signals or files may have irrelevant data or noise encoded into them

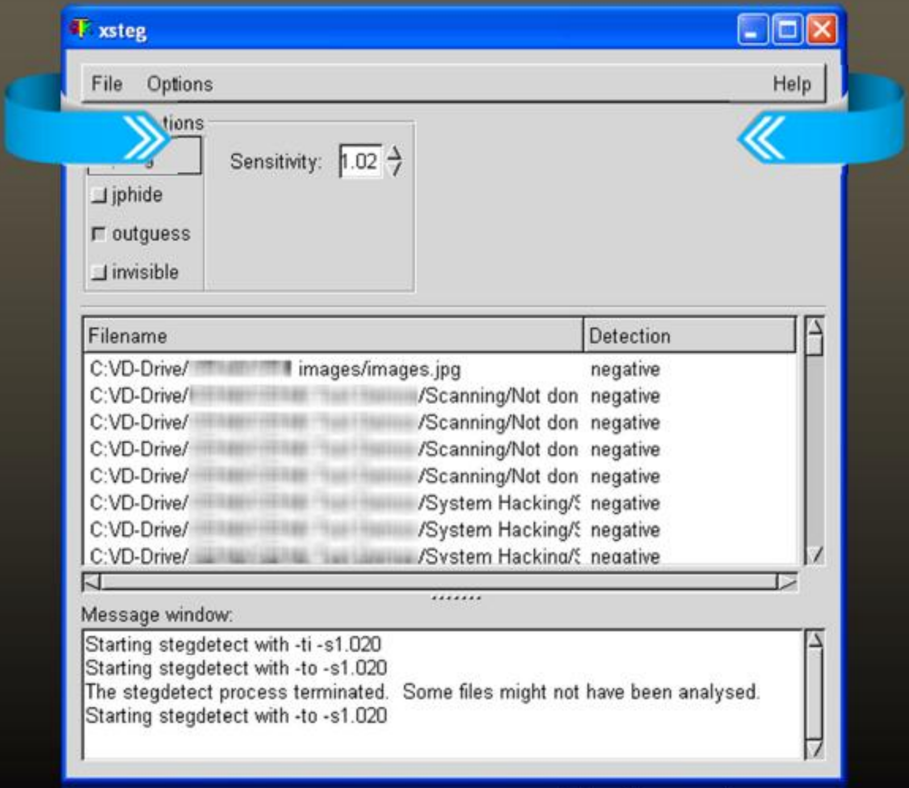
Encrypts the hidden data before inserted into a file or signal



Steganalysis Methods/Attacks on Steganography

Only the steganography medium is available for analysis	Stego-only	Reformat	The format of the file is changed. This works because different file formats store data in different ways
Original and stego-object are available and the steganography algorithm is known	Known-stego	Known-cover	The stego-object is compared with the original cover object to detect hidden information
The hidden message and the corresponding stego-image are known	Known-message	Chosen-message	The goal is to determine patterns in the stego-object that may point to the use of the specific steganography tools or algorithms
During the communication process, active attackers can change the cover	Disabling or Active	Chosen-stego	The stego-object and steganography algorithm are identified

Steganography Detection Tool: Stegdetect



□ jphide

□ outguess

□ invisible

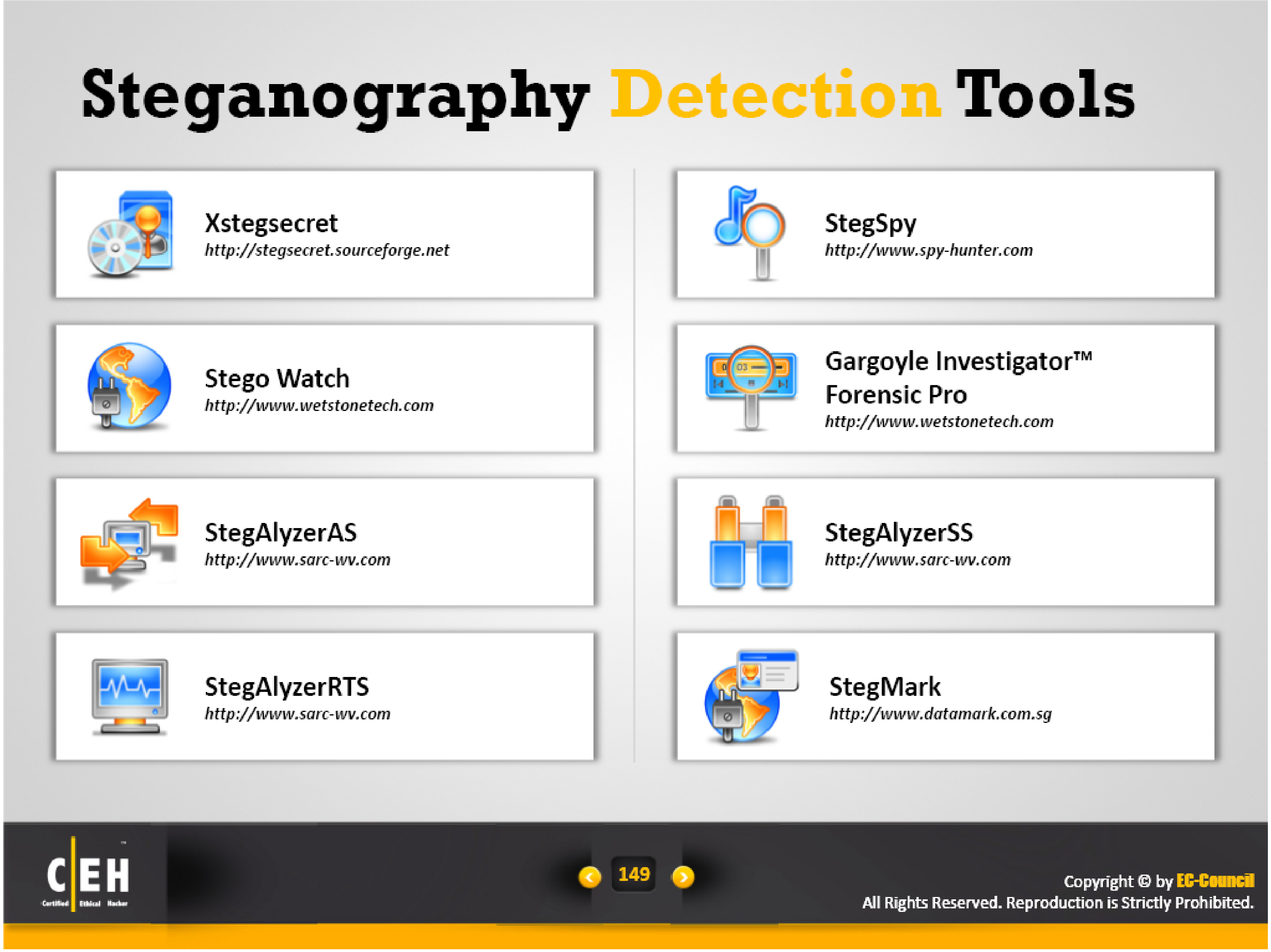
Sensitivity: 1.02

Filename	Detection
C:VD-Drive/[redacted] images/images.jpg	negative
C:VD-Drive/[redacted]/Scanning/Not don	negative
C:VD-Drive/[redacted]/Scanning/Not don	negative
C:VD-Drive/[redacted]/Scanning/Not don	negative
C:VD-Drive/[redacted]/Scanning/Not don	negative
C:VD-Drive/[redacted]/System Hacking/S	negative
C:VD-Drive/[redacted]/System Hacking/S	negative
C:VD-Drive/[redacted]/System Hacking/S	negative

Message window:

```
Starting stegdetect with -ti -s1.020
Starting stegdetect with -to -s1.020
The stegdetect process terminated.  Some files might not have been analysed.
Starting stegdetect with -to -s1.020
```

http://www.outguess.org



Steganography Detection Tools

Xstegsecret
http://stegsecret.sourceforge.net

Stego Watch
http://www.wetstonetech.com

StegAlyzerAS
http://www.sarc-wv.com

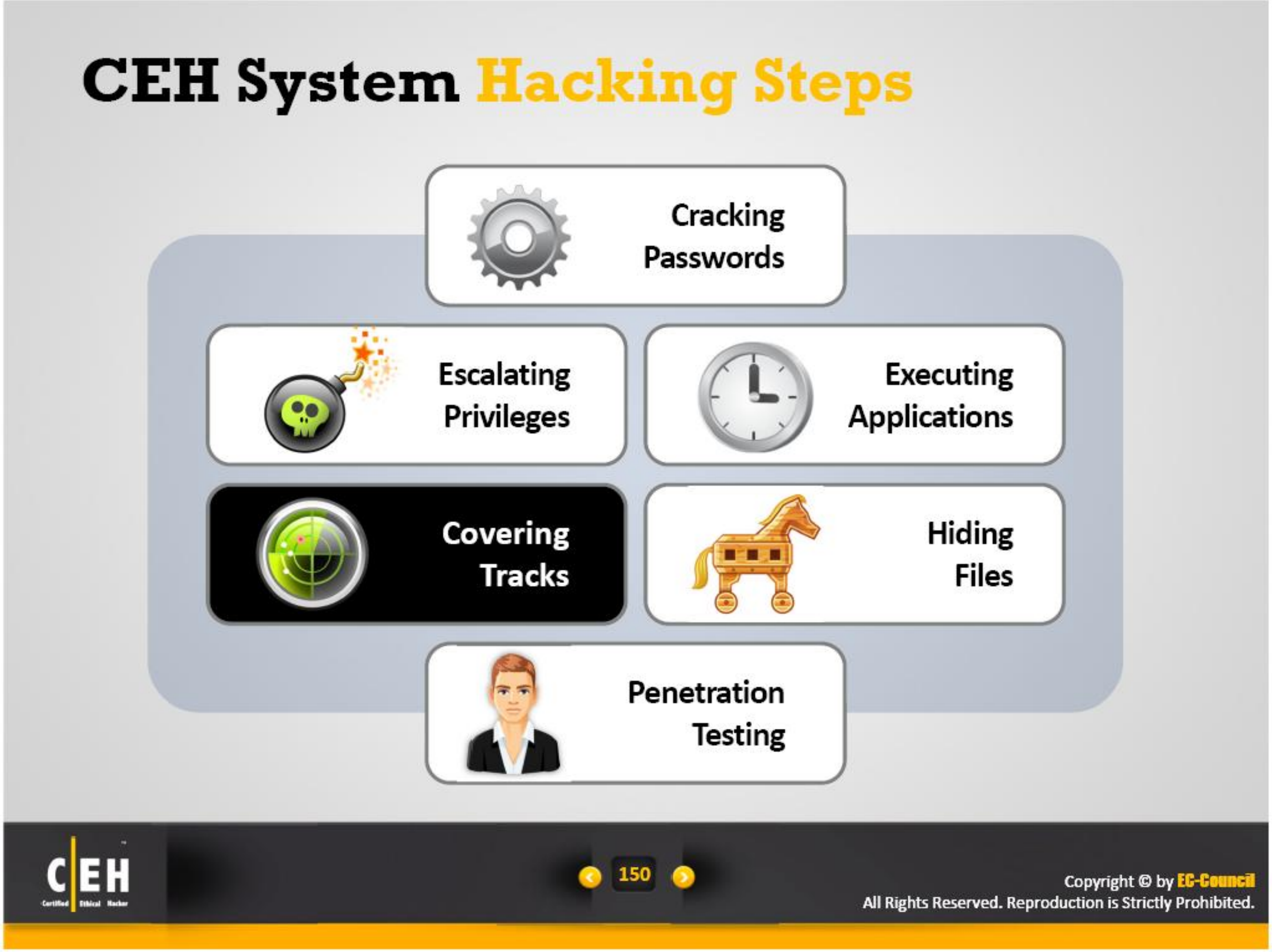
StegAlyzerRTS
http://www.sarc-wv.com

StegSpy
http://www.spy-hunter.com

Gargoyle Investigator™ Forensic Pro
http://www.wetstonetech.com

StegAlyzerSS
http://www.sarc-wv.com

StegMark
http://www.datamark.com.sg



CEH System Hacking Steps

Cracking Passwords

Escalating Privileges

Executing Applications

Covering Tracks

Hiding Files

Penetration Testing

Why Cover Tracks?

01:09 Action A1
01:09 Action A2
01:09 Action A3
01:09 Action A4
01:09 Action A5
01:09 Actio

Attackers cover tracks so that:

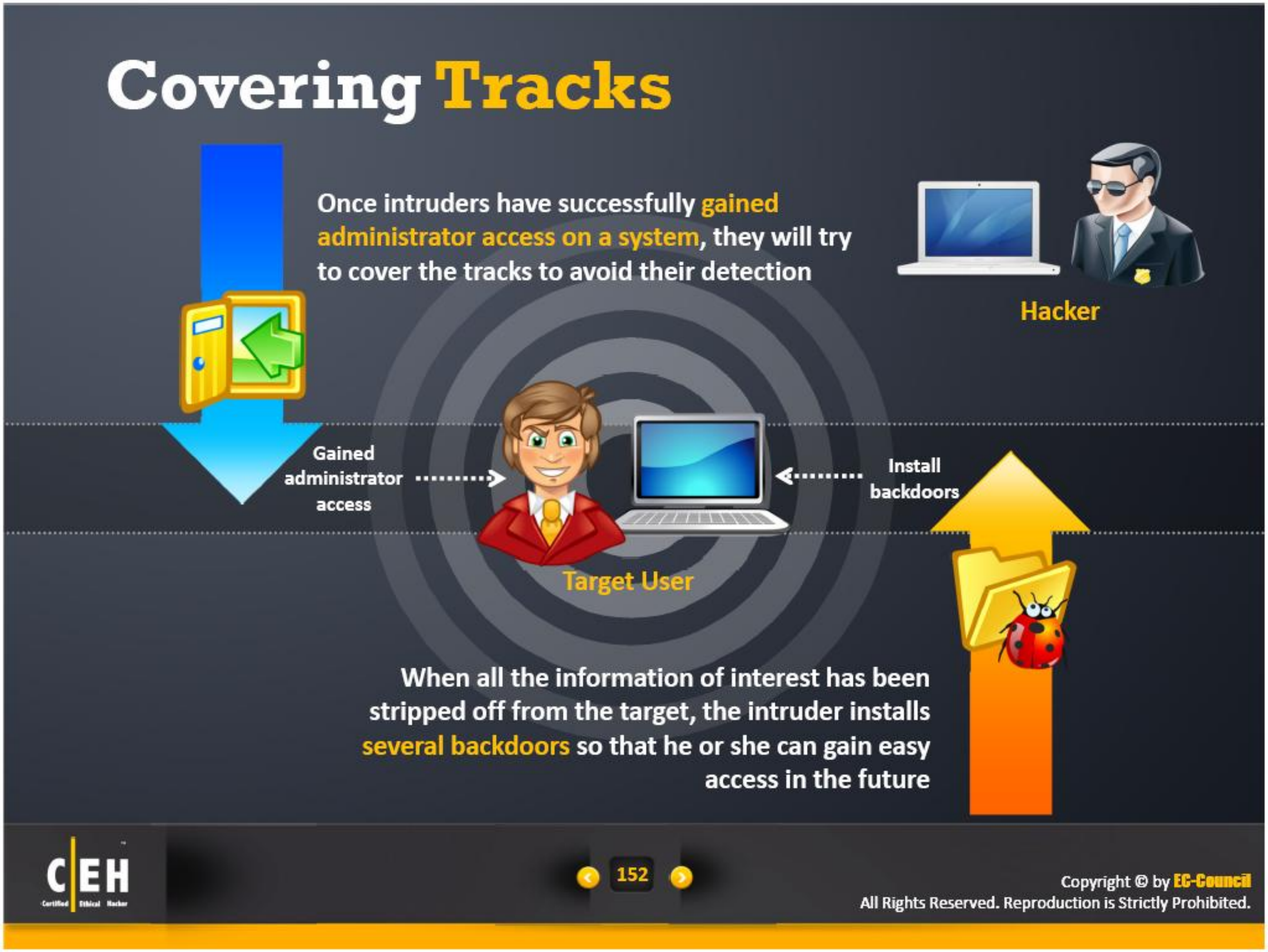
1. They can attack again
2. They can cover the tracks to avoid their detection
3. They can install backdoors to gain access in future

Manipulating the log files

1. **SECEVENT.EVT (security):** Failed logins, accessing files without privileges
2. **SYSEVENT.EVT (system):** Driver failure, things not operating correctly
3. **APPEVENT.EVT (applications)**

Altering event logs

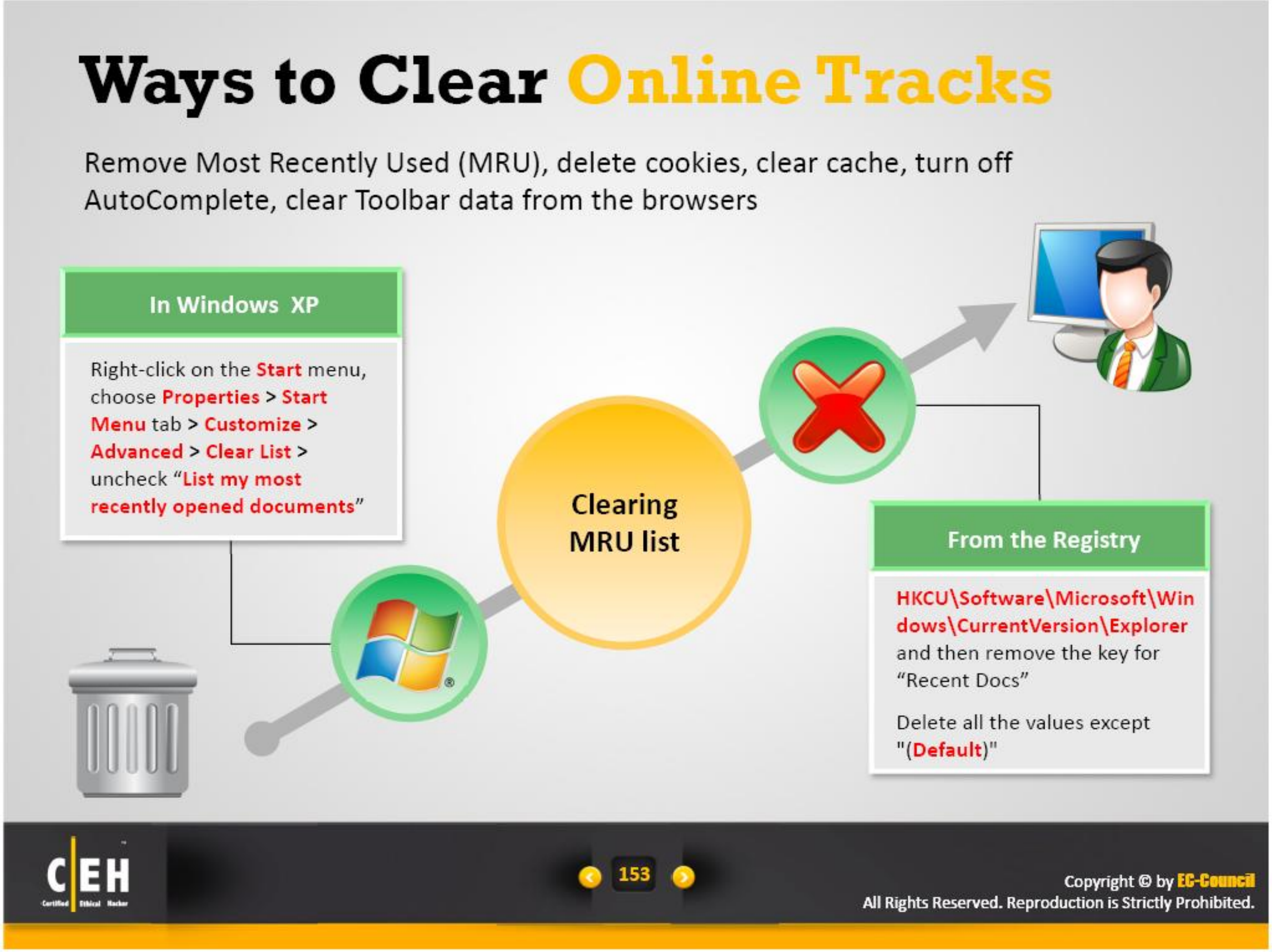
The attacker might not want to delete the entire log



Covering Tracks

Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection

When all the information of interest has been stripped off from the target, the intruder installs several backdoors so that he or she can gain easy access in the future



Ways to Clear Online Tracks

Remove Most Recently Used (MRU), delete cookies, clear cache, turn off AutoComplete, clear Toolbar data from the browsers

In Windows XP

Right-click on the **Start** menu, choose **Properties** > **Start Menu** tab > **Customize** > **Advanced** > **Clear List** > uncheck "**List my most recently opened documents**"

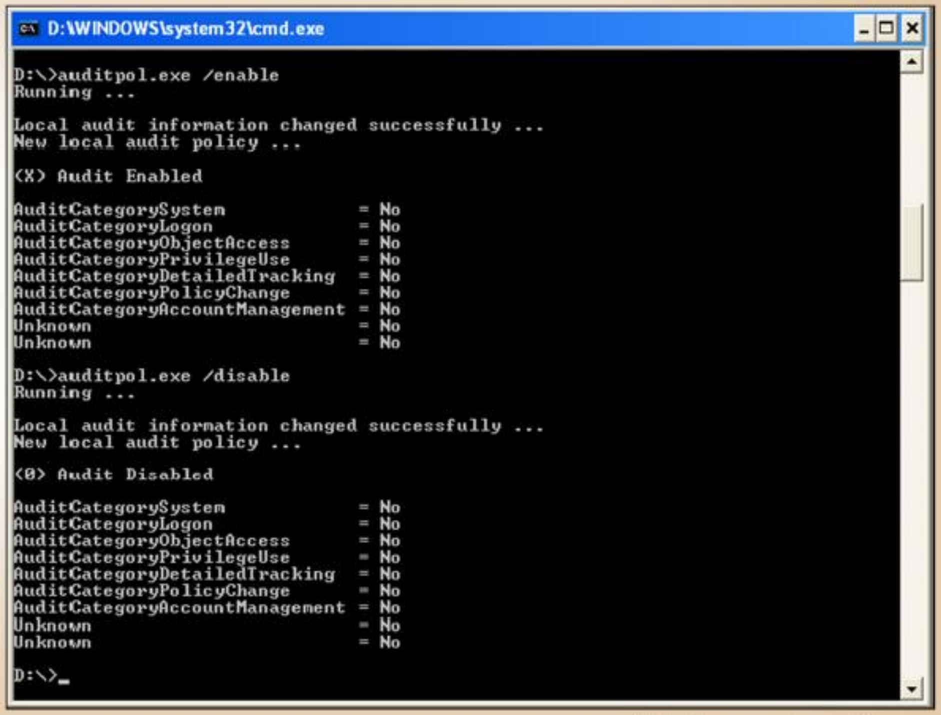
From the Registry

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer and then remove the key for "Recent Docs"

Delete all the values except "(**Default**)"

Disabling Auditing: Auditpol

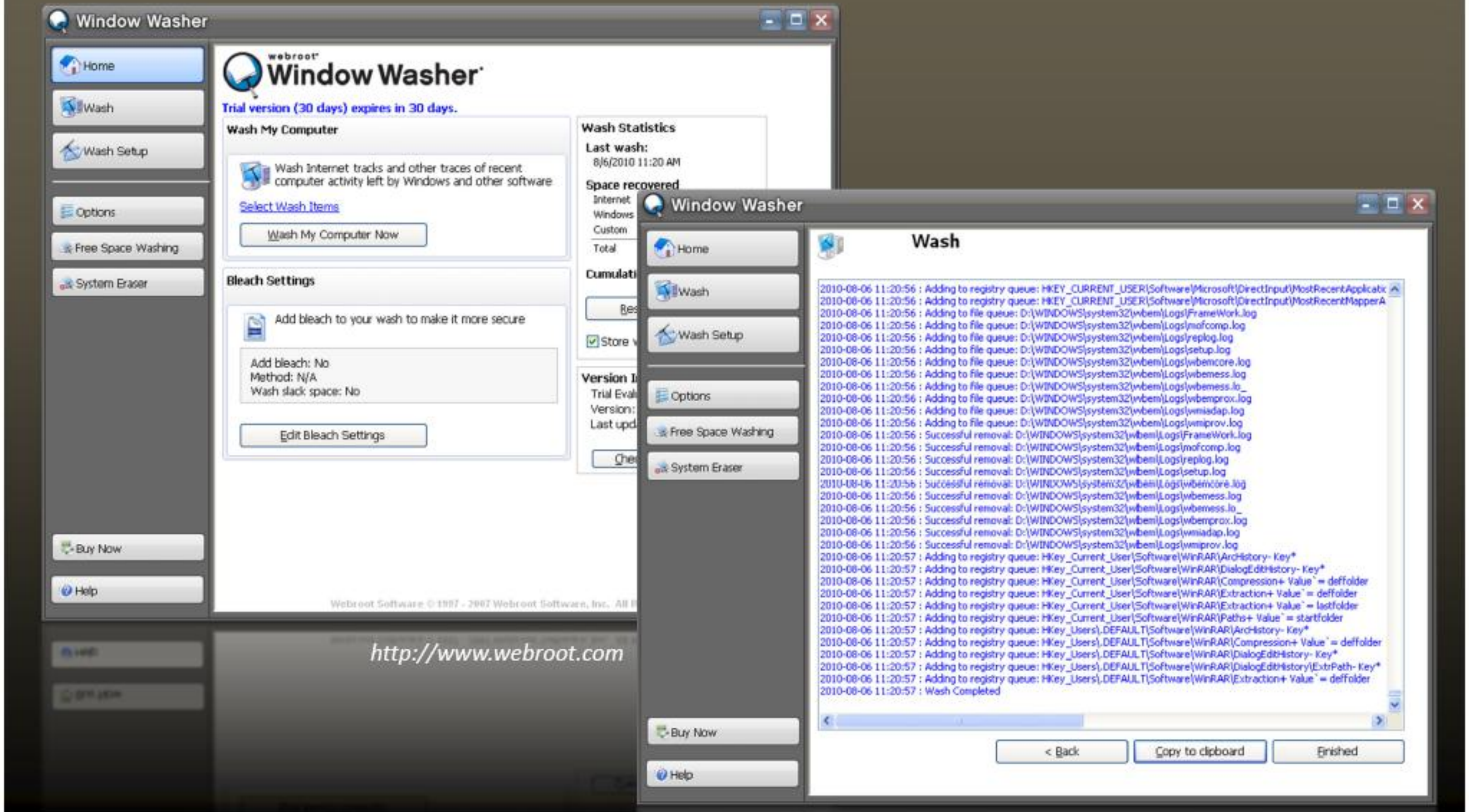
- Intruders will disable auditing immediately after gaining administrator privileges
- At the end of their stay, the intruders will just turn on auditing again using auditpol.exe



```
D:\>auditpol.exe /enable
Running ...

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

(X) Audit Enabled

AuditCategorySystem               = No
AuditCategoryLogon                = No
AuditCategoryObjectAccess         = No
AuditCategoryPrivilegeUse         = No
AuditCategoryDetailedTracking     = No
AuditCategoryPolicyChange         = No
AuditCategoryAccountManagement    = No
Unknown                           = No
Unknown                           = No

D:\>auditpol.exe /disable
Running ...

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

(0) Audit Disabled

AuditCategorySystem               = No
AuditCategoryLogon                = No
AuditCategoryObjectAccess         = No
AuditCategoryPrivilegeUse         = No
AuditCategoryDetailedTracking     = No
AuditCategoryPolicyChange         = No
AuditCategoryAccountManagement    = No
Unknown                           = No
Unknown                           = No

D:\>_
```

http://www.microsoft.com

Covering Tracks Tool: Window Washer



Trial version (30 days) expires in 30 days.

Wash My Computer

Wash Internet tracks and other traces of recent computer activity left by Windows and other software

Bleach Settings

Add bleach to your wash to make it more secure

Add bleach: No
Method: N/A
Wash slack space: No

Wash Statistics

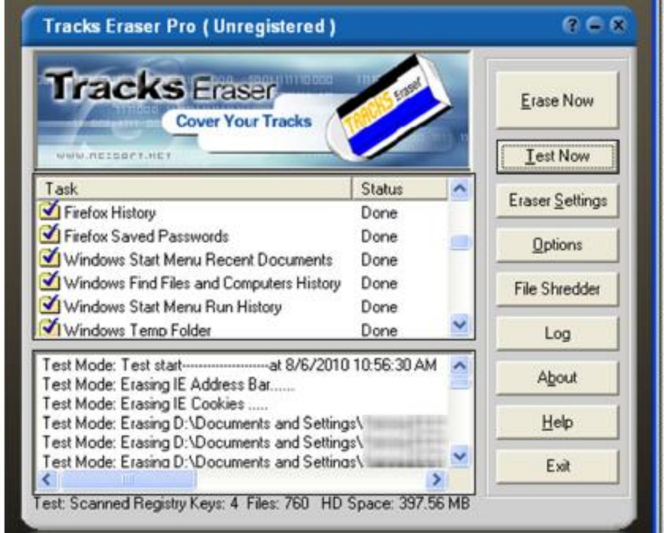
Last wash:
8/6/2010 11:20 AM

Space recovered
Internet
Windows
Custom
Total

```
2010-08-06 11:20:56 : Adding to registry queue: HKEY_CURRENT_USER\Software\Microsoft\DirectInput\MostRecentApplicatic
2010-08-06 11:20:56 : Adding to registry queue: HKEY_CURRENT_USER\Software\Microsoft\DirectInput\MostRecentMapperA
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\FrameWork.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\mofcomp.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\replog.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\setup.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wbemcore.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wbemess.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wbemess.lo_
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wbemprox.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wmiadap.log
2010-08-06 11:20:56 : Adding to file queue: D:\WINDOWS\system32\wbem\Logs\wmiprov.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\FrameWork.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\mofcomp.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\replog.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\setup.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wbemcore.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wbemess.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wbemess.lo_
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wbemprox.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wmiadap.log
2010-08-06 11:20:56 : Successful removal: D:\WINDOWS\system32\wbem\Logs\wmiprov.log
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\ArcHistory- Key*
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\DialogEditHistory- Key*
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\Compression+ Value`= deffolder
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\Extraction+ Value`= deffolder
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\Extraction+ Value`= lastfolder
2010-08-06 11:20:57 : Adding to registry queue: HKey_Current_User\Software\WinRAR\Paths+ Value`= startfolder
2010-08-06 11:20:57 : Adding to registry queue: HKey_Users\.DEFAULT\Software\WinRAR\ArcHistory- Key*
2010-08-06 11:20:57 : Adding to registry queue: HKey_Users\.DEFAULT\Software\WinRAR\Compression+ Value`= deffolder
2010-08-06 11:20:57 : Adding to registry queue: HKey_Users\.DEFAULT\Software\WinRAR\DialogEditHistory- Key*
2010-08-06 11:20:57 : Adding to registry queue: HKey_Users\.DEFAULT\Software\WinRAR\DialogEditHistory\ExtrPath- Key*
2010-08-06 11:20:57 : Adding to registry queue: HKey_Users\.DEFAULT\Software\WinRAR\Extraction+ Value`= deffolder
2010-08-06 11:20:57 : Wash Completed
```

http://www.webroot.com

Covering Tracks Tool: Tracks Eraser Pro

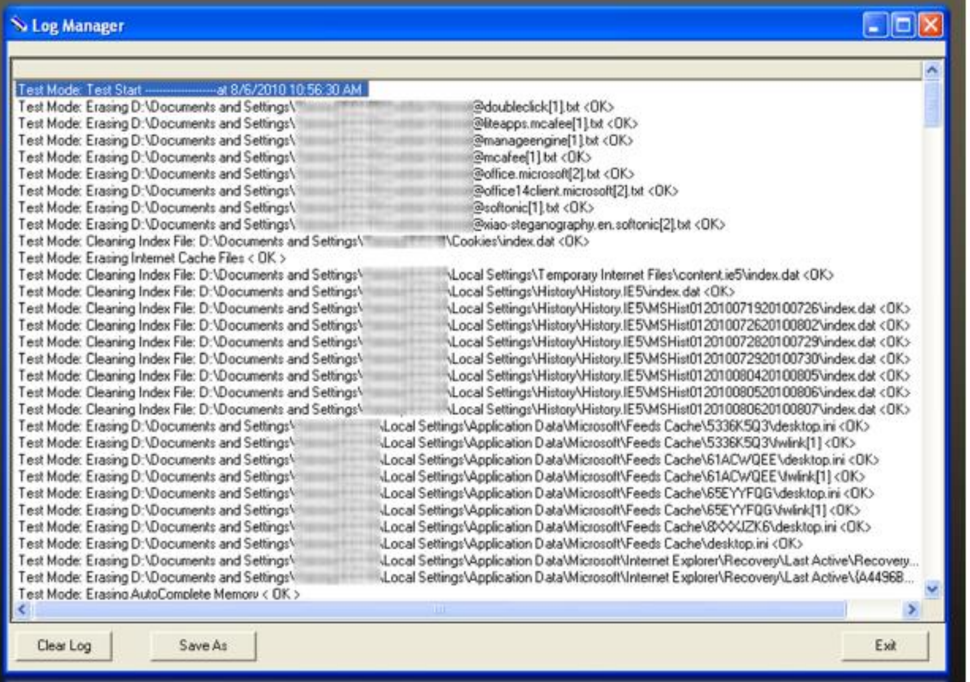


Task	Status
☑ Firefox History	Done
☑ Firefox Saved Passwords	Done
☑ Windows Start Menu Recent Documents	Done
☑ Windows Find Files and Computers History	Done
☑ Windows Start Menu Run History	Done
☑ Windows Temp Folder	Done

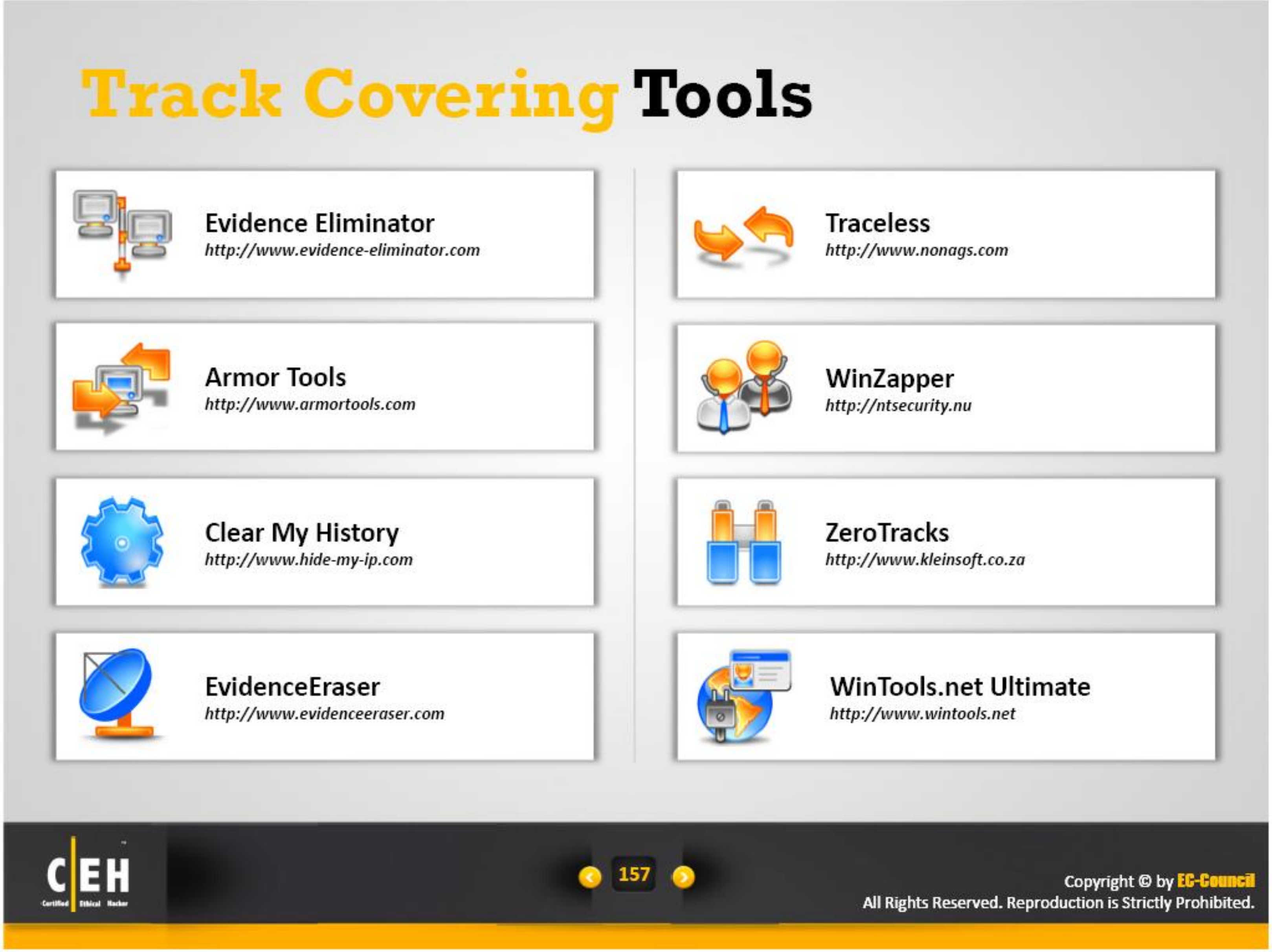
```
Test Mode: Test start--------------------at 8/6/2010 10:56:30 AM
Test Mode: Erasing IE Address Bar......
Test Mode: Erasing IE Cookies .....
Test Mode: Erasing D:\Documents and Settings\[redacted]
Test Mode: Erasing D:\Documents and Settings\
Test Mode: Erasing D:\Documents and Settings\
```

Test: Scanned Registry Keys: 4 Files: 760 HD Space: 397.56 MB

http://www.acesoft.net



```
Test Mode: Test Start --------------------at 8/6/2010 10:56:30 AM
Test Mode: Erasing D:\Documents and Settings\[redacted]@doubleclick[1].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@liteapps.mcafee[1].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@manageengine[1].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@mcafee[1].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@office.microsoft[2].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@office14client.microsoft[2].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@softonic[1].txt <OK>
Test Mode: Erasing D:\Documents and Settings\@xiao-steganography.en.softonic[2].txt <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\[redacted]\Cookies\index.dat <OK>
Test Mode: Erasing Internet Cache Files < OK >
Test Mode: Cleaning Index File: D:\Documents and Settings\[redacted]\Local Settings\Temporary Internet Files\content.ie5\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010071920100726\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010072620100802\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010072820100729\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010072920100730\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010080420100805\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010080520100806\index.dat <OK>
Test Mode: Cleaning Index File: D:\Documents and Settings\Local Settings\History\History.IE5\MSHist012010080620100807\index.dat <OK>
Test Mode: Erasing D:\Documents and Settings\[redacted]\Local Settings\Application Data\Microsoft\Feeds Cache\5336K5Q3\desktop.ini <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\5336K5Q3\fwlink[1] <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\61ACWQEE\desktop.ini <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\61ACWQEE\fwlink[1] <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\65EYYFQG\desktop.ini <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\65EYYFQG\fwlink[1] <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\8XXXJZK6\desktop.ini <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Feeds Cache\desktop.ini <OK>
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\Recovery...
Test Mode: Erasing D:\Documents and Settings\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Last Active\{A44968...
Test Mode: Erasing AutoComplete Memory < OK >
```



Track Covering Tools

Evidence Eliminator
http://www.evidence-eliminator.com

Armor Tools
http://www.armortools.com

Clear My History
http://www.hide-my-ip.com

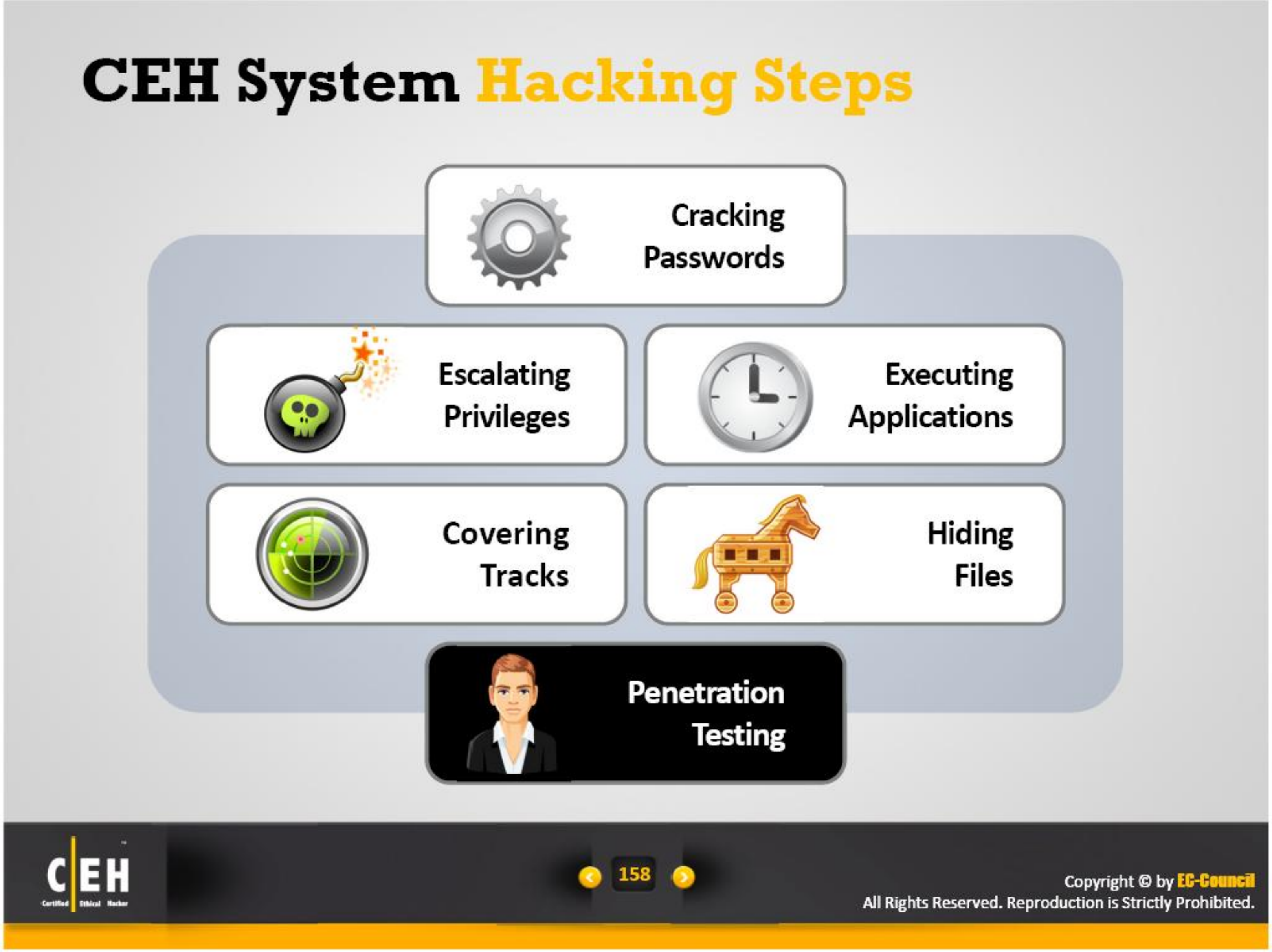
EvidenceEraser
http://www.evidenceeraser.com

Traceless
http://www.nonags.com

WinZapper
http://ntsecurity.nu

ZeroTracks
http://www.kleinsoft.co.za

WinTools.net Ultimate
http://www.wintools.net



CEH System Hacking Steps

Cracking Passwords

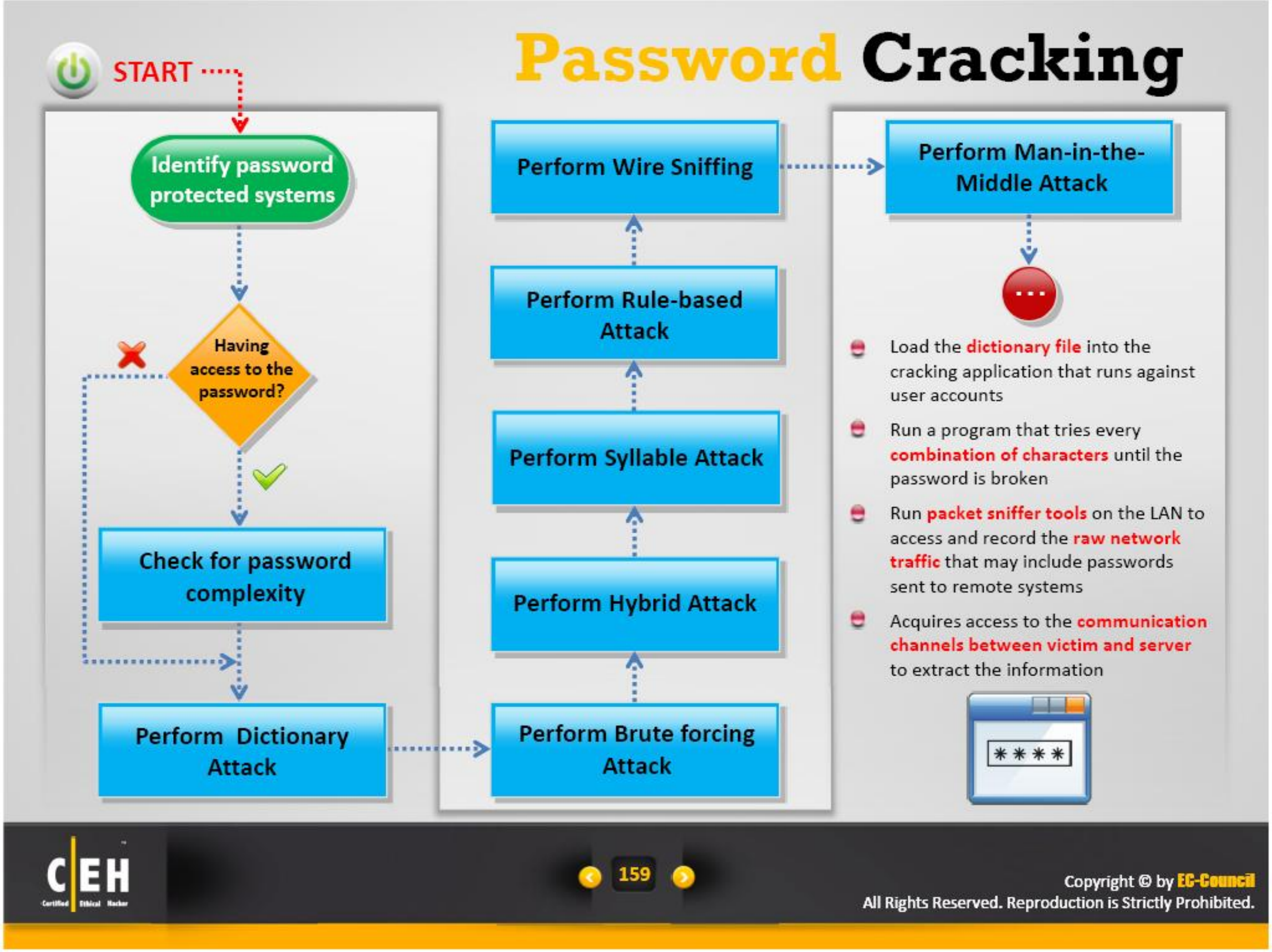
Escalating Privileges

Executing Applications

Covering Tracks

Hiding Files

Penetration Testing



Password Cracking

START

Identify password protected systems

Having access to the password?

✗

✓

Check for password complexity

Perform Dictionary Attack

Perform Brute forcing Attack

Perform Hybrid Attack

Perform Syllable Attack

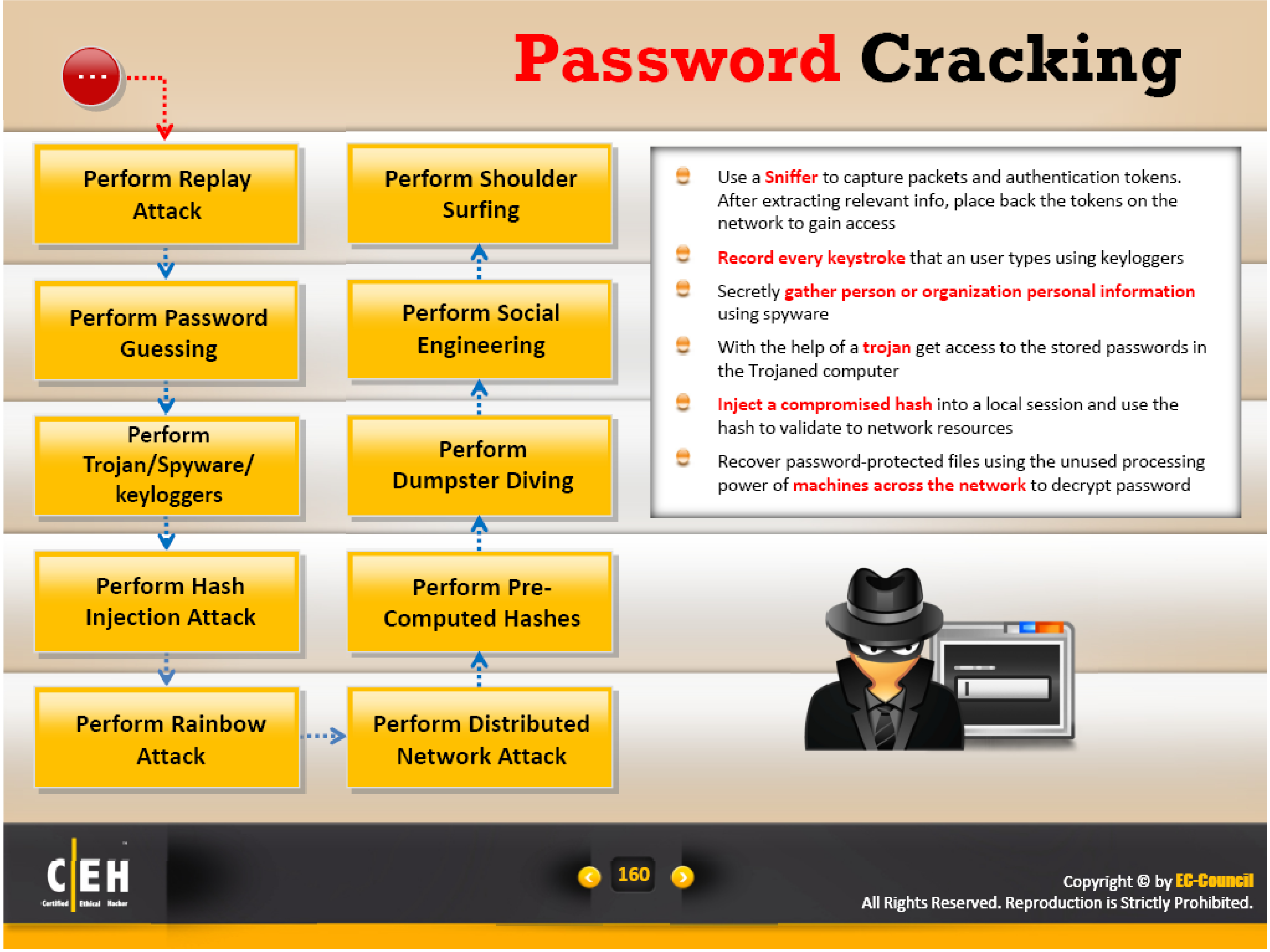
Perform Rule-based Attack

Perform Wire Sniffing

Perform Man-in-the-Middle Attack

...

- Load the **dictionary file** into the cracking application that runs against user accounts
- Run a program that tries every **combination of characters** until the password is broken
- Run **packet sniffer tools** on the LAN to access and record the **raw network traffic** that may include passwords sent to remote systems
- Acquires access to the **communication channels between victim and server** to extract the information



Password Cracking

Perform Replay Attack

Perform Password Guessing

Perform Trojan/Spyware/ keyloggers

Perform Hash Injection Attack

Perform Rainbow Attack

Perform Distributed Network Attack

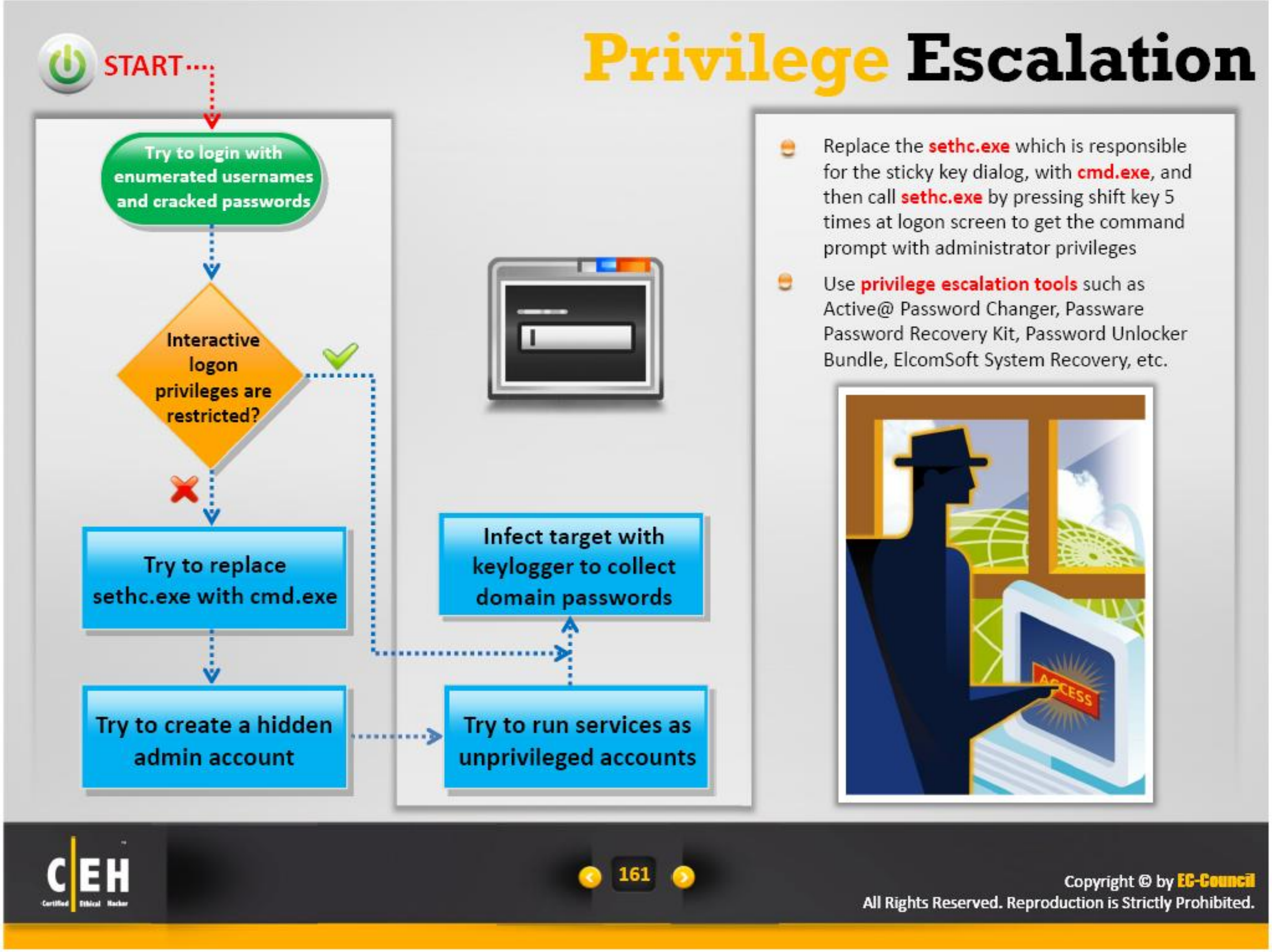
Perform Pre-Computed Hashes

Perform Dumpster Diving

Perform Social Engineering

Perform Shoulder Surfing

- Use a **Sniffer** to capture packets and authentication tokens. After extracting relevant info, place back the tokens on the network to gain access
- **Record every keystroke** that an user types using keyloggers
- Secretly **gather person or organization personal information** using spyware
- With the help of a **trojan** get access to the stored passwords in the Trojaned computer
- **Inject a compromised hash** into a local session and use the hash to validate to network resources
- Recover password-protected files using the unused processing power of **machines across the network** to decrypt password



Privilege Escalation

START

Try to login with enumerated usernames and cracked passwords

Interactive logon privileges are restricted?

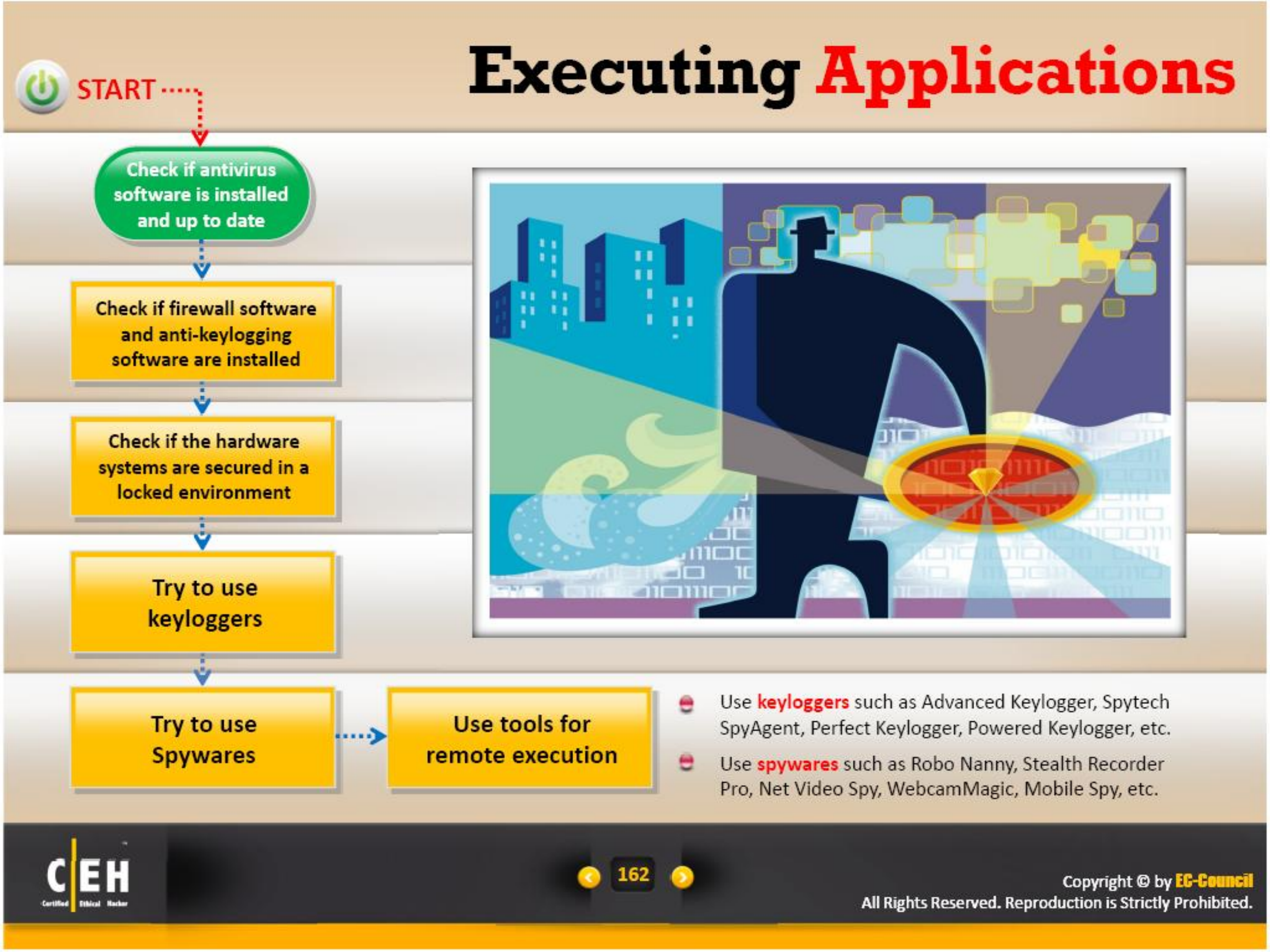
Try to replace sethc.exe with cmd.exe

Try to create a hidden admin account

Try to run services as unprivileged accounts

Infect target with keylogger to collect domain passwords

- Replace the **sethc.exe** which is responsible for the sticky key dialog, with **cmd.exe**, and then call **sethc.exe** by pressing shift key 5 times at logon screen to get the command prompt with administrator privileges
- Use **privilege escalation tools** such as Active@ Password Changer, Passware Password Recovery Kit, Password Unlocker Bundle, ElcomSoft System Recovery, etc.



Executing Applications

START

Check if antivirus software is installed and up to date

Check if firewall software and anti-keylogging software are installed

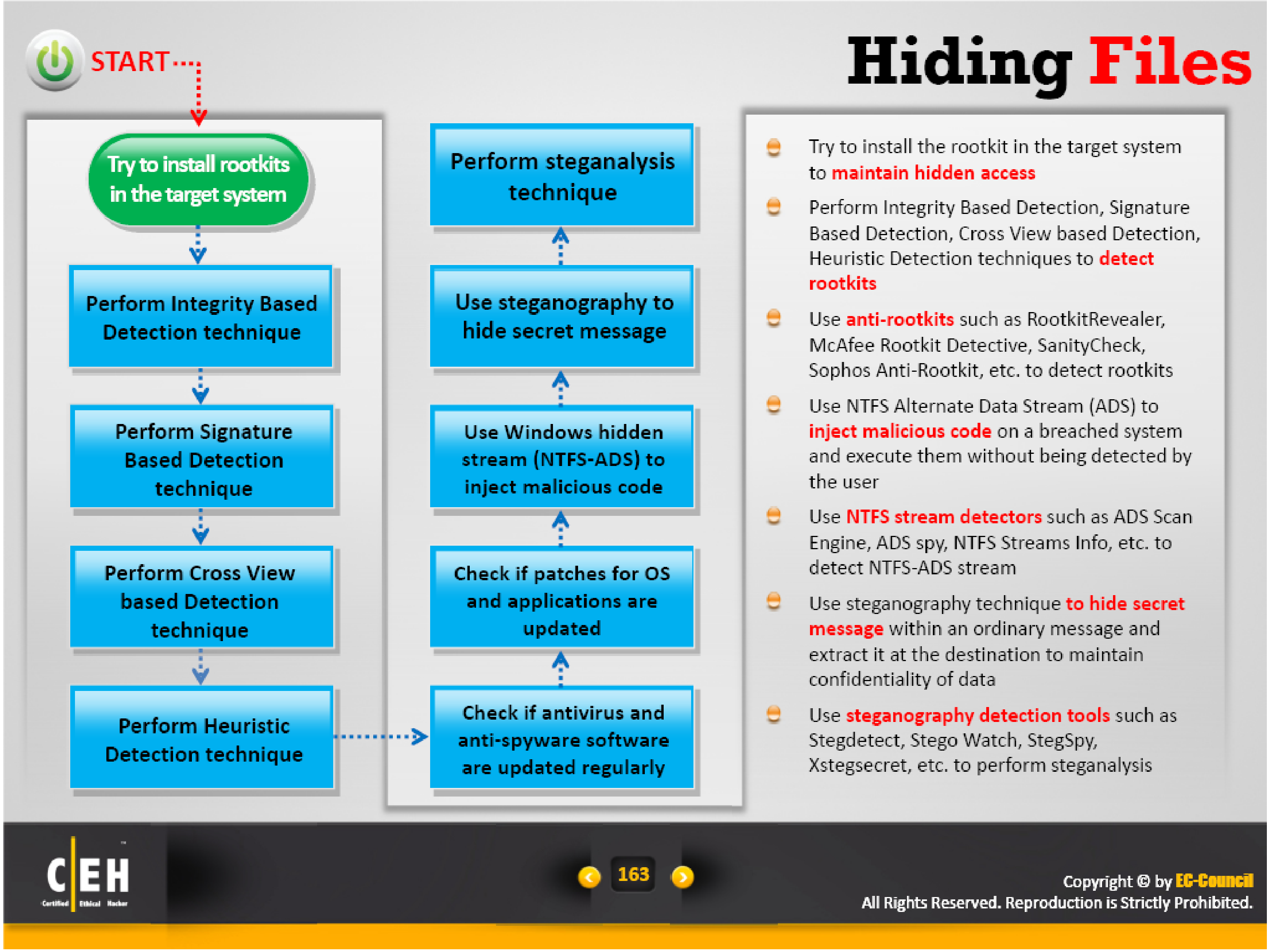
Check if the hardware systems are secured in a locked environment

Try to use keyloggers

Try to use Spywares

Use tools for remote execution

- Use **keyloggers** such as Advanced Keylogger, Spytech SpyAgent, Perfect Keylogger, Powered Keylogger, etc.
- Use **spywares** such as Robo Nanny, Stealth Recorder Pro, Net Video Spy, WebcamMagic, Mobile Spy, etc.



Hiding Files

START

Try to install rootkits in the target system

Perform Integrity Based Detection technique

Perform Signature Based Detection technique

Perform Cross View based Detection technique

Perform Heuristic Detection technique

Check if antivirus and anti-spyware software are updated regularly

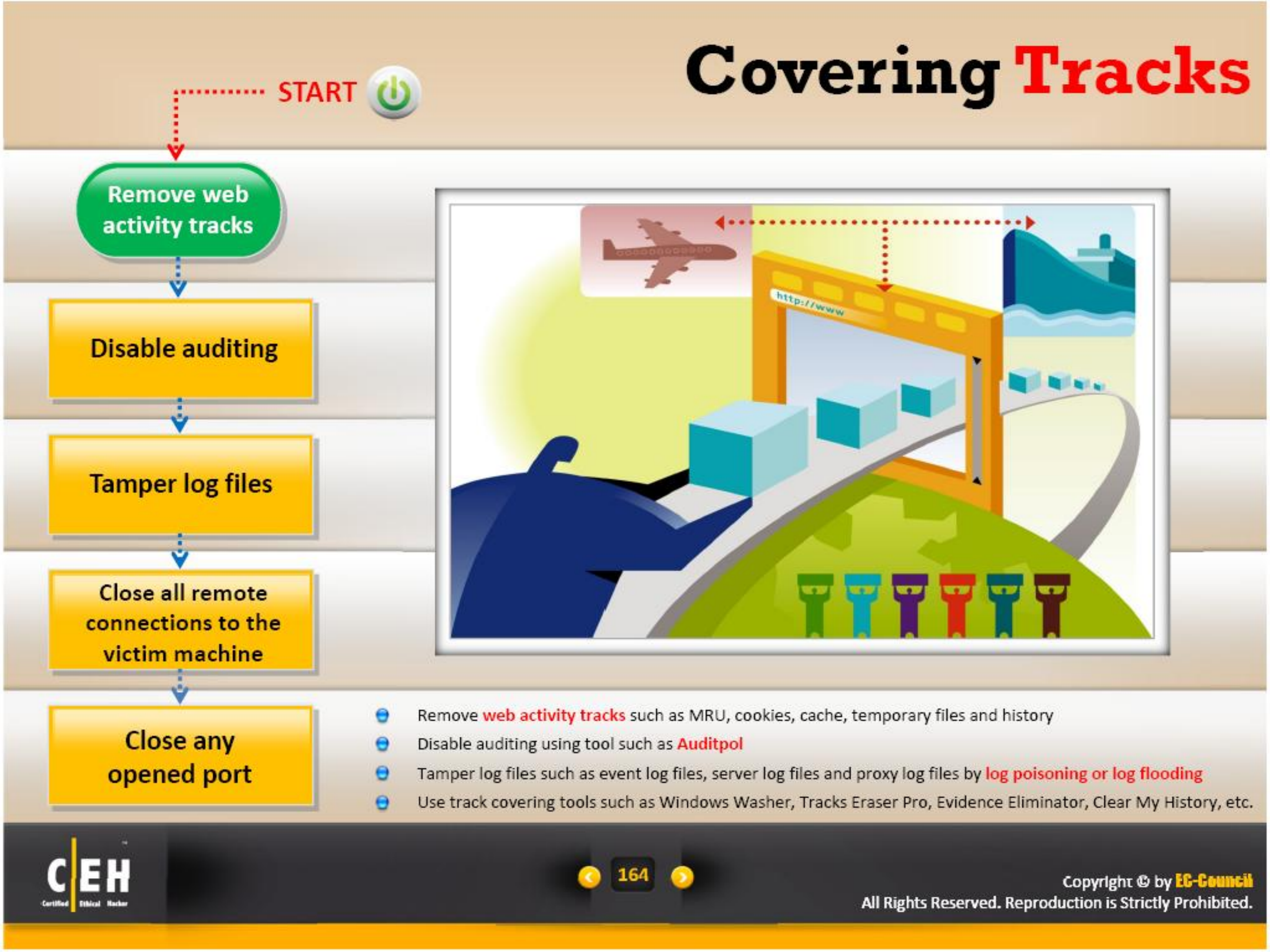
Check if patches for OS and applications are updated

Use Windows hidden stream (NTFS-ADS) to inject malicious code

Use steganography to hide secret message

Perform steganalysis technique

- Try to install the rootkit in the target system to **maintain hidden access**
- Perform Integrity Based Detection, Signature Based Detection, Cross View based Detection, Heuristic Detection techniques to **detect rootkits**
- Use **anti-rootkits** such as RootkitRevealer, McAfee Rootkit Detective, SanityCheck, Sophos Anti-Rootkit, etc. to detect rootkits
- Use NTFS Alternate Data Stream (ADS) to **inject malicious code** on a breached system and execute them without being detected by the user
- Use **NTFS stream detectors** such as ADS Scan Engine, ADS spy, NTFS Streams Info, etc. to detect NTFS-ADS stream
- Use steganography technique **to hide secret message** within an ordinary message and extract it at the destination to maintain confidentiality of data
- Use **steganography detection tools** such as Stegdetect, Stego Watch, StegSpy, Xstegsecret, etc. to perform steganalysis



Covering Tracks

START

Remove web activity tracks

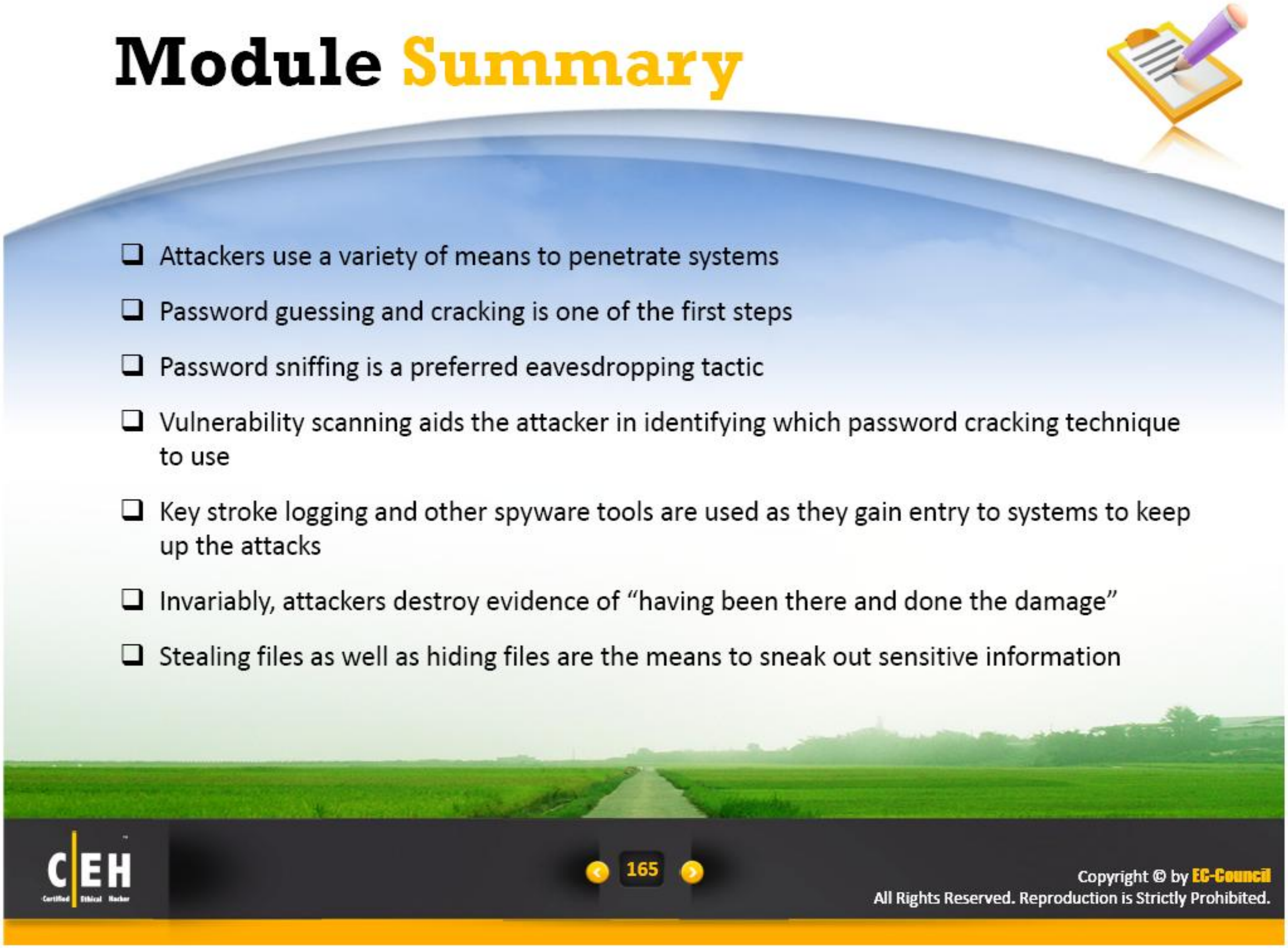
Disable auditing

Tamper log files

Close all remote connections to the victim machine

Close any opened port

- Remove web activity tracks such as MRU, cookies, cache, temporary files and history
- Disable auditing using tool such as Auditpol
- Tamper log files such as event log files, server log files and proxy log files by log poisoning or log flooding
- Use track covering tools such as Windows Washer, Tracks Eraser Pro, Evidence Eliminator, Clear My History, etc.



Module Summary

- ❑ Attackers use a variety of means to penetrate systems
- ❑ Password guessing and cracking is one of the first steps
- ❑ Password sniffing is a preferred eavesdropping tactic
- ❑ Vulnerability scanning aids the attacker in identifying which password cracking technique to use
- ❑ Key stroke logging and other spyware tools are used as they gain entry to systems to keep up the attacks
- ❑ Invariably, attackers destroy evidence of "having been there and done the damage"
- ❑ Stealing files as well as hiding files are the means to sneak out sensitive information

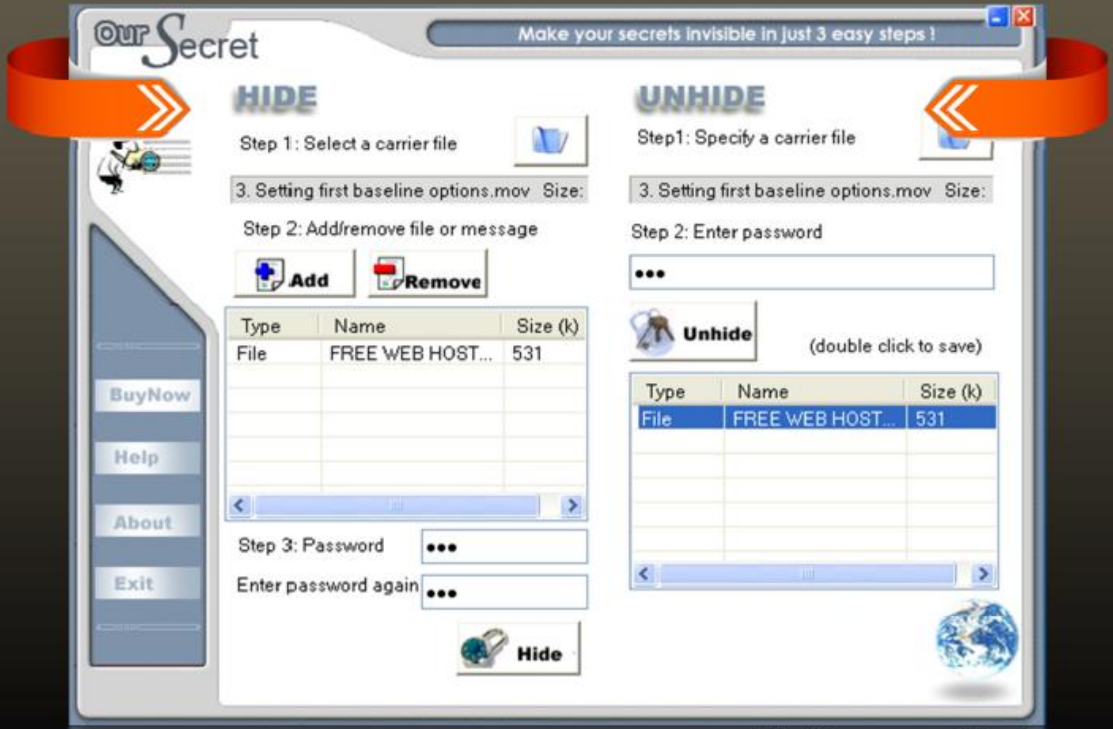
Quotes

> “A lot of hacking is playing with other people, you know, getting them to do strange things.”

- **Steve Wozniak**,
Computer Engineer and
Co-founder, Apple
Computer, Inc.

Video Steganography: Our Secret

In video steganography, the information is hidden in video files of different formats such as .AVI, .MPG4, .WMV, etc.



HIDE

Step 1: Select a carrier file

3. Setting first baseline options.mov Size:

Step 2: Add/remove file or message

Add Remove

Type	Name	Size (k)
File	FREE WEB HOST...	531

Step 3: Password •••

Enter password again •••

Hide

UNHIDE

Step1: Specify a carrier file

3. Setting first baseline options.mov Size:

Step 2: Enter password

•••

Unhide (double click to save)

Type	Name	Size (k)
File	FREE WEB HOST...	531

http://www.securekit.net