

Threat Events: Software Attacks (cont.)

➤ INFORMATION – cont.

STEALER

- 2) **Memory (RAM) Scraper** – steals data when processed in memory

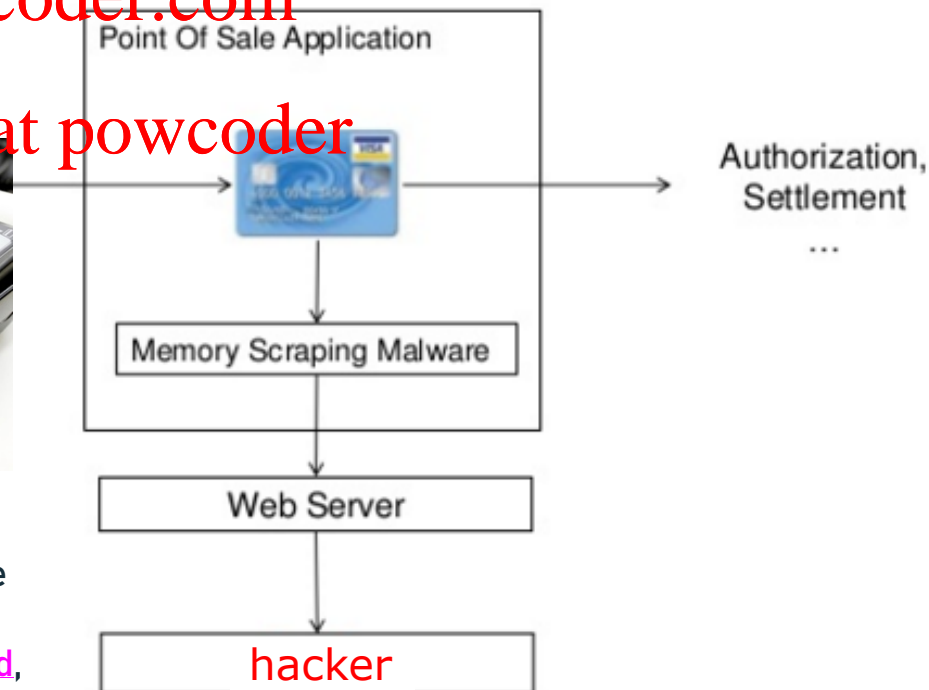
Assignment Project Exam Help
Desired project to steal data everything is decrypted

<https://powcoder.com>

Add WeChat powcoder



The payment card industry has a set of data security standards known as **PCI-DSS**. These standards require end-to-end encryption of sensitive payment data when it is **transmitted**, **received** or **stored**.



Threat Events: Software Attacks (cont.)

➤ INFORMATION – cont. STEALER

3) **Desktop Recorder** – takes screenshots of the desktop (e.g.) when mouse clicked or keyboard pressed

disadvantage: amount of that that needs to be stored / transmitted
<https://powcoder.com>

Add WeChat powcoder



Threat Events: Software Attacks (cont.)

- **RANSOMWARE** – holds data or access to systems containing data until the victim pays a ransom

- ◆ subcategories of ransomware based on

Assignment Project Exam Help

1) **CryptoLockers** – encrypts victim's data or entire hard-drive get encrypted
<https://powcoder.com>

Add WeChat powcoder

2) **ScreenLockers** – user is locked out and denied login to the system





Your computer has been locked!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)

18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)

18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to \$250,000.

Technical details:

Involved IP address: [REDACTED]

Involved host name: [REDACTED]

Source or intermediary sites: <http://pornerbros.com>

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of \$300.

HOW TO UNLOCK YOUR COMPUTER:

1

\$

Take your cash to one of this retail locations:

Walmart

CVS pharmacy

Kmart

Walgreens

7-Eleven

2

Get a MoneyPak and purchase it with cash at the register

3

Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code:

Submit

1	2	3
4	5	6
7	8	9
Delete	0	Enter

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Threat Events: Software Attacks (cont.)

- **SCAREWARE** – malicious programs that aim to scare users into installing a program and sometimes even paying for it

Assignment Project Exam Help
♦ program is 'supposed' to solve a problem that does not exist!

<https://powcoder.com>

Add WeChat powcoder



Threat Events: Software Attacks (cont.)

- **SPYWARE** – software that spies on users by gathering information without their consent, thus violating their privacy

Assignment Project Exam Help
➤ example: ZoneAlarm – transmits detailed information to advertisers about Web sites you visit

<https://powcoder.com>
➤ legal spyware – parental monitoring of Internet usage by children

Add WeChat powcoder



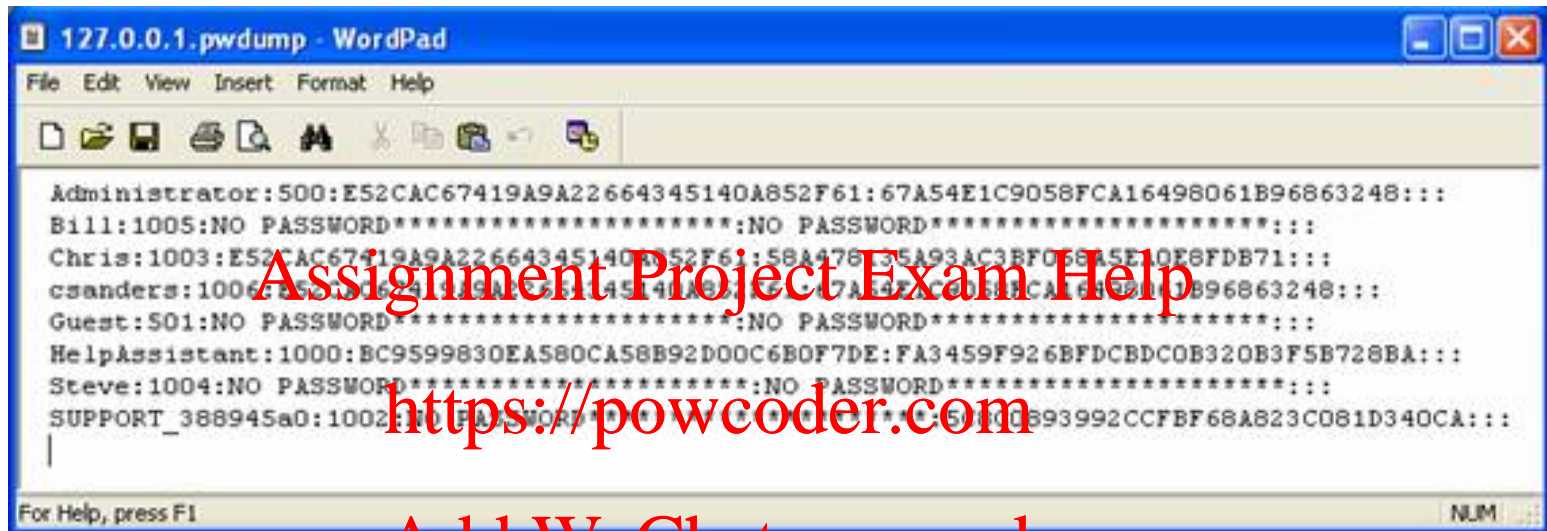
- **ADWARE** – software that delivers advertising content in a manner that is unexpected and unwanted by the user

Threat Events: Software Attacks (cont.)

b) Password Cracking

- ◆ can be 'on-line' and 'off-line'
- ◆ **off-line** crackers attempt to reverse-calculate a password
- ◆ requires that a copy of Security Account Manager (SAM)
 - a registry data file - be obtained
 - **SAM file** (c:\windows\system32\config\SAM) contains the hashed representation of the user's password – LM or NTLM hash algorithms are used
 - cracking procedure: hash any random password using the same algorithm, and then compare to the SAM file's entries
 - SAM file is locked when Windows is running: cannot be opened, copied or removed (unless **pwdump** is run by the administrator)
 - off-line copy of SAM's content can be obtained (e.g.) by booting the machine on an alternate OS such as NTFSDOS or Linux

Threat Events: Software Attacks (cont.)



```
Administrator:500:E52CAC67419A9A22664345140A852F61:67A54E1C9058FCA16498061B96863248:::  
Bill:1005:NO PASSWORD*****:NO PASSWORD*****::  
Chris:1003:E52CAC67419A9A22664345140A852F61:58A478135A93AC3BFC68A5E10E8FDB71:::  
csanders:1006:E52CAC67419A9A22664345140A852F61:7A442AC3BFC68A5E10E8FDB71:896863248:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****::  
HelpAssistant:1000:BC9599830EA580CA58B92D00C6B0F7DE:FA3459F926BFDCBDCOB320B3F5B728BA:::  
Steve:1004:NO PASSWORD*****:NO PASSWORD*****::  
SUPPORT_388945a0:1002:NO PASSWORD*****:5A00B93992CCFBF68A823C081D340CA:::
```

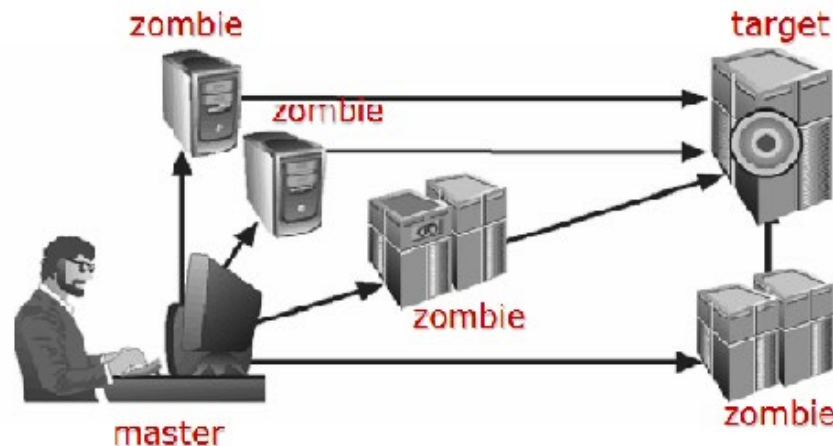
Add WeChat powcoder

- ◆ types of password cracking attacks
 - **brute force** – every possible combination/password is tried
 - **dictionary** – a list of commonly used passwords (the dictionary) is used
 - **guessing** – the attacker uses his/her knowledge of the user's personal information and tries to guess the password

Threat Events: Software Attacks (cont.)

c) Denial of Service (DoS)

- ◆ attacker sends a large number of requests to a target
 - target gets overloaded and cannot respond to legitimate requests
- ◆ **distributed DoS = DDos** - a coordinated stream of requests is launched from many locations (zombies) simultaneously
 - **zombie/bot** - a compromised machine that can be commanded remotely by the master machine
 - **botnet** - network of bots + master machine



Threat Events: Software Attacks (cont.)

◆ DDoS ‘as a service’

“Given the ready availability of DDoS as a service offerings and the increasing affordability of such services, organizations of all sizes and industries are at a greater risk than ever of falling victim to a DDoS attack that can cripple network availability and productivity.”

<http://securityaffairs.co/wordpress/33916/cyber-crime/verisign-ddos-attacks-as-a-service.html>

Service Name	Service Pricing (USD)
Xakepy.cc	1 hour starts at \$5 24 hours starts at \$30 1 week starts at \$200 1 month starts at \$800
World DDoS Service	1 day starts at \$50 1 week starts at \$300 1 month starts at \$1,200
King's DDoS Service	1 hour starts at \$5 12 hours starts at \$25 24 hours starts at \$50 1 week starts at \$500 1 month starts at \$1,500
MAD DDoS Service	1 night starts at \$35 1 week starts at \$180 1 month starts at \$500
Gwapo's Professional DDoS Service	1-4 hours at \$2 per hour 5-24 hours at \$4 per hour 24-72 hours at \$5 per hour 1 month at \$1,000 fixed
PsyCho DDoS Service	1 hour for \$6 1 night for \$60 1 week for \$380 1 month for \$900
DDoS Service 911	1 night for \$50
Blaiz DDoS Service	1 day for \$70 1 week starts at \$450
Critical DDoS Service	1 day starts at \$50 1 week starts at \$300 1 month starts at \$900
No. 1* DDoS_SERVICE	1 day starts at \$50 1 week starts at \$300 1 month starts at \$1,000

Threat Events: Software Attacks (cont.)

Example: Mafiaboy story - DDoS

In 2000, a number of major firms were subjected to devastatingly effective distributed denial-of-service (DDoS) attack that blocked each of their e-commerce systems for hours at a time. Victims of this series of attacks included: CNN.com, eBay, Yahoo.com, Amazon.com, Dell.com, ZDNet, and other firms.

The Yankee Group estimated that these attacks cost \$1.2 billion in 48 hours:

\$100 million from lost revenue

\$100 million from the need to create tighter security

\$1 billion in combined market capitalization loss.

At first, the attack was thought to be the work of an elite hacker, but it turned to be orchestrated by a 15-year-old hacker in Canada.

He was sentenced to eight months detention plus one year probation and \$250 fine.

http://journal.fibreculture.org/issue9/issue9_genosko.html

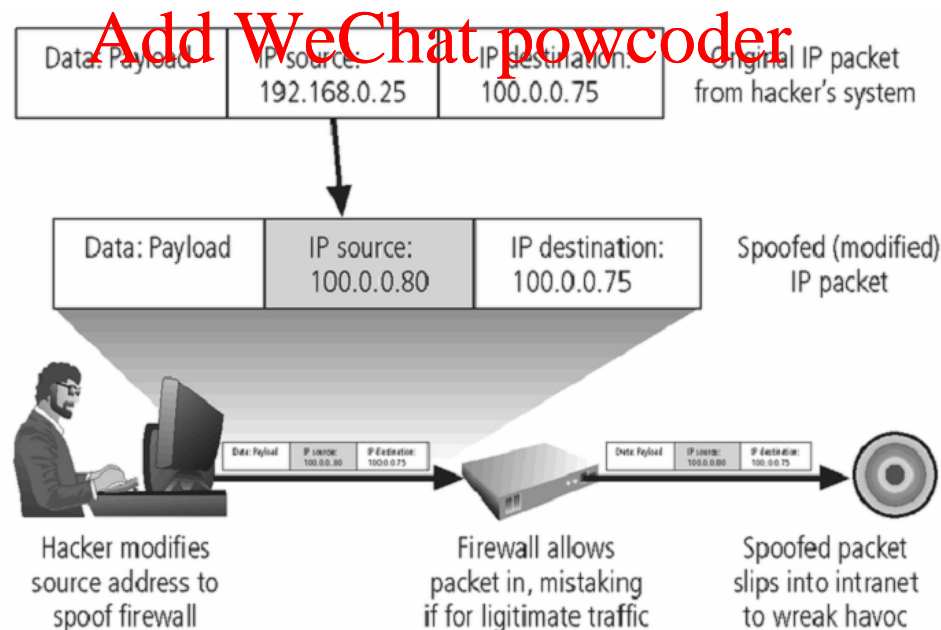
Threat Events: Software Attacks (cont.)

d) Spoofting

- ◆ insertion of forged **Internet identification data** in order to gain an illegitimate advantage

- ◆ types of spoofing

- IP Spoofing – creation of IP packets with a forged source IP address, e.g. for the purpose of 'passing through a firewall'



Threat Events: Software Attacks (cont.)

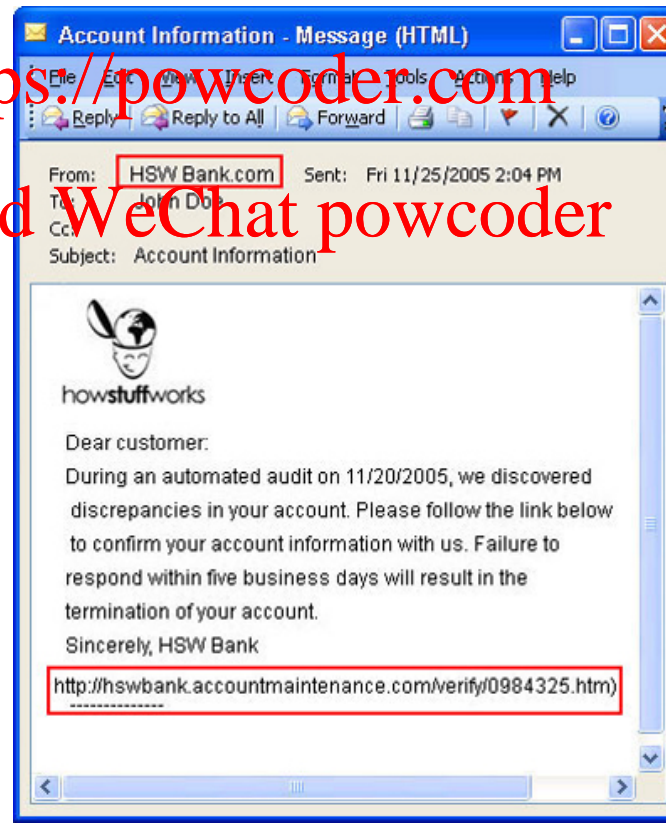
❖ types of spoofing (cont.)

- Email Address Spoofing – creation of email messages with a forged sender address, e.g. for the purposes of social engineering and data phishing

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



Threat Events: Software Attacks (cont.)

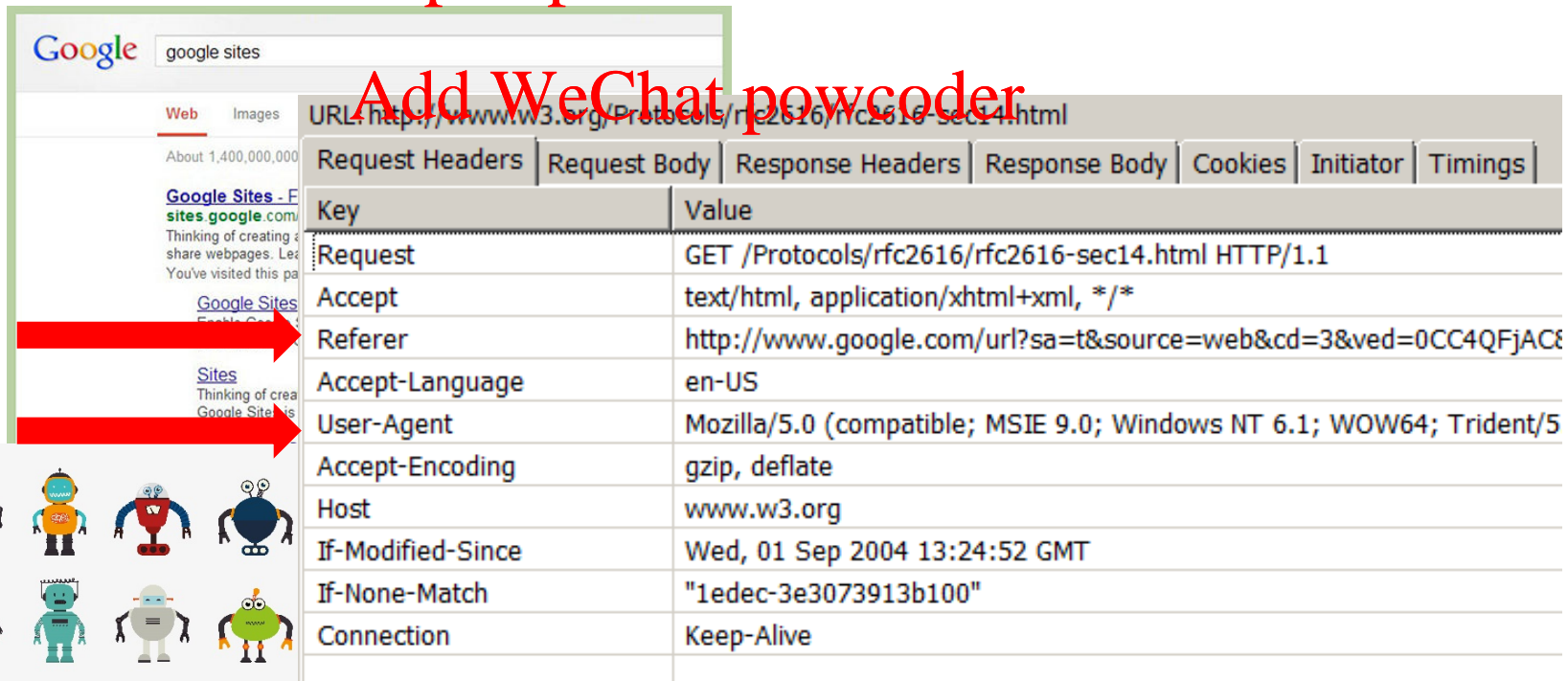
◆ types of spoofing (cont.)

- Referrer or User Agent Spoofing – creation of HTTP requests with forged fields in order to gain access to a protected web-site

* some sites allow access to their material only from certain approved (login) pages and/or only to humans

<https://powcoder.com>

Add WeChat powcoder



Key	Value
Request	GET /Protocols/rfc2616/rfc2616-sec14.html HTTP/1.1
Accept	text/html, application/xhtml+xml, */*
Referer	http://www.google.com/url?sa=t&source=web&cd=3&ved=0CC4QFjAC8
Accept-Language	en-US
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5
Accept-Encoding	gzip, deflate
Host	www.w3.org
If-Modified-Since	Wed, 01 Sep 2004 13:24:52 GMT
If-None-Match	"1edec-3e3073913b100"
Connection	Keep-Alive

Threat Events: Software Attacks (cont.)

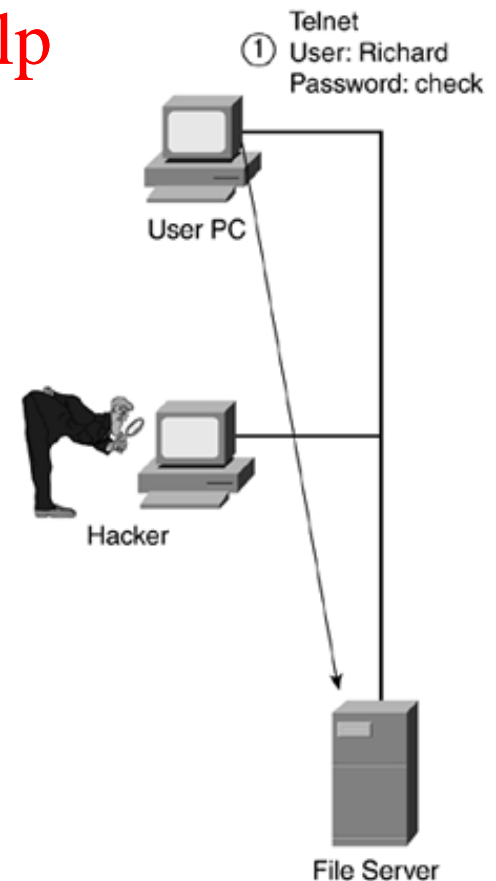
e) Sniffing

- ◆ use of a program or device that can monitor data traveling over a network

- unauthorized sniffers can be very dangerous – they cannot be detected, yet they can sniff/extract critical information from the packets traveling over the network

- wireless sniffing is particularly simple, due to the 'open' nature of the wireless medium

- popular sniffers:
 - Wireshark** – wired medium
 - Cain & Abel** – wireless medium



Threat Events: Software Attacks (cont.)

f) Man-in-the-Middle Attacks

- ◆ gives an illusion that two computers are communicating with each other, when actually they are sending and receiving data with a computer between them

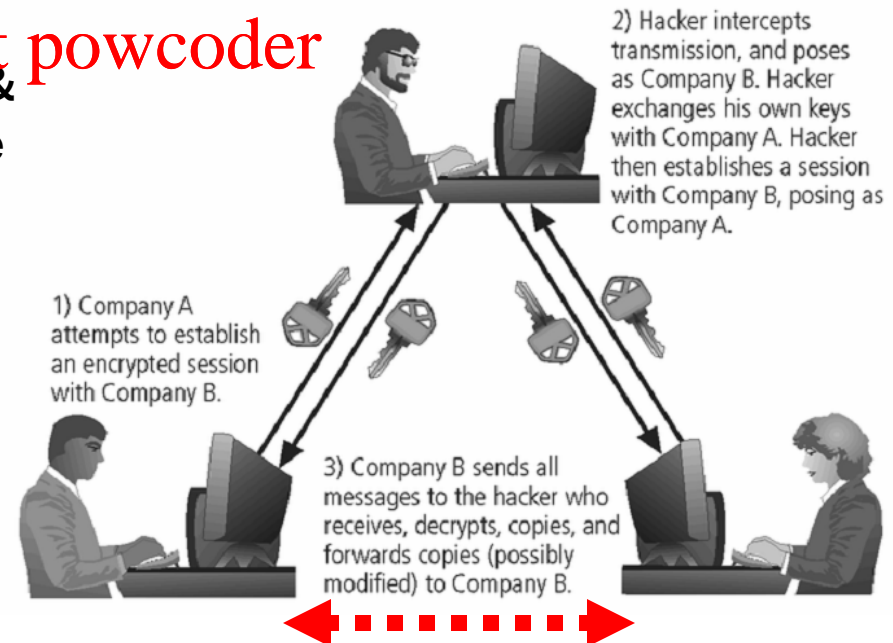
- spoofing and/or sniffing can be involved

<https://powcoder.com>

- ◆ examples:

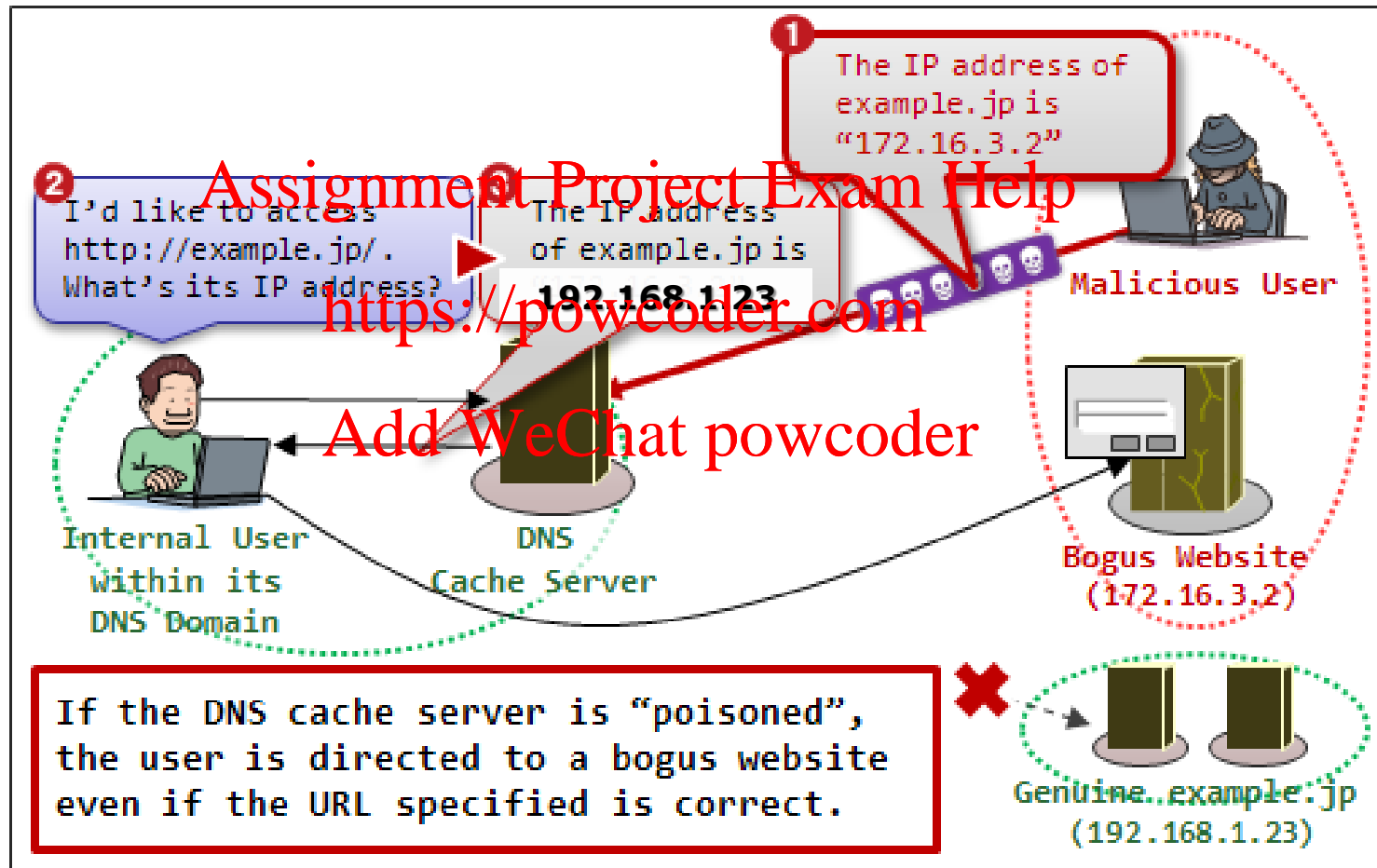
- **passive** – attacker records & resends data at a later time (acts as a signal/packet repeater)

- **active** – attacker intercepts, alters and sends data before or after the original arrives to the recipient



Threat Events: Software Attacks (cont.)

Example: DNS Poisoning (active Man-in-the-Middle attack)



Threat Events: Software Attacks (cont.)

Social Engineering

- ◆ process of using social skills to manipulate people into revealing vulnerable information
 - either by believing that an email came from a legitimate person or believing that a web-site is the real web-site, or both!
<https://powcoder.com>

g) Phishing

- ◆ attempt to gain sensitive personal information by posing as a legitimate entity
 - **SIMPLE PHISHING:** an email is sent to the victim informing them of a problem (e.g. with their email or banking account) and asking them to provide their username, password, etc.;
 - ‘From’ email address is spoofed to look legitimate, ‘Reply To’ email address is an account controlled by the attacker

Threat Events: Software Attacks (cont.)

Example: Simple Phishing



Threat Events: Software Attacks (cont.)

- **SOPHISTICATED PHISHING:** an email is sent to the victim containing a link to a bogus website that looks legitimate

Assignment Project Exam Help

<https://powcoder.com>

Example: Phishing using URL Links Embedded in HTML-based Emails

<http://1example.link.com>

http://53d8b.malicious_phishing_site.com/index.php

Threat Events: Software Attacks (cont.)

Example: Phishing using URL Links Embedded in HTML-based Emails (cont.)

Assignment Project Exam Help
<https://powcoder.com>
Add WeChat powcoder

The image displays a phishing attack. On the left, a screenshot of a GroupWise email client shows a message from 'online@regions.com' dated January 26, 2007, with the subject 'You have 1 new ALERT message'. The email body contains a link to 'Go To RegionsNet'. On the right, a screenshot of a web browser (Mozilla Firefox) shows a fake 'RegionsNET - Online Banking' login page. The page includes a 'Secure Login' section with fields for 'Login ID' and 'Password', and a button labeled 'Access Accounts'. The URL in the address bar is 'http://alienhub.kg.net.pl/regions/regionsnet/EB/login/index.htm', which is a suspicious domain. The page also features a 'Disclaimer' section and a footer with links for 'Copyright Information', 'Privacy Pledge', 'Member FDIC', and 'Equal Housing Lender'.

Threat Events: Software Attacks (cont.)

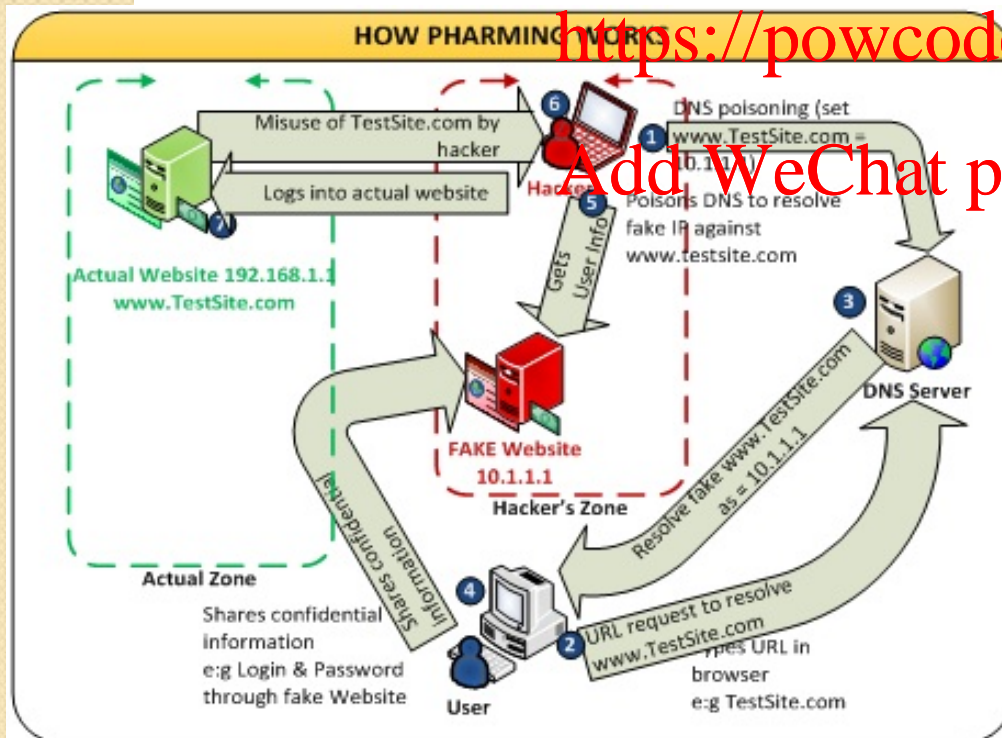


<http://www.informacija.rs/Clanci/Phishing-Obmanjivanje-korisnika.html>

Threat Events: Software Attacks (cont.)

i) Pharming

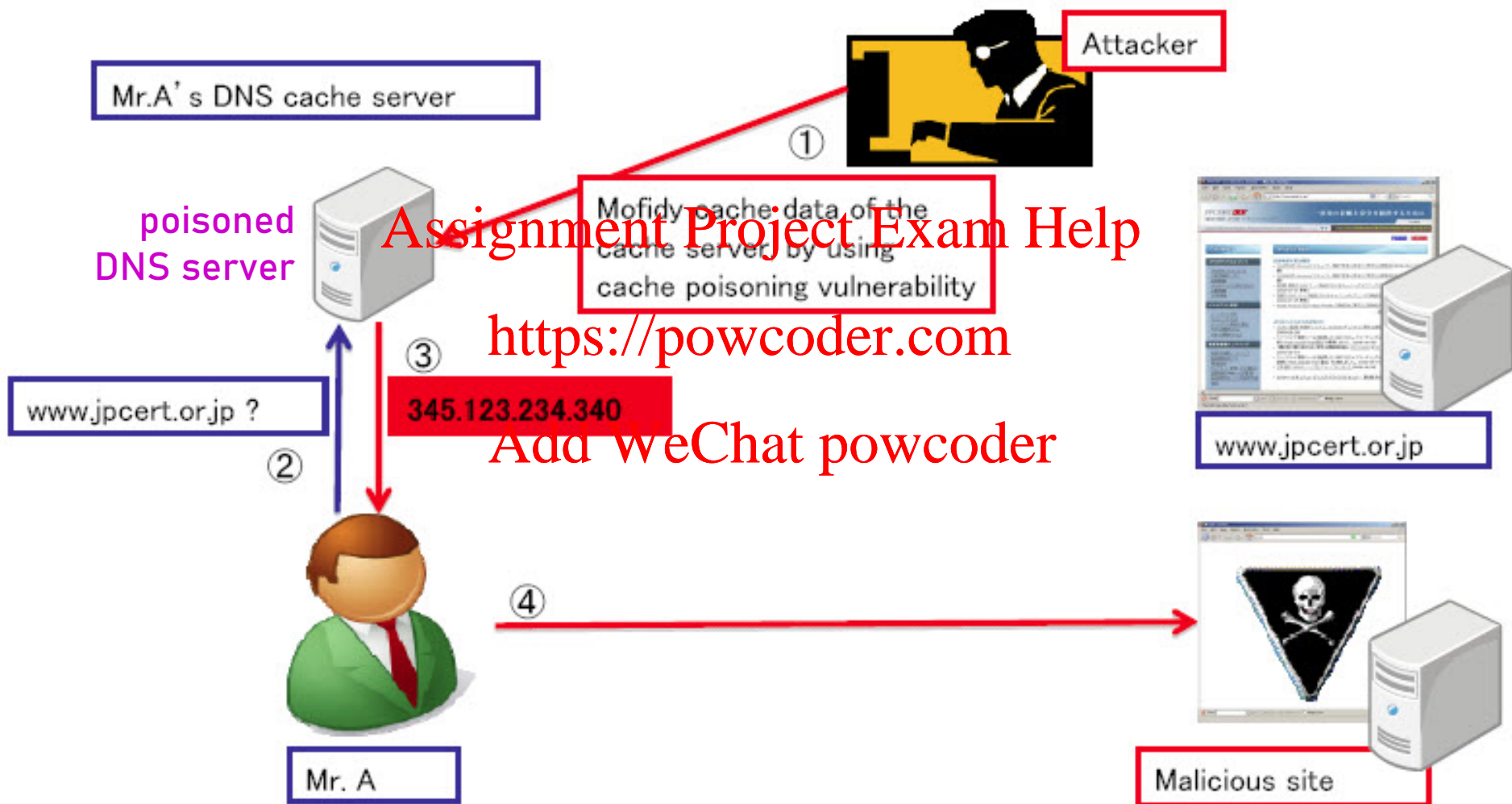
- ❖ phishing is accomplished by getting users to type in or click on a bogus URL
- ❖ pharming redirects users to false website without them even knowing it – typed in or clicked on URL looks OK



- performed through **DNS poisoning** – user's local DNS Cache or DNS server are 'poisoned' by a virus

Overview of DNS cache poisoning vulnerability

What is DNS cache poisoning



Threat Events: Software Attacks (cont.)

- **Biggest Challenge of Information Security** – How much security?!

Information security should balance protection & access
- a completely secure information system would not allow anyone access!

Add WeChat powcoder

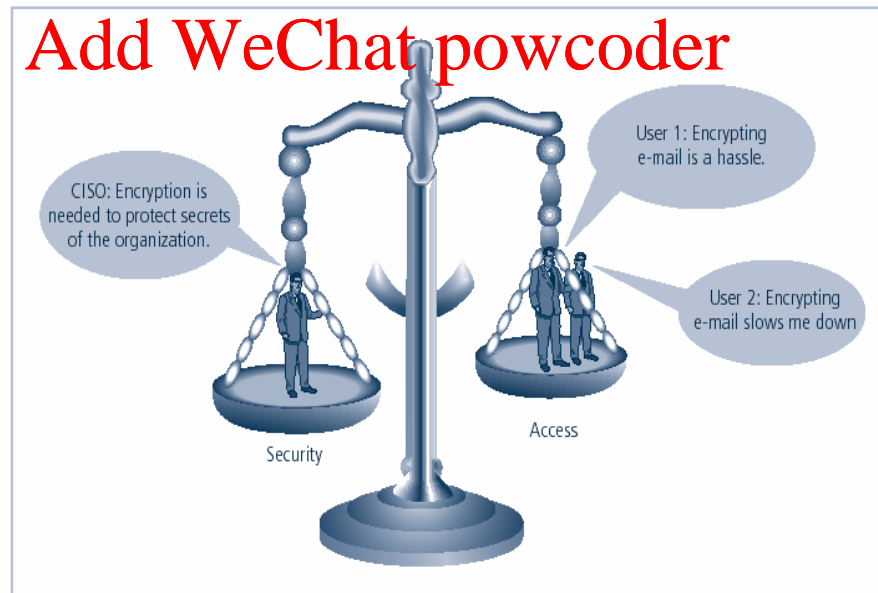


FIGURE 1-7 Balancing Information Security and Access