

Lies, lies and plagiarism

Infosec Institute vs. Corelan

This story starts in September 2010, when a member of the well-known and respected Corelan crew (<http://www.corelan.be>) receives a copy of the lab-book for Infosec Institute's "Expert Penetration Tester" course. Within minutes it is clear that the document is an almost verbatim copy of the Corelan tutorials which are, to date, publicly available on the Corelan website. Tutorials that anybody who has ever had the faintest interest in exploit development has undoubtedly run across. Content, publicly available to the infosec community, that took close to 24 months to develop.

Note that content on the Corelan website is subject to very specific 'Terms of Use', linked to from every page on the website and to be found at <https://www.corelan.be/index.php/terms-of-use/>.

While full-disclosure seemed obvious to many who saw the document - we will prove the case with side-by-side screenshots later in this document - Corelan chose to pursue its copyright in the most civil manner. With Corelan hailing from Europe and Infosec Institute from Chicago in the U.S. they were looking at an expensive process. Copyright law already is a complex matter, even more so in an international context. This largely puts the joke on the party that needs to protect it while giving those infringing upon it plenty of opportunity to get away with it. Not so in the infosec community. We want this to be a clear message that anybody who knowingly and willingly steals content from this community can count on it that it will come out and that it will fly right back in the face, stomach and groin. Hard.

After attracting a Belgian law firm, a registered letter was written and sent to Infosec Institute, informing them of the copyright infringement and making specific requests. This letter remains, to date, unanswered. The letter is distributed together with this document.

Given the international complexity Corelan was advised by the Belgian lawfirm to engage a US-based lawfirm and through its sister firm a second and third registered letter was addressed to Infosec Institute. Both of these letters remain, to date, unanswered. The letters are distributed together with this document.

While the copyright infringement started to get publicly known, attempts were made to get in touch with Infosec Institute with the goal to discuss the matter without the involvement of lawyers. No reply was ever received from the organisation. Either Corelan was being willingly ignored or something was awfully wrong with the online presence of Infosec Institute.

By now, we had moved well into 2011 and no less than \$10,000 had been spent on legal representation. This was also the time that Infosec Institute started to post interviews with well-known researchers on their blog at <http://resources.infosecinstitute.com>. Corelan decided to get in touch with some of those researchers to present them the evidence while asking them the question to, if they believed copyright was infringed, ask Infosec Institute to remove their contributions from the blog. While they are big, we choose not to reveal the names of the persons who supported Corelan. They know who they are and a humble thank you to them is in place. At the same time (ISC)² detected that Infosec Institute was using some of its logos unrightfully. After a few days, the logos were removed. Finally, Infosec Institute decided to get in touch with Corelan and discuss the issue in depth. It was June 2011, well over 9 months after Corelan was informed about the plagiarism and well over 6 months after the first registered letter was sent to Infosec Institute.

Hereafter is a chronological account of the relevant e-mail messages that were exchanged by all parties involved. We have redacted all names as they are not relevant to the case and this is not a personal matter.

=====
From: Infosec Institute

To : Corelan

“[redacted], can we discuss this? We have responded to the legal notices from the law firm in Belgium and got no response back a few months ago, I assumed the matter was closed? Obviously it is not and we would like to assist.

[redacted]”

=====
From : Corelan

To : Infosec Institute

[redacted],

thanks for getting back to us. I've forwarded your e-mail to [redacted] (who owns the corelan content) and am awaiting his response.

I would suggest to set up a conference call in the coming days to discuss further.

In the mean time, do you have a copy of the response you sent to the Belgian legal firm? Was it sent as a registered letter and do you have the confirmation of receipt of that letter?

It would have made sense to reach out to corelan at the moment students notified you of the blatant plagiarism by that trainer. It would have prevented a lot of grief on the corelan side, but we appreciate you reaching out now.

I will get back to you as soon as I talked to [redacted]! In the mean time, I will not pursue publishing of the documents in any shape or form.

Kind Regards,
[redacted]

=====
From : Infosec Institute

To : Corelan

Thanks [redacted]. I sent it via regular mail, I will dig up the letter I sent and send it to you. Basically was the same content as I sent to [redacted]. We would like to work things out, and apologize for the trouble.

[redacted]

=====
From : Corelan

To : Infosec Institute

[redacted],

I hope you realize that answering to an international registered letter from a legal firm with a regular letter sounds a little silly. I'm convinced you did this in good faith though.

You also received a letter after that from a US based firm, which was not replied to either.

I've discussed with [redacted] and he's willing to come to an agreement on the following conditions :

- A public apology with details on how it happened is published
- An agreement is reached where ISI obtains a license for the content that was used for the period it was used. [redacted] expects a reasonable offer from your side on this subject. This license will only cover the period of the abuse and will not grant use of the content from now on forward.
- [redacted] has incurred \$9596 in legal costs for the two letters that were sent to you. [redacted] has all contracts and payment proof for that amount.
- We are provided a copy of the current lab manual for that course (Expert Penetration Testing) as proof that the infringement has stopped.

I have, before we finally got in touch, presented the proof to [redacted] and [redacted], who I believe have both contacted you (or your company) in the past few days. Concurrently I'm talking to [redacted] to raise this issue and they are investigating. I have chosen not to publish any of it yet because I'm sure we can reach a reasonable agreement.

I'm happy to discuss this on the phone somewhere tomorrow. You can reach me on my Belgian Mobile Number [redacted]. [redacted] is attending a conference abroad and will not be reachable until the middle of next week but has authorised me to talk to you on this matter.

Thanks again for reaching out to us, I look forward to talking to you.

=====

From : Infosec Institute
To : Corelan

Thanks [redacted] for this offer. I will have a meeting here and review and get back to you. Can you please give me an overview in your involvement in [redacted]'s site?

I think at the outset we can do points 1 and 2, im not sure about 3 and 4.

The book was used for a single course, with a total of 6 or 7 students, and we never used it after that. Im sure you can confirm this from the guy from [redacted] that reported this to you.

=====

From : Corelan
To : Infosec Institute

[redacted],

I'm not involved in [redacted]'s site at all. I'm just a concerned member of the infosec community and a good friend that offered help to [redacted] to get this out of the way. It would be one thing if [redacted] was asking for an excessive amount of money, he is however looking to recover the costs he incurred to make right what shouldn't have been wrong in the first place.

Bear into mind that the guy has a wife and kid at home and has spent \$10,000 of his

own money to address you, without response.

I'm pretty sure [redacted] doesn't want this to happen, but he is currently busy gathering the funds to file an official lawsuit to protect his content. With the proof being so blatant, I'm inclined to bet that is a sure win.

I got the documents, including the copies from the letters sent to you by his lawyers, from [redacted] himself. I'm not aware of "the guy from [redacted]" you mention.

I wouldn't dare to say that I'd grant a pardon to the guy that raped my kid "only once" ...

Kind Regards,

[redacted]

=====

From : Infosec Institute
To : Corelan

[redacted], I think you are going overboard here claiming we "raped" someone. I find that quite disturbing and frankly out of line. As someone who has witnessed a real life sexual crime, I am deeply offended by your choice of words.

We are more than willing to work this out, but, please be aware that we immediately corrected the issue once we were aware of it. We incurred zero profit, actually, a loss, from this incident and have not profited from [redacted]'s website ever. All students in that class were upset and were refunded or issued a credit. We terminated the contract instructor, and, in our contract we specific that use of copyrighted material is not allowed and have appropriate legal protections into the contract. I am totally willing to make these statements in a court of law and provide documentation and provide a public apology. As you may be aware, in US law, you would be awarded damages equal to potentially three times the profit incurred, which is about $3 \times 0 = 0$. Any reasonably competent attorney would advise [redacted] to settle.

If you really want to help here, I am grateful for it, if you are just looking to pick a fight for the sake of picking a fight, I don't know what the point of us conversing is?

=====

From : Corelan
To : Infosec Institute

[redacted],

I'm pretty sure you understand the use of metaphors in this context. Someone has been trying to get in touch for almost 10 months because you infringed their copyright, I hope you understand a little frustration on this side of the equation.

Let's imagine you found out I used "The shellcoders handbook" verbatim to provide \$3700 courses, how would you feel?

Let's talk tomorrow (call me at any time you are availabe, it's a holiday here in Belgium.), I'm pretty sure this can be worked out.

Cheers,

[redacted]

=====

From : Infosec Institute
To : Corelan

I do completely understand your frustration, and do want to make the situation right. We had responded via snail mail, and I didn't think this was such a serious event, so I assumed that our response was adequate and the matter was closed.

I'll give you a call tomorrow to discuss.

=====

From : Corelan
To : Infosec Institute

[redacted],

I was in expectance of your call yesterday but apparently something got in between plans.

[redacted], as copyright owner, has to defend his copyright (by law) or he will lose it, so he will continue to do so.

You understand that, with the proof at hand, if this goes to court, it is pretty much a lost cause at your end?

I would like you to read up on copyright law. You will quickly notice that the 3x0=0 logic doesn't make much sense in that regard.

It is a little silly that while the wrongdoing lies in your camp, we have to do so much effort to get at least some kind of response from your side. In the mean time, I've worked with [redacted] and [redacted] to notify them of this case. I am also working with several journalists who are most interested in this matter (especially after the Gregory Evans/LIGATT debacle last year and the case of [redacted] and his largely plagiarized book in 2009). I will also, relentlessly, contact anyone who gave interviews to your site to provide them the proof of plagiarism and have them make up their own mind.

I hope we can talk before everybody knows about this.

Cheers,

[redacted]

=====

From : Infosec Institute
To : Corelan

Thanks [redacted]. I was in contact with my attorney about next steps to take. My attorney has advised me to speak with [redacted] over this matter, as he owns the copyright, not you. Can you please provide his contact details (phone number) and we will take it from there?

=====

From : Corelan
To : Infosec Institute

[redacted],

I've talked to [redacted] as he's abroad for business at the moment. He's willing to discuss a proposal from your side based on the four points I already communicated earlier :

- A public apology with details on how it happened is published
- An agreement is reached where ISI obtains a license for the content that was used for the period it was used. [redacted] expects a reasonable offer from your side on this subject. This license will only cover the period of the abuse and will not grant use of the content from now on forward.
- [redacted] has incurred \$9596 in legal costs for the two letters that were sent to you. [redacted] has all contracts and payment proof for that amount.
- We are provided a copy of the current lab manual for that course (Expert Penetration Testing) as proof that the infringement has stopped.

Best would be to communicate your proposal to [redacted] before agreeing on a best time to have the call.

Kind Regards,

[redacted]

=====

From : Infosec Institute
To : Corelan

Thanks. We do want to resolve this. On points #1 and #2, we can accomodate. I am not sure what license amount is appropriate? I think we need to discuss this.

On points #3, we need to further understand this, I am not sure why a letter cost almost \$10,000? I do believe that [redacted] did indeed spend that amount, no need to provide proof.

On point #4, we do not have a replacement lab manual. We never ran the course after the time it was a failure, and we never used the manual again. Please check our website (and cached versions available anywhere) to see that we have no course dates for this course.

My attorney has advised me to schedule a call and talk these points over. I dont think we are getting anywhere via email here.

Also, what do you plan to do about the contract instructor that actually used the website content? I am more than willing to turn his name and contact details over to you, as well as a signed copy of the contract that shows he agreed to never use copyrighted material when producing course content. I feel like I am a double victim here.

=====

From : Infosec Institute
To : Corelan

Thanks [redacted]. First of all, I want to formally apologize on the behalf of InfoSec Institute, as well as for myself (I personally contracted the rogue instructor) for this issue. It has caused us a lot of pain over the last couple weeks and it is a totally regrettable situation. We are a small security company, without much resources, we are not a SANS or Global Knowledge, and we always try to do the right thing.

We would like to provide a public apology as well as compensate you for the 6 course books printed during the class, at \$150/student. This is typical courseware fee you can find for any courseware out there, please check Microsoft Official Courseware, etc. Also, as we cannot meet your fourth request, of providing you the new book, because there is none, we will provide any reasonable legal assurance that the rogue instructor only used the website content for that one class, and no classes before it, and no classes after it.

We are also looking into our legal options as far as suing the contract instructor, but the initial feedback has been that the lawsuit would cost upwards of \$50,000. I think our best course of action will be to turn the contact details and contract over to [redacted] to make things right.

=====

One mail was left out here because it contained in-line comments and was difficult to redact in the context of this document. It didn't contain more information but rather was a reiteration of points previously mentioned.

=====

From : Infosec Institute
To : Corelan

Thanks [redacted]. I do agree with you, we should have made a better effort to get in contact with you before this got out of hand, I do apologize for not spending more time on this matter previously as you suggested. I did write a regular postal mail letter in response, and received no response back from you, so I had made a wrong assumption that the matter was closed. Again, I apologize for that.

My previous proposal was serious, it was just all that I know I can offer myself without having to get everyone involved here. I did not intent to insult you, please do not think that. I will take your feedback seriously and have a meeting this week to see what we can do.

Please do take into consideration that this was courseware provided by a contract instructor, not by infosec itself, and we have some pretty strong legal protections in our contract if a contractor uses copyrighted material. We also refunded or credited everyone from the one single class that was taught. We are more than willing to sign any legal document that states we did not use the website content beyond this one single class with just a handful of students in it.

Best wishes,

[redacted]

=====

From this point on, the discussion basically stopped. It ended with this final e-mail :

=====

From : Infosec Institute
To : Corelan

[redacted], it is not a matter of taking this seriously or not, I assure you, we do take this seriously, which is why we are conversing here in the first place. This is not a personal issue, no one is trying to insult you here. Please do not think this. I was screwed by a contractor, now im being screwed by you. I am the one who should be upset here, but I am trying to be civil and professional as possible.

Our attorney has assured us many times over that any lawsuit will be thrown out immediately with our contract, and your course of recourse will be to sue the contractor. They estimated \$5000 to have this thrown out, and I really don't want to waste time in court and waste time preparing our defense. We also have quite a lot of evidence of harassment and threats accumulated from the emails sent by [redacted].

I am sorry you are not accepting our offer, but I don't know what else I can do to make you happy? Are you sure it is in your best interest to spend time, money on legal fees rather than other productive things in life? Are your attorney's simply wanting to earn more fees?

Please do some soul searching here and lets get this wrapped up so we can move on.

=====

With the incurred costs running well over \$10,000, the \$5,000 offered by Infosec Institute was and remains unacceptable for Corelan, whereafter all communications seized. There was no purpose in pursuing this issue through e-mail and although phone numbers were exchanged early in the e-mail conversation, Infosec Insitute never chose to use them. The fact that Infosec Institute claimed they were the victim adds insult to injury. We might not be in agreement on who needs to do some soul searching here.

We hereby reiterate the claims made by Infosec Institute in the e-mail conversation :

1. Infosec Institute did what it had to do

According to Infosec Institute, they replied to the first registered letter immediately. With a regular letter. Let me reiterate that. Infosec Institute replied to an official document, sent to them by registered mail, with a regular letter and subsequently assumed the matter was settled. The other registered letters were therefore ignored. The emails asking them to get in touch were therefore ignored. While Corelan asked for a copy of the letter that was never received, Infosec Institute chose not to produce this letter. The registered letters are provided to you both as a reference to the the time that has elapsed and as evidence to the effort done by Corelan to reach out to Infosec Institute.

2. Infosec Institute is not liable in this matter

According to Infosec Institute the course was written by a contractor. Infosec Institute claimed to have a contract that puts all liability for copyright infringement with that contractor. The name of said contractor was never revealed and Infosec Institute did never produce the contract to support this claim. Given that Infosec Institute put their logo and name on the manual and all mentions of Corelan in the manual were replaced by Infosec Institute mentions, we don't believe liability lies with the person or persons who gave the course. It was and remains Infosec Institute's responsibility to verify copyright before using the document in a course. Any basic review of the document, as attached, would have raised questions immediately.

3. Course retirement and reimbursement of students

According to infosec institute the course was given once and never given again after the copyright issue was raised by, at least, one of their students. It was also claimed that the students attending the course were reimbursed. No evidence to support this claim was given nor could it be otherwise confirmed. Moreover, the course remains present on the website today :

http://www.infosecinstitute.com/courses/expert_penetration_testing_training.html

It is noted that there are no scheduled dates but that doesn't mean the course has been retired ... And the content of the webpage has changed little over the past two years:

web.archive.org/web/20110403223335/http://www.infosecinstitute.com/courses/expert_penetration_testing_training.html

10 captures 21 Jun 09 - 15 May 11

DEC APR MAY 3 1471-0059 2010 2011 2012

InfoSec Institute

WHAT'S NEW ABOUT INFOSEC COURSE CATALOG CONTACT US

Learn to hack your organization before the bad guys do

[FIND OUT PRICING](#)
[COURSE CATALOG](#)
[GET A DETAILED SYLLABUS](#)
[GET AN ON-SITE QUOTE](#)

The InfoSec Institute Advantage:

- » The Planet's Most Comprehensive Training Experience
- » Hands On Security Training
- » Cutting-Edge Course Content
- » Satisfaction Guarantee
- » World Renown Instructors
- » Boot Camp Style Training
- » Luxury Accommodations

Enterprise Security Awareness:

- » Security Awareness for IT Users
- » Security Awareness for PCI DSS
- » Security Awareness for IT Pros
- » Security Awareness for Software Developers

Hands-On Security Training:

- » Ethical Hacking
- » Advanced Ethical Hacking
- » Penetration Testing - 10 Day
- » Expert Penetration Testing
- » Intrusion Prevention
- » Computer Forensics Training
- » Advanced Computer Forensics
- » Data Recovery Training

Expert Penetration Testing: Writing Windows Exploits

InfoSec Institute: Information Security Training

The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform.

This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time. Lab sessions are generally run four times per day. The lab sessions are a crucial learning component of the class, and are strongly recommended.

The labs ask students to reverse engineer sample programs as well as real production software to discover vulnerabilities. In addition to static analysis methods, various runtime vulnerability discovery methods such as fuzzing and runtime analysis in a debugger will be used.

Later exercises demonstrate more advanced concepts and tools - such as exploiting SafeSEH, the new ASLR protections found in Vista and Windows 7, and many others.

[FIND OUT PRICING](#)

After taking this information security course, you will walk out the door with the skills to defeat the latest OS and compiler protections found on the Microsoft Windows platform.

Some of the topics you will learn to master during the course:

Module 1: Primer on Windows Internals

- A primer on windows internals
- Windows architecture
- Windows internals from the ground up
- Windows exploits

web.archive.org/web/20091216062844/http://www.infosecinstitute.com/courses/expert_penetration_testing_training.html

10 captures 21 Jun 09 - 15 May 11

JUN DEC JAN 16 1471-0059 2008 2009 2010

InfoSec Institute

WHAT'S NEW ABOUT INFOSEC COURSE CATALOG CONTACT US

Call toll free 1(866)471-0059
Call direct +1-708-689-0131

Learn to hack your organization before the bad guys do

[FIND OUT PRICING](#)
[COURSE CATALOG](#)
[GET A DETAILED SYLLABUS](#)
[GET AN ON-SITE QUOTE](#)

Expert Penetration Testing: Writing Windows Exploits

InfoSec Institute: Information Security Training

The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform.

This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time. Lab sessions are generally run four times per day. The lab sessions are a crucial learning component of the class, and are strongly recommended.

The labs ask students to reverse engineer sample programs as well as real production software to discover vulnerabilities. In addition to static analysis methods, various runtime vulnerability discovery methods such as fuzzing and runtime analysis in a debugger will be used.

Later exercises demonstrate more advanced concepts and tools - such as exploiting SafeSEH, the new ASLR protections found in Vista and Windows 7, and many others.

[FIND OUT PRICING](#)

After taking this information security course, you will walk out the door with the skills to defeat the latest OS and compiler protections found on the Microsoft Windows platform.

Some of the topics you will learn to master during the course:

- » Small Class Size
- » Hands On Security Training
- » Cutting-Edge Course Content
- » Satisfaction Guarantee
- » World Renown Instructors
- » Boot Camp Style Training
- » Luxury Accommodations

Enterprise Security Awareness:

- » Security Awareness for IT Users
- » Security Awareness for PCI DSS
- » Security Awareness for IT Pros
- » Security Awareness for Software Developers

Hands-On Security Training:

- » Ethical Hacking
- » Advanced Ethical Hacking
- » Penetration Testing - 10 Day
- » Expert Penetration Testing
- » Intrusion Prevention

InfoSec Institute

WHAT'S NEW ABOUT INFOSEC COURSE CATALOG CONTACT US



Learn to hack your organization before the bad guys do

- [FIND OUT PRICING](#)
- [COURSE CATALOG](#)
- [GET A DETAILED SYLLABUS](#)
- [GET AN ON-SITE QUOTE](#)

The InfoSec Institute Advantage:

» The Planet's Most Comprehensive Training Experience

- » Hands On Security Training
- » Cutting-Edge Course Content
- » Satisfaction Guarantee
- » World Renown Instructors
- » Boot Camp Style Training
- » Luxury Accommodations

Enterprise Security Awareness:

- » Security Awareness for IT Users
- » Security Awareness for PCI DSS
- » Security Awareness for IT Pros
- » Security Awareness for Software Developers

Hands-On Security Training:

- » Ethical Hacking
- » Advanced Ethical Hacking
- » Penetration Testing - 10 Day

Expert Penetration Testing: Writing Windows Exploits

InfoSec Institute: Information Security Training

The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform.

This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time. Lab sessions are generally run four times per day. The lab sessions are a crucial learning component of the class, and are strongly recommended.

The labs ask students to reverse engineer sample programs as well as real production software to discover vulnerabilities. In addition to static analysis methods, various runtime vulnerability discovery methods such as fuzzing and runtime analysis in a debugger will be used.

Later exercises demonstrate more advanced concepts and tools - such as exploiting SafeSEH, the new ASLR protections found in Vista and Windows 7, and many others.

[FIND OUT PRICING](#)

After taking this information security course, you will walk out the door with the skills to defeat the latest OS and compiler protections found on the Microsoft Windows platform.

Learn to hack your organization before the bad guys do

[GET AN ON-SITE QUOTE](#)

- » Small Class Size
- » Hands On Security Training
- » Cutting-Edge Course Content
- » Satisfaction Guarantee
- » World Renown Instructors
- » Boot Camp Style Training
- » Luxury Accommodations

Enterprise Security Awareness:

- » Security Awareness for IT Users
- » Security Awareness for PCI DSS
- » Security Awareness for IT Pros
- » Security Awareness for Software Developers

Hands-On Security Training:

- » Ethical Hacking
- » Advanced Ethical Hacking
- » Penetration Testing - 10 Day
- » Expert Penetration Testing
- » Intrusion Prevention
- » Computer Forensics Training
- » Advanced Computer Forensics
- » Data Recovery Training
- » Forensics & Data Recovery - 10 Day
- » Security Architecture Design
- » Application Security
- » SCADA Security
- » Reverse Engineering Training
- » Advanced Reverse Engineering Malware
- » Information Security Training
- » DIACAP Training
- » Incident Response and Network Forensics
- » VOIP Security Course
- » Wireless Security Training
- » On-Site Training

Expert Penetration Testing: Writing Windows Exploits

InfoSec Institute: Information Security Training

The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform.

This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time. Lab sessions are generally run four times per day. The lab sessions are a crucial learning component of the class, and are strongly recommended.

The labs ask students to reverse engineer sample programs as well as real production software to discover vulnerabilities. In addition to static analysis methods, various runtime vulnerability discovery methods such as fuzzing and runtime analysis in a debugger will be used.

Later exercises demonstrate more advanced concepts and tools - such as exploiting SafeSEH, the new ASLR protections found in Vista and Windows 7, and many others.

[FIND OUT PRICING](#)

After taking this information security course, you will walk out the door with the skills to defeat the latest OS and compiler protections found on the Microsoft Windows platform.

Some of the topics you will learn to master during the course:

Module 1: Primer on Windows Internals

- A primer on windows internals
- Windows architecture
- Windows internals from the ground up
- Windows sockets
- Threads and Processes
- File handling
- File formats
- Process injection and remote thread injection
- Understanding exploit development across different windows versions

Module 2: Stack Overflows

- Understanding modularity of code and how it can lead to a stack overflow situation
- Typing stack overflows
- Functions and Prologs
- Controlling EIP through RET
- Returning to shellcode on the stack
- Shellcode strategies

web.archive.org/web/20110515075523/http://www.infosecinstitute.com/courses/expert_penetration_testing_training.html

Internet Archive Wayback Machine

InfoSec Institute

10 captures 21 Jun 09 - 15 May 11

Virtualization
Linux
Project Management
ITIL
BS70

CISSP Prep
Intrusion Prevention
Computer Forensics
Data Recovery
SCADA Security
*VIEW MORE SECURITY COURSES

APR MAY JUN
15
2010 2011 2012

HOME // INFORMATION SECURITY TRAINING // EXPERT PENETRATION TESTING

Expert Penetration Testing: Writing Windows Exploits

SEC-540

“ Master the latest advanced level methodologies, tools, and manual techniques used by ethical hackers to **enter the top 10% of security professionals in terms of skill.** ”

WHAT'S ON THIS PAGE?

- Course Overview
- What You'll Learn
- Dates & Locations
- What Students Are Saying
- Prerequisites & Related Courses
- Pricing (What's Included?)

GET QUOTE

Expert Penetration Testing Course Overview

COURSE LENGTH: 3-DAY

The InfoSec Institute Expert Hacking course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform.


This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time. Lab sessions are generally run four times per day. The lab sessions are a crucial learning component of the class, and are strongly recommended.

The labs ask students to reverse engineer sample programs as well as real production software to discover vulnerabilities. In addition to static analysis methods, various runtime vulnerability discovery methods such as fuzzing and runtime analysis in a debugger will be used.

Later exercises demonstrate more advanced concepts and tools – such as exploiting SafeSEH, the new ASLR protections found in Vista and Windows 7, and many others.

HOW YOU'LL BENEFIT:

- Gain the **in-demand career skills** of a highly skilled and specialized penetration tester.
- Master the latest advanced level methodologies, tools, and manual techniques used by ethical hackers to **enter the top 10% of security professionals** in terms of skill.
- Move **beyond the most well known ethical hacking techniques** and into the realm of an **smart penetration tester**.



Created and taught by Best-selling Industry Authors

4. Infosec Institute is the victim here

According to our contact at Infosec Institute, they are to be regarded as a victim in this matter. No less than two times! First they were betrayed by above mentioned external contractor. Secondly they are victimized because of Corelan trying to protect its copyright. It is obvious that this document will draw some community attention towards Infosec Institute but had it acted prudently and with respect for content owned by a third party, this would not have been the case. A driver who dies when his car crashes into a tree after “he was fed several pints of beer at a local pub” obviously is a victim of a car crash but that doesn’t make the company producing the beer liable for the driver’s death. We leave it up to the reader to understand and judge on the issue at hand.

Also, Infosec Institute felt threatened by the e-mails sent to them. Since when is pursuing your copyright considered ‘harrassment’? Apart from the, possibly a little out of line ‘rape metaphor’, what language in these e-mails could be interpreted as threats?

It is now October 2011 and while Infosec Institute has apologized for the copyright infringement (repeatedly), there is no indication that they are aware of the impact of their actions nor is there any indication that they are really sorry about this. Just a few days ago, probably because the number of people asking their contributions to be removed getting too high, <http://resources.infosecinstitute.com> became unreachable from Belgium and The Netherlands. Not sure what they have against the Dutch but this is the message you'll receive when visiting from a Belgian or Dutch IP Address :

Thank you for visiting us at Resources.InfoSecInstitute.com.
Unfortunately we've had to close down this area of our site indefinitely.
Please go to <http://www.infosecinstitute.com> if you're interested in IT and Security training .



Proxies across the world were helpful to show that the site was still very much alive for the rest of the planet.

Hereafter you will find exhibits from the full PDF containing the most blatant examples of plagiarism in the course manual. Plagiarism is a serious crime and anybody taking part in this practice should perform his or her own soul searching. It was, is and will always be unacceptable. The full pdf of the lab manual is distributed with this document.

Exhibit one : copyright and verbatim copy

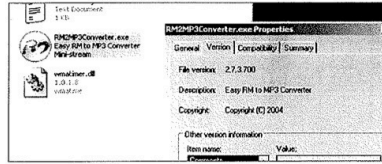
page 2 of 'Expert Penetration Testing Lab Manual'

Verify the bug

First of all, let's verify that the application does indeed crash when opening a malformed m3u file.

Install the vulnerable version of Easy RM to MP3. You will find a copy of it in the "vulnerable programs to exploit" directory on the desktop of the VM.

Public vulnerability reports of this vulnerability states that the exploit works on XP SP2 (English), but we will use XP SP3 (English).

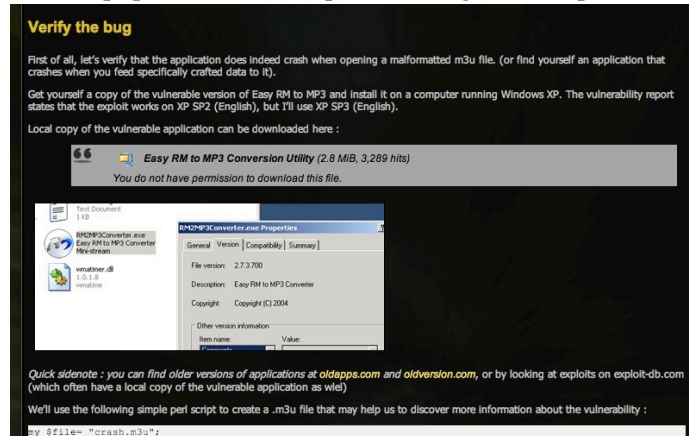


Quick sidenote : you can find older versions of applications at oldapps.com and oldversion.com.

We'll use the following simple perl script to create a .m3u file that may help us to discover more information about the vulnerability :

```
my $file= "crash.m3u";
```

<http://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>



- Every page in the manual is marked 'Copyright Infosec Institute, Inc.'
- Text is copied verbatim from the Corelan website, including screenshots.

Exhibit 2 : typos

Page 4 of the manual

Process Memory

When an application is stared in a Win32 environment, a process is created and virtual memory is assigned to. In a 32 bit process, the address ranges from 0x00000000 to 0xFFFFFFFF, where 0x00000000 to 0x7FFFFFFF is assigned to "user-land", and 0x80000000 to 0xFFFFFFFF is assigned to "kernel land". Windows uses the flat memory model, which means that the CPU can directly/sequentially/linearly address all of the available memory locations, without having to use a segmentation/paging scheme.

Kernel land memory is only accessible by the OS.

When a process is created, a PEB (Process Execution Block) and TEB (Thread Environment Block) are created.

The PEB contains all user land parameters that are associated with the current process :

- Location of the main executable

Copyright InfoSec Institute, Inc. | Expert Penetration Testing Lab Manual 4

<http://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

Process Memory

When an application is started in a Win32 environment, a process is created and virtual memory is assigned to. In a 32 bit process, the address ranges from 0x00000000 to 0xFFFFFFFF, where 0x00000000 to 0x7FFFFFFF is assigned to "user-land", and 0x80000000 to 0xFFFFFFFF is assigned to "kernel land". Windows uses the flat memory model, which means that the CPU can directly/sequentially/linearly address all of the available memory locations, without having to use a segmentation/paging scheme.

Kernel land memory is only accessible by the OS.

- typo : 'stared' instead of 'started' was copied.

Exhibit 3 : Mass find/replace action

Page 13 of the manual

INFOSEC INSTITUTE

Let's use Windbg. Windbg is already installed on your VM, but you must still register it as a "lab-mortem" debugger using "windbg -WE".

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Debugging Tools for Windows (x86)>windbg -I
C:\Program Files\Debugging Tools for Windows (x86)>_
```

<http://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

The debugger

In order to see the state of the stack (and value of registers such as the instruction pointer, stack pointer etc), we need to hook up a debugger to the application, so we can see what happens at the time the application runs (and especially when it dies).

There are many debuggers available for this purpose. The two debuggers I use most often are Windbg, and Immunity's Debugger

Let's use Windbg. Install Windbg (Full install) and register it as a "post-mortem" debugger using "windbg -I".

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Debugging Tools for Windows (x86)>windbg -I
C:\Program Files\Debugging Tools for Windows (x86)>_
```

- 'I' was replaced by 'WE', which changed windbg -I to windbg -WE.
- the screenshot still shows the right command syntax.

Exhibit 4

Page 31 of the manual

Let's use this shellcode. The new exploit looks like this : we have manually broken the shellcode shown here. So if you use it the exploit it will not work. But you should know by now how to make a working exploit.

```
#
#
#
my $file= "exploitrmomp3.m3u";

my $junk= "A" x 26094;
my $eip = pack('V',0x01ccf23a); #jmp esp from MSRMcodec02.dll

my $shellcode = "\x90" x 25;

# windows/shell_bind_tcp - 703 bytes
# http://www.metasploit.com
# Encoder: x86/alpha_upper
# EXITFUNC=seh, LPORT=4444, RHOST=
$shellcode=$shellcode." \x89\xe1\xdb\xd4\xd9\x71\xf4\x58\x50\x59\x49\x49\x49\x49" .
"\x43\x43\x43\x43\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56" .
"\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30\x41\x30\x30\x41" .
"\x42\x41\x41\x42\x54\x00\x41\x51\x32\x41\x42\x32\x42\x42" .
"\x30\x42\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x42" .
```

Copyright InfoSec Institute, Inc. | Expert Penetration Testing Lab Manual 31

<http://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/>

```
Let's use this shellcode. The new exploit looks like this : P.S. I have manually broken the shellcode shown here. So if you copy & paste the exploit it will not work. But you should know by now how to make a working exploit.

# Exploit for Easy RM to MP3 27.3.700 vulnerability, discovered by Crazy_Hacker
# Written by Peter Van Eeckhoutte
# http://www.corelan.be:8800
# Greetings to Saumil and SK :-)
#
# tested on Windows XP SP3 (En)
#
#
my $file= "exploitrmomp3.m3u";

my $junk= "A" x 26094;
my $eip = pack('V',0x01ccf23a); #jmp esp from MSRMcodec02.dll

my $shellcode = "\x90" x 25;

# windows/shell_bind_tcp - 703 bytes
# http://www.metasploit.com
```

- text was slightly altered.
- references to Peter Van Eeckhoutte and Corelan were removed from the code.

Exhibit 5

Page 104 of the manual

INFOSEC INSTITUTE

```
custom vulnerable server.
    },
'Author'      => { 'InfoSec' },
'Version'    => '$Revision: 9999 $',
'DefaultOptions' =>
(
    'EXITFUNC' => 'process',
),
'Payload'    =>
(
    'Space'    => 1400,
    'BadChars' => " " ,
```

- Author was changed to 'Infosec'

Exhibit 6

Page 310 of the manual

INFOSEC INSTITUTE

```
004040A0 68 6C616E00 PUSH 6E616C
004040A5 68 486F7265 PUSH 65726F48
004040AA 8B0C MOV EBX,ESP
004040AC 68 616E2000 PUSH 206E61
004040B1 68 6F72656C PUSH 6C65726F
004040B6 68 62732043 PUSH 43207962
004040BB 68 6E656420 PUSH 2064656E
004040C0 68 6E207077 PUSH 7770206E
004040C5 68 20626565 PUSH 65656220
004040CA 68 68617665 PUSH 65766168
004040CF 68 596F7520 PUSH 20756F59
004040D4 8BCC MOV ECX,ESP
004040D6 33C0 XOR EAX,EAX
004040D8 50 PUSH EAX
004040D9 50 PUSH EAX
004040DA 51 PUSH ECX
004040DB 50 PUSH EAX
004040DC 50 PUSH EAX
004040DD C7C6 EA07457E MOV ESI,USER32.MessageBoxA
004040E3 FFE6 JNF ESI
```

- The hex code in this screenshot contains :

corelan

you have been owned by corelan

Conclusion

1. Copyright infringement is a serious crime. Being sorry doesn't make this right. The evidence is clear and Infosec Institute acknowledges the infringement.
2. Infosec institutes transfers liability to a 'rogue instructor' without proof while the evidence supports the assumption that it is Infosec Institute who is at fault.
3. The infosec community has a right to know who plagiarizes content and/or infringes copyright. The act is repulsive, illegal and intolerable.
4. It can not be denied that Corelan, to date, has done everything within its means to resolve this issue.