Programació de codi segur

José María Alonso Cebrián
Jordi Gay Sensat
Antonio Guzmán Sacristán
Pedro Laguna Durán
Alejandro Martín Bailón
Jordi Serra Ruiz
Josep Vañó Chic

PID_00213937

Material docent de la UOC

UOC
Universitat Oberta de Catalunya

José María Alonso Cebrián

Enginyer informàtic per la Universitat Rey Juan Carlos de Madrid, on està acabant la tesi doctoral sobre seguretat en aplicacions web. Ha estat premiat amb el títol de Most Valuable Professional per Microsoft en l'àrea de seguretat informàtica des de l'any 2004, distinció que avui dia només tenen tres persones a Espanya. Escriu habitualment en revistes tecnològiques sobre seguretat informàtica i és ponent en conferències nacionals com la Gira de Seguretat de Microsoft, Masters, el Technet Security Day o l'Asegúr@IT a més de participar en conferències internacionals com Blackhat, Defcon, ToorCon o ShmooCon. Treballa com a consultor de seguretat en Informática 64 i escriu un blog sobre seguretat informàtica titulat "Un informático en el lado del mal".

Jordi Gay Sensat

Enginyer informàtic per la Universitat Politècnica de Catalunya. Ha exercit de professor a la Universitat de Girona. Ha participat en diversos reptes de *hacking* com Izhal, Boinas negras (I i II), Hackerslab o NGsec. Actualment és el cap del Departament de Tecnologia del Centre de Convencions Internacional de Barcelona.

Antonio Guzmán Sacristán

Doctor en Informàtica des de l'any 2006 per la Universitat Rey Juan Carlos (URJC) de Madrid, on desenvolupa pràcticament tota la seva tasca docent i investigadora. Cofundador del grup d'investigació en arquitectures d'altes prestacions i professor de l'Àrea d'Arquitectura i Tecnologia de Computadors de la Universitat Rey Juan Carlos des de l'any 2000. Coordinador de les assignatures d'*Arquitectura de computadors* i *Seguretat informàtica* en la titulació d'Enginyeria Informàtica. Ha participat en 10 projectes d'investigació de diferent abast, ha impartit prop de 200 crèdits en programes de grau i postgrau oficials i està especialment involucrat en projectes d'innovació educativa. Té publicacions en les conferències internacionals Blackhat, Defcon, Toorcon i ShmooCon.

Pedro Laguna Durán

Treballa com a consultor de seguretat en Informática 64. Ha estat premiat amb el títol d'MSP (Microsoft Student Partner) que Microsoft dóna als estudiants que destaquen per la seva tasca en comunitats tècniques. És ponent habitual en conferències de seguretat i està especialitzat en tècniques XSS. Ha estat el creador de WebBrowsing Fingerprinting i Thumbando, eines per a l'anàlisi de navegadors i de fitxers de miniatures. http://www.informatica64.com/wbfingerprinting i http://www.informatica64.com/thumbando/. Investiga temes de seguretat i reporta errors habitualment en serveis basats en Web.

Alejandro Martín Bailón

Enginyer informàtic per la Universitat de Salamanca i màster en Tecnologies de la informació i sistemes informàtics per la Universitat Rey Juan Carlos de Madrid. Director de desenvolupament de solucions en Informática 64 i especialista en seguretat en xarxes sense fil, temes sobre els quals ha publicat múltiples articles en revistes i congressos i sobre els quals ha impartit conferències en congressos com FIST o Asegúr@IT.

Jordi Serra Ruiz

Doctor en Informàtica per la UOC. Enginyer informàtic per la Universitat Autònoma de Barcelona (UAB). Màster en Informàtica industrial per la UAB. Professor del Departament d'Informàtica de la UAB fins al 2002. Actualment, és professor de la Universitat Oberta de Catalunya (UOC) i director acadèmic del màster de Seguretat informàtica de la UOC.

Josep Vañó Chic

Enginyer en Informàtica i màster en Direcció i gestió de sistemes i tecnologies de la informació, per la UOC. Professional en l'àrea de desenvolupament de programari des de 1985, inicialment en l'àmbit de l'empresa privada i actualment en l'Administració pública, combinant aquesta tasca amb la de consultor de la UOC en el màster interuniversitari de Seguretat de les tecnologies de la informació i les comunicacions.

L'encàrrec i la creació d'aquest material docent han estat coordinats pel professor Jordi Serra Ruiz per al programa del Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions –MISTIC– (2014)

Tercera edició: setembre 2014
© José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán, Pedro Laguna Durán, Alejandro Martín Bailón, Jordi Serra Ruiz, Josep Vañó Chic
Tots els drets reservats
© d'aquesta edició, FUOC, 2014
Av. Tibidabo, 39-43, 08035 Barcelona
Disseny: Manel Andreu
Realització editorial: Oberta UOC Publishing, SL
Dipòsit legal: B-18.671-2014

Mòduls 2 i 6 sota llicència *Copyright*

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Mòduls 1,3,4 i 5 sota llicència *Creative Commons*

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Comons. Podeu copiar-los, distribuir-los i transmetre'lspúblicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un üscomercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca

Continguts

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán,
Pedro Laguna Durán, Alejandro Martín Bailón i Jordi Serra Ruiz

1. Escriptura de *shellcodes*
2. *Shellcodes* per entrada estàndard
3. *Shellcodes* alfanumèrics
4. Un exemple de *shellcode*
5. Adreça de la funció per cridar
6. El *shellcode* en assemblador
7. El *shellcode* en binari
8. L'*exploit* amb el *shellcode*

Bibliografia

AT&T. http://www.att.com/

Basic Architecture (vol. 1). http://download.intel.com/design/processor/manuals

Codegear. *Borland C++ compiler*. http://www.codegear.com/downloads/free/cppbuilder

CVE.Mitre. *Common Vulnerabilities and Exposures*. http://cve.mitre.org/cve/

GCC. GNU. *GCC online documentation*. http://gcc.gnu.org/onlinedocs/

GCC. GNU. *The GNU Compiler Collection*. http://gcc.gnu.org/

GNU. *GDB: The GNU Project Debugger*. http://www.gnu.org/software/gdb/

GNU. *GNU Binutils (Objdump i altres aplicacions)*. http://www.gnu.org/ software/binutils/

IBM. *Linux / Inside memory management: Garbage Collection*.http://www.ibm.com/developerworks/linux/library/l-memory/#N103DD

Inline Assembly. http://www.delorie.com/djgpp/doc/brennan/brennan_att_inline_djgpp.html

Insight: The GDB GUI. http://sources.redhat.com/insight/

Intel. *Intel 64 and IA-32 Architectures Software Developer's Manuals*. http://www.intel.com/products/processor/manuals/index.htm

Intel. *Intel 64 and IA-32 Architectures Software Developer's Manuals. Volume 2A: Instruction Set Reference, A-M*. http://download.intel.com/design/processor/manuals/253666.pdf

Intel. *Intel 64 and IA-32 Architectures Software Developer's Manuals. Volume 2A: Instruction Set Reference, N-Z*. http://download.intel.com/design/processor/manuals/253667.pdf

Intel. http://www.intel.com/

Kernel. *Linux*. http://www.kernel.org/

Microsoft. *Debugging tools for Windows*. http://www.microsoft.com/whdc/devtools/debugging/default.mspx

Microsoft. *Windows*. http://www.microsoft.com/WINDOWS/

MSDN. *Microsoft Visual Studio 2008/.NET: Garbage Collection*. http://msdn.microsoft.com/en-us/library/0xy59wtx.aspx

NASM. *The Netwide Assembler*. http://www.nasm.us/

OllyDbg. http://www.ollydbg.de/

Secunia. http://secunia.com/advisories/

SecurityFocus. http://www.securityfocus.com/bid

Sourcerware. *Debugging with GDB*. http://sourceware.org/gdb/download/onlinedocs/gdb.html

Sourcerware. *GNU Binary Utilities (Documentació d'Objdump i altres aplicacions)*. http://sourceware.org/binutils/docs-2.19/binutils/index.html

Sourcerware. *AS Documentation (part of Binutils)*. http://sourceware.org/binutils/docs-2.19/as/

Sourcerware. *AT&T Syntax versus Intel Syntax*. http://sourceware.org/binutils/docs/as/i386_002dSyntax.html#i386_002dSyntax

Unix. http://www.unix.org/