

Sommaire

1

Les astuces de Microsoft Vista	35
1.1 Les privilèges des systèmes d'exploitation Vista	38
Windows Vista Start Edition	38
Windows Vista Home Basic	39
Windows Vista Home Premium	39
Windows Vista Business	40
Windows Vista Entreprise	40
Windows Vista Ultimate Edition	41
1.2 La sécurité Vista	42
Les normes de sécurité pour la communication	42
Internet Explorer 7	43
La protection NAP (Network Access Protection)	43
Le pare-feu Windows	44
Windows Defender et MSRT	44
L'installation des pilotes	44
Une clé publique améliorée avec PKI	44
La sécurité des ordinateurs portables	44
1.3 Les promesses de Vista	45
1.4 Obtenir davantage de privilèges sur le système Vista	47
1.5 L'intégration de Windows Vista Ultimate dans un domaine	50
1.6 Sauvegarder des données avec Vista	56
1.7 Transférer un fichier sur une clé USB	57
1.8 Les restrictions basiques pour Windows Vista	58
1.9 Le logiciel HackingInterditSecurityVista pour Windows Vista et XP ..	59
1.10 Logiciel (HIL) HackingInterditLanceur Multi-langues	64
Lanceur pour des applications Windows Vista et Windows XP	65
Choix entre des applications Windows XP ou Windows Vista	66
Personnaliser votre base de données	74
1.11 Configuration d'un serveur Proxy	85
Avantage d'un Proxy	85
Création des comptes Locaux	86
Proxy Plus	86
Installation de Proxy + pour Vista	87
Configurer le Proxy + sur Windows Vista	88
Configuration pour les utilisateurs à distance	88
Gérer les utilisateurs	89
Configurer les ports d'écoute pour les clients	90
Gestion du cache	90
Configurer Dns Cache	91
Configuration d'Internet Explorer	91

2

Protéger son ordinateur 93

2.1 Sauvegarder ses données 95

2.2 Utiliser un pare-feu 97

 L'analyse des IP et des paquets d'un réseau 98

 L'analyse des applications 99

 Les avantages du pare-feu 99

 Utiliser le pare-feu de Windows XP SP2 100

 Utiliser Kaspersky Anti-Hacker 119

2.3 Se protéger contre les virus 142

 Utiliser Norton 143

2.4 Se protéger contre les troyens 152

 Détecter la présence d'un cheval de Troie dans un PC 152

 Le programme T-Anti-Troyen 154

2.5 Trouver des stratégies de défense 156

 Les pots de miel 156

 Les antisniffers 157

 Les antitraceurs 158

 Se protéger contre les failles du système 158

 Utiliser un coffre-fort 159

 La protection parentale 161

 Protéger le transfert des données avec IpSec 162

 Utiliser Access Denied 166

3

Protéger sa vie privée 169

3.1 L'e-mail anonyme 171

3.2 Protéger sa machine contre les connexions Telnet 177

3.3 Récupérer des cookies effacés 177

3.4 Se protéger contre les caches 187

3.5 Naviguer avec Internet Explorer en toute sécurité 188

 Retirer l'enregistrement automatique des mots de passe d'Internet Explorer 188

 Créer un compte d'utilisateur 189

3.6 Utiliser des logiciels antimouchards 191

 Ad-aware : un antimouchard puissant 191

 Spybot-search & destroy : l'ennemi numéro 1 des mouchards 194

 Cookie Pal 17 démo : la terreur des mouchards 195

 XP-Antispy : l'antimouchard Microsoft 196

 Se débarrasser manuellement des espions d'ICQ 199

 Désactiver l'espion de Media Player 199

	Effacer les mouchards d'ActiveX	201
3.7	Désinfecter le système grâce à SmitfraudFix	201
3.8	Éliminer les fenêtres pop-up avec Stopzilla	205
3.9	Trouver des programmes anti-pop-up gratuits	206
3.10	Trouver des antispywares gratuits ou des versions de démonstration	207
3.11	Lutter contre le spamming	210
	Qui sont les spammeurs ?	211
	Comment les spammeurs procèdent-ils ?	213
	Le déni de service avec Spamassasin	213
	Trouver les spammeurs	214

4

Nettoyage et récupération de données 219

4.1	Supprimer un programme depuis le Panneau de configuration	221
4.2	Assainir et renforcer la Base de registre	222
	L'éditeur du Registre	223
	Brève présentation du registre	224
	Rechercher et supprimer un programme dans la Base de registre	226
	Protéger la Base de registre	227
	Bloquer des applications à partir du Registre	230
	Mieux gérer la Base de registre	243
4.3	Effacer ses traces	259
	Effacer ses traces des Propriétés d'Internet Explorer	259
	Effacer les données du journal d'événements Windows XP SP2 et Windows Vista Ultimate	267
	Des logiciels de nettoyage performants	269
4.4	Récupérer ses données	276
	Récupérer des fichiers à partir de la Base de registre avec Undelete	277
	Restaurer des données effacées avec Restorer 2000	279
	Utiliser Vedit	280
	Utiliser Ultraedit	280
	Récupérer un mot de passe	281

5

La configuration client/serveur et les types d'analyse de système 285

5.1	Les techniques	288
5.2	Créer un environnement de test	289
	La machine virtuelle	289
	Créer un contrôleur de domaine pour Windows 2003 Serveur	305
	Vérifier le DNS pour Windows Server 2003	307
	Configurer un serveur DHCP	309

	Créer des utilisateurs dans l'Active Directory	311
	Configurer un serveur web	314
	Les relations de confiance entre deux serveurs Windows	317
	Créer un sous-domaine	320
	Le serveur maître	323
	Défragmenter l'Active Directory	325
	Ajouter un nouveau membre au domaine	328
5.3	Tester les vulnérabilités à l'aide des scanners	333
	Le scanner NMAP et les sniffers	336
	Le scanner Tenable Nessus Vulnerability Scanner	361
	Les scanners de ports	367
	Les scanners de failles système	375
	Le scanner Web Acunetix	383
	Le scanner de vulnérabilités des pages HTTP et HTTPS N-Stealth HTTP Security Scanner	388
	Scanner des liens valides sur son site web avec Xenu	391
	Le scanner de Proxy ProxyHunter	394
	Le scanner BTScanner	399

6

Les sniffers et le repérage de domaines 401

6.1	L'annuaire Whois	403
	Les serveurs dans les différents continents	403
	La base Uwhois	406
	Le Whois magique	408
6.2	Les traceurs	410
	Le programme de traçage VisualRoute	410
	Le programme de traçage NeoTrace	414
	Trouver un pirate grâce au traçage MS-DOS de Windows	416
	Les traceurs en ligne	417
6.3	Les sniffers et renifleurs	421
	Le sniffer Ettercap	422
	Le sniffer Ethereal et les exploits de spoofing	430
	Renifler avec Netstat	442
	Le sniffer X-NetStat Professional	445
	Rechercher des informations sur les systèmes d'exploitation	454
	Les sniffers de réseaux sans fil	457
6.4	Trouver la cartographie d'un domaine	461

7

Les types de connexion sur le réseau 465

7.1	Configurer une connexion distante Terminal Server	467
-----	---	-----

7.2	Connexion VPN	469
	Établir une connexion VPN client Windows XP SP2	470
	Configurer une connexion VPN Windows XP	472
	Connexion VPN Connexion à votre espace de travail Windows Vista	484
	Connexion VPN (Connexion par modem) Windows Vista	492
7.3	Connexion à Internet avec un camouflage	494
	Steganos Internet Anonyme VPN	499
	Anonyme Stealther	504
7.4	Décryptage des mots de passe VPN Dial up	511
7.5	Connexion TightVNC	514
	Client Serveur VNC (Virtual Network Computing)	514
	Client VNC	519
	Connexion à l'ordinateur à distance par VNC	522
7.6	Connexion via Telnet	524
7.7	Sécurité du réseau sans fil	526
	Les modes d'accès Wi-Fi	527
	Fonctionnement d'IEEE 802.11	528

8

Cryptage et décryptage de données 555

8.1	La cryptologie utilisée par Caïn & Abel	557
	Avant de continuer sur le logiciel Caïn & Abel	558
	Craqueur de Caïn	558
	Les sniffers utilisés par Caïn & Abel	559
	Les bibliothèques de Caïn & Abel	562
	Configurer la carte réseau	562
	Configuration Dialog	563
	ABEL en action	565
	Le réseau du logiciel Caïn & Abel	566
	Gestion de l'ordinateur local	572
	Craquer les mots de passe grâce à Caïn Codebreakers	578
	Ajouter un HASH	581
	Récupération de mots de passe Access	583
	Boîte Revealer	584
	Décodeur à distance de mots de passe d'ordinateur de bureau	586
	Cisco Type-7 Password Decoder	588
	Dialup Password Decoder	589
	Directeur protégé de mots de passe de stockage	590
	Traceroute	591
	Décodeur de mot de passe de VNC	592
	Test du sniffer de Caïn	594
	Wireless	607

	Conclusion	607
8.2	Cryptage grâce au logiciel gratuit Security BOX	608
8.3	Cryptage et décryptage Locktight	611
	Cryptage d'un fichier	612
	Apercevoir le fichier hola.doc crypté	613
	Décryptage de fichiers	613
8.4	La sécurité absolue avec le cryptage PGP Entreprise	615
	Installation de PGP 9	615
	Types de cryptages sur PGP 9	625
	Options du PGP	627
8.5	Les hackers et le décryptage des mots de passe Windows	638
8.6	La stéganographie	640
	Présentation de la stéganographie	640
	Le cryptage utilisant la stéganographie	641
	Le logiciel Invisible Secret	641

9

Troyens, keyloggers, virus et vers 647

9.1	Les chevaux de Troie	649
	Les types de chevaux de Troie	649
	Les méthodes d'introduction d'un cheval de Troie	653
	ProRat : troyen ou administrateur à distance	657
9.2	Les keyloggers : Blazingtools Perfect Keylogger	685
	Configuration générale	686
	Configuration de logging	687
	Les captures d'écran	688
	Configuration du FTP	692
	Les alertes	694
	Installation à distance	695
9.3	Les programmes espions	698
	Technique d'utilisation	698
9.4	Les virus	699
	La détection des virus	699
	Les programmes farceurs	701

10

La force brute 709

10.1	La force brute Bluesnarf sur un téléphone Nokia	711
10.2	Le logiciel de force brute Brutus AET2	717
	Détails du logiciel Brutus	718
	Types d'attaques	720
	Options d'authentification	722

	Modes de craking	723
	Création d'un dictionnaire en .txt	725
	Brutus en mode d'attaque Telnet	726
	Capture de Brutus	727
	Test de vulnérabilité avec Brutus	728
	Faiblesse de Brutus	733
10.3	Le logiciel l0pthcrack	733
	Type d'attaque L0pthcrack	734
	Méthodes pour le test de vulnérabilité des mots de passe	736
	Type de rapport	741
	Début de l'audit de vulnérabilité des mots de passe	743
	Utilisation de Pwdump3 dans l'Invite de commandes	751
	Vérification des mots de passe	753
10.4	Arrêter les attaques de force brute	754
	Changement de nom d'administrateur pour Windows XP SP2 et Windows 2003 Serveur	754
	Verrouillage de compte	755
	Utilisation du moniteur réseau	757

11

Les exploits 763

11.1	Les exploits HPING pour Linux et pour Windows	766
	Les techniques d'attaque de ports fermés	773
	TCP SYN (drapeau)	775
	ACK (ACKnowledgement) activé	777
	Tous les flags (drapeaux) TCP	779
	Spoofing Avec HPING TCP -a	782
	Scanner des hôtes	785
	Test Spoofing avec HPING et Ethereal	792
	Mesures	797
11.2	Les exploits Genkeys et Aslead pour Windows et Linux	798
	Test de vulnérabilité d'une connexion VPN	799
	Connaître l'interface réseau dans Windows XP SP2	804
	Les exploits Genkeys et Asleap	805
	Contre-mesures	810
11.3	Les exploits des spammeurs	810
11.4	Les exploits destinés à trouver des fuites d'informations sur Internet	812
	Le logiciel .NET framework	812
	L'exploit Athena	813
	Analyse de la base de données d'Athena : les 1001 clés d'Athena	816
	Contre-mesures	842

11.5	L'exploit Netcat pour Windows XP/2000/2003	843
	La fonction scanneur de ports	844
	L'aide de Netcat pour résoudre une adresse IP d'un ordinateur à distance	845
	Écouter des ports avec Netcat	846
	La fonction sniffer	846
	Le transfert de fichiers	847
	Envoyer des e-mails grâce à Netcat	847
11.6	Le transfert de zones DNS avec des exploits	849
	Généralités	849
	Le transfert de zone grâce à l'exploit DIG pour Windows	851
	Les fonctions de l'exploit Retina	853
11.7	L'exploit Resource Hacker	854
11.8	Les fonctions de l'exploit Nuke	855
	Configuration de Nuke	855
	Mise en action de Nuke	855

12

Les intrusions, les failles système et leurs conséquences . . . 857

12.1	Les fuites d'informations d'intranet sur Internet	859
	Les fissures de sites web	860
	Les fuites d'informations sensibles	860
	Les techniques de repérage des fichiers temporaires sur Internet	863
	Techniques de repérage des fichiers logs sur Internet	870
	Découvrir les logs des Proxies anonymes	879
	Récolter des informations sensibles d'un serveur	879
	Tromper le moteur de recherche	881
	Les dangers des recherches	881
	Repérer des e-mails privés sur Internet	882
	L'intrusion visuelle : les caméras web	883
	Repérer les mots de passe d'un site sur Internet	888
12.2	Capter des flux RSS et des agrégateurs sur le Web	897
	Capter les nouvelles grâce au logiciel TekiNews	899
	Capter des fichiers audio et vidéo grâce au flux RSS Podcasting	901
	Le logiciel de capture de fichiers audio et vidéo Ipodder	903
	Capter les émissions de radio, les podcasts, les vidéos grâce au logiciel iTunes	908
12.3	Intrusion dans l'ère Wi-Fi pour Windows	910
	Le logiciel d'intrusion Wireless Air Crack	911
	Le logiciel d'intrusion Wireless Airodump	914
12.4	Injection PHPBB	916
12.5	Intrusion sur des sites de chat privés	922

13**Trouver tout type de fichiers sur Internet 931**

- 13.1 Les sites de téléchargement de logiciels P2P 933
- 13.2 La recherche de documents sur Internet 936
 - Rechercher des fichiers Word 937
 - Rechercher des fichiers Excel 939
 - Rechercher des fichiers PowerPoint 943
 - Rechercher des fichiers PDF 944
 - Rechercher des fichiers texte 945
 - Rechercher des fichiers image 947
- 13.3 Les techniques de recherche de logiciels 950
 - Les sites connus de téléchargement de logiciels 950
 - Rechercher des logiciels sur Internet 951
 - Rechercher des logiciels dans les fichiers temporaires 953
 - Rechercher des jeux sur Internet 955
 - Télécharger des DLL 955
- 13.4 Les techniques de recherche de fichiers audio 957
- 13.5 Les techniques de recherche de fichiers vidéo 959
- 13.6 Les rapports de tests de vulnérabilité sur Internet 963
- 13.7 Contre-mesures 964

14**L'ingénierie sociale 965**

- 14.1 Des informations attirantes pour les espions 968
 - Les informations publiques 968
 - Les informations internes 969
 - Les informations privées 969
 - Les informations sensibles 969
- 14.2 Règles générales d'une attaque d'un espion industriel 970
- 14.3 Exemple 1 : manipulation et intrusion à distance 971
 - Histoire d'une entreprise au bord du dépôt de bilan 971
 - Élaboration d'un plan 972
 - Des appels téléphoniques avec une liste de questions clés 972
 - Dépanner un collègue 974
 - Réflexions sur la ruse de l'exemple 1 975
- 14.4 Exemple 2 : manipulation et intrusion avec un complice 977
 - Le harcèlement d'une personne 977
 - L'altération d'une page web 978
 - La manipulation avec un alibi 978
 - Aider un collègue en difficulté 979

Sommaire

	Résultat de la ruse de l'exemple 2	979
14.5	Exemple 3 : intimidation et déséquilibre émotionnel	980
	La vengeance d'un ex-salarié	980
	L'interception illicite	982
	La vente d'un produit à la concurrence	982
	Complice à volonté	984
	La déstabilisation émotionnelle	984
	L'intimidation	985
	Recommandation	986
	Nous sommes là pour vous aider	987
	Fausse panne	989
	Monsieur manipulateur, j'ai besoin de vous	989
	La victime vous fait totalement confiance	990
	Réflexion sur la ruse de l'exemple 3	991
14.6	Exemple 4 : usurpation d'identité et stratégie de la compassion	992
	La poubelle	992
	L'usurpation d'identité	992
	L'accident intentionnel	993
	Entrer dans un endroit sécurisé par la grande porte	993
	La stratégie de la compassion	994
	Réflexion sur la ruse de l'exemple 4	995
14.7	Exemple 5 : fusion	997
	Plan d'action	997
	La fusion des entreprises	997
	Le personnel avec des papiers falsifiés	999
	Les futures occupations de l'espion une fois en poste	1000

15

Le phishing et les vulnérabilités sur Internet 1001

15.1	La technique du phishing	1003
15.2	Se protéger contre les attaques du phishing	1004
	Le navigateur Internet Explorer 7	1004
	Le navigateur Firefox pour Windows	1005
	La barre d'outils Netcraft	1006
15.3	Les objectifs du phishing	1007
	Exemple 1 : le phishing HTTPS	1007
	Description d'une attaque en phishing	1010
	Démonstration d'un cas réel de phishing	1014
	Conseils antiphishing	1018
	Éviter d'être pris au piège par le phishing	1020
15.4	Phishing et usurpation d'identité e-mail	1025
	Test de phishing avec le logiciel Outlook Express	1025

	Conseils pour éviter le phishing par e-mail	1031
15.5	Exemple 2 : les banques en danger	1034
	Séduction	1034
	Détournement d'appel	1036
	Connexion Internet dans une maison vide	1037
	Restauration de la vraie page par l'intermédiaire d'un complice à l'étranger	1038
	Recommandations	1038
	Réflexion sur la ruse de l'exemple 2	1039
15.6	L'altération d'une page web	1040
15.7	Conseil pour effectuer des transactions ou des achats en ligne .	1042
15.8	Les arnaques en ligne : faiblesse humaine et crédulité	1044
15.9	L'e-mail bombing	1047
15.10	Les dangers d'Internet	1047
	Information et désinformation sur Internet	1047
	Les groupes de haine	1047
	L'exploitation sexuelle sur Internet	1048

16

La sécurité des entreprises 1051

16.1	Les tactiques d'attaques courantes	1053
	L'attaque à distance	1054
	La manipulation	1054
16.2	Protéger l'entreprise	1055
16.3	Protéger les informations publiques	1056
	Les achats en ligne	1056
	La ligne téléphonique	1057
	Les annonces publicitaires	1058
	Le personnel et les appels téléphoniques	1058
	Des spams à volonté	1058
	La boîte vocale	1058
	Les procédures pour des envois de colis	1058
16.4	Protéger les informations internes et implémenter le matériel .	1058
	Créer des badges de couleurs différentes	1059
	Les lignes téléphoniques avec différentes sonneries	1059
	Le traçage d'appel	1059
	L'annuaire	1060
	Créer des stratégies de mots de passe complexes	1060
	Installer un antivirus, un antitroyen, un pare-feu	1060
	Les caméras de surveillance	1060
	Masquer les propriétés du système	1060
	Désactiver les outils amovibles	1060

	Couleur et sensibilité des informations	1061
	La photocopieuse	1061
	Configurer le fax, le routeur	1061
	Mettre en place de systèmes biométriques dans des endroits sensibles . .	1062
	La destruction des informations sensibles ou du matériel contenant des informations sensibles	1062
	Configurer le modem	1063
	Protéger les corbeilles à papier et les poubelles	1063
	Les informations internes	1063
	Configurer un réseau sans fil	1063
	Configurer le moniteur réseau	1064
	Installer un pare-feu interne et externe	1064
	Les privilèges des utilisateurs	1065
	Former des employés	1065
	Créer un groupe de gestion des incidents	1065
	Former des salariés	1065
	Les catégories des informations	1067
	Les responsables hiérarchiques	1067
	Diffuser des informations à un tiers	1067
	Éviter la manipulation téléphonique	1068
16.5	Les informations sensibles	1069
16.6	Les tests de vulnérabilité	1070
16.7	Vérifier des antécédents	1073
16.8	Les recommandations aux administrateurs réseaux	1073
16.9	Les recommandations aux utilisateurs	1075
16.10	Sécuriser l'entreprise contre les vulnérabilités Wi-Fi	1076
16.11	Le test de vulnérabilité Scan Modem et le RAS	1080
16.12	Vulnérabilité du pare-feu et protection de NAT	1082
16.13	Protéger un site contre les fuites d'informations	1086
	Stratégie de sécurité	1086
	Test de vulnérabilité de votre site	1091
	Les scanners	1091
	Combattre les robots indiscrets	1091
	Empêcher l'indexation de quelques dossiers et fichiers	1092
	Les fuites d'informations exposées	1094
	Synthèse	1095
17	Des recherches sophistiquées sur Internet	1097
17.1	Trouver des annuaires pour retrouver des personnes et des entreprises .	1099
	Rechercher des professionnels grâce aux pages jaunes	1101
	Rechercher dans les annuaires américains	1102

	Rechercher dans les annuaires africains	1103
	Rechercher des informations dans les pages jaunes du monde	1104
	Faire une recherche inversée de numéros de téléphone	1106
	Rechercher des adresses électroniques	1108
	Trouver des informations grâce aux moteurs de recherche	1109
	Traduire des textes dans les sites web	1112
17.2	Les métamoteurs	1116
	Recherche d'informations	1116
	Recherche cartographique	1116
	Avantages des métamoteurs	1117
17.3	Les moteurs multimédias	1118
17.4	Les moteurs de recherche sécurisés pour vos enfants	1119
17.5	Structurer les mots-clés	1119
	Trouver des sites pour indexer sa page web	1119
	Trouver l'aide en ligne pour créer ses mots-clés	1121
	Utiliser des termes spécifiques	1122
17.6	La syntaxe des moteurs de recherche	1122
	La fonction des symboles	1123
	Combiner les mots-clés avec des symboles	1129
	Résumé de la syntaxe	1132
17.7	Les opérateurs booléens des moteurs de recherche	1133
	L'opérateur booléen NOT	1133
	L'opérateur booléen OR	1134
	Combiner des opérateurs basiques avec des opérateurs booléens et des symboles	1135
	Trouver des sites FTP de téléchargement	1138
	Trouver des fichiers PDF dans la racine d'un site web	1140
	Trouver des fichiers audio, vidéo et des images avec des opérateurs	1141
	Trouver des sites interdits	1142
	Résumé de la syntaxe des opérateurs booléens	1143
17.8	Google et Yahoo : une syntaxe puissante	1143
	Entreprendre des recherches sur Google et à Yahoo, les bases	1144
	Indexer une page web sur Google	1144
	Trouver des pages web par leurs titres	1145
	Trouver des pages web par leur URL	1146
	Trouver des fichiers par leur extension	1152
	Trouver les textes dans les pages web et dans les liens des URL	1153
	Trouver des copies de sauvegarde de pages web	1156
	Trouver des pages selon la date d'apparition	1157
	Trouver les pages similaires d'un site	1159
	Trouver des liens de sites pointant vers d'autres sites	1160
	Trouver des sites sur Internet	1161

Trouver les annuaires	1164
Trouver une liste de numéros de téléphone	1166
Trouver les pages similaires d'un site	1167
Autres moteurs de recherche et opérateurs	1168
Travailler avec des opérateurs dans les groupes de Google et Yahoo	1168
Synthèses des opérateurs de moteurs de recherche	1176

18

ANNEXES 1179

18.1	Réseaux d'ordinateurs et réseaux Internet	1181
	Définitions des réseaux d'ordinateurs	1181
	Topologie d'un réseau	1192
	Classifications du réseau	1197
	Matériel de communication d'un réseau	1199
	Modèle de référence OSI	1204
	Les classes d'adresses	1206
18.2	Glossaire	1212
18.3	Les logiciels	1224
	Scanners	1224
	Traceurs	1225
	Renifleurs	1226
	Renifleurs sans fil	1226
	Crack de mot de passe	1227
	Internet anonyme	1227
	Antimouchards	1228
	Troyens	1228
	Force brute	1229
	Analyseurs de failles	1229
	Cryptage et décryptage	1230
	Stéganographie	1231
	Destructeur de traces	1231
	Récupérateurs de données	1232
	Anti-tout	1232
	Détection d'intrusion	1233
	Les pare feu	1233
	Autres outils utiles	1234
18.4	Lois contre le piratage	1234
	Lois sur la protection intellectuelle (CNIL)	1234
	Articles du code pénal sur le piratage en France	1235

19

Index 1239