

ÍNDICE

ACERCA DE LOS AUTORES.....	15
INTRODUCCIÓN	17
CAPÍTULO 1. SISTEMAS AAA.....	21
1.1 LAS TRES “AES”: AAA	22
1.1.1 Orígenes, descripción y regulación	24
1.1.2 Autenticación	28
1.1.3 Autorización	30
1.1.4 Arqueo	32
1.1.5 Auditoría, la cuarta “A”	34
1.2 MARCO DE AUTORIZACIÓN AAA.....	35
1.3 OTROS PROTOCOLOS AAA.....	39
1.3.1 TACACS, TACACS+	39
1.3.2 Diameter	40
CAPÍTULO 2. RADIUS / 802.1X	43
2.1 INTRODUCCIÓN A RADIUS	44
2.1.1 Orígenes.....	44
2.1.2 Descripción del protocolo.....	46
2.1.3 Especificaciones de RADIUS.....	48
2.1.4 Multiplataforma (GNU-Linux, Windows, Solaris...)	50
2.2 MÉTODOS DE AUTENTICACIÓN	51
2.2.1 Autenticación simple y autenticación mutua.....	54
2.2.2 PAP, CHAP, MS-CHAP y otros sabores	55
2.2.3 Un capítulo para EAP (“o casi”).....	57

2.2.3.1 EAP-MD5.....	59
2.2.3.2 EAP-TLS Y OTROS SABORES SIMILARES.....	60
2.2.3.3 MÉTODOS EAP BASADOS EN TLS.....	60
2.2.3.4 EAP-TTLS.....	62
2.2.3.5 EAP-PEAP.....	63
2.2.3.6 TABLA COMPARATIVA DE TIPOS DE EAP.....	64
2.2.4 Autenticación contra archivo de usuarios.....	66
2.2.5 Autenticación contra el sistema operativo.....	66
2.2.6 Autenticación contra bases de datos.....	67
2.2.7 Autenticación contra Servicios de Directorio.....	68
2.2.8 Reautenticación.....	68
2.3 SHARED SECRET. EL SECRETO MEJOR GUARDADO.....	69
2.4 ATRIBUTOS AVP & VSA. DICCIONARIOS.....	70
2.5 DOMINIOS DE RADIUS (REALMS).....	74
2.6 RADIUS HINTS.....	76
2.7 ESTRUCTURA DE LAS COMUNICACIONES RADIUS.....	76
2.7.1 Formato de mensaje RADIUS. Paquete de datos.....	77
2.7.2 Secuencia de autenticación de RADIUS.....	80
2.8 ÁMBITOS DE UTILIZACIÓN Y ESCALABILIDAD.....	82
2.8.1 Modelos de implantación.....	83
2.9 ESTADÍSTICAS Y LOGS.....	84
2.10 EXTENSIONES DE AUTORIZACIÓN DINÁMICA.....	86
2.11 LIMITACIONES DE RADIUS.....	87
2.12 EL ESTÁNDAR 802.1X.....	88
2.12.1 Capas del modelo OSI (¡Por enésima vez!).....	89
2.12.2 El estándar 802.1x.....	93
2.13 ESTRUCTURA DE LAS COMUNICACIONES EAP.....	98
2.13.1 Formato de mensaje EAP. Paquete de datos.....	98
2.13.2 Secuencias de autenticación EAP.....	100
2.13.3 Ámbitos de aplicación (Enterprise Ethernet).....	104
2.13.4 Modelos de implantación.....	105
2.14 UN CAPÍTULO PARA WI-FI (“O CASI”).....	106
2.14.1 Conceptos de Wi-Fi.....	108
2.14.2 Secuencia de conexión Wi-Fi.....	110
2.14.3 Estructura de una red Wi-Fi.....	111
2.14.4 La seguridad en las redes Wi-Fi.....	114
2.14.4.1 HACKING WI-FI.....	116
2.14.4.2 PROTEGIENDO WI-FI.....	116

CAPÍTULO 3. INFRAESTRUCTURA DE CLAVE PÚBLICA. PKI..... 119

3.1 SISTEMAS CRIPTOGRÁFICOS.....	123
3.1.1 Sistemas de clave simétrica.....	125
3.1.2 Sistemas de clave asimétrica.....	126
3.1.3 Algoritmo RSA para cifrado asimétrico.....	127

3.1.4 Protocolo SSL y TLS.....	128
3.1.5 Algoritmo DH (Diffie Hellman).....	129
3.1.6 Algoritmos de reducción o resumen de mensaje.....	129
3.1.6.1 DEBILIDADES DE LOS ALGORITMOS DE REDUCCIÓN.....	131
3.1.6.2 COLISIONES DE HASH.....	132
3.1.6.3 EJEMPLOS DE HASHES EN VARIOS ALGORITMOS.....	132
3.2 CA. AUTORIDAD CERTIFICADORA.....	133
3.2.1 Tipos de entidades participantes en PKI.....	135
3.2.2 Organismos privados.....	136
3.2.3 Organismos públicos.....	136
3.2.4 Self signing CA o certificados autofirmados.....	137
3.2.5 CA gratuitas.....	137
3.3 SISTEMA BASADO EN LA CONFIANZA (TRUSTED).....	138
3.3.1 Listas incluidas en las aplicaciones y SO.....	140
3.4 REVOCACIÓN DE CERTIFICADOS (CRL).....	140
3.5 FORMATOS Y TIPOS DE CERTIFICADOS.....	143
3.6 FIRMA DIGITAL.....	149
3.6.1 No-repudio.....	152
3.7 SMARTCARDS Y OTROS CRIPTOSISTEMAS.....	152
3.7.1 Una mención especial para el DNle.....	153
3.7.1.1 EL DNle EN LA PRÁCTICA.....	157
3.8 SISTEMAS DE GESTIÓN DE CERTIFICADOS.....	159

CAPÍTULO 4. APLICACIÓN REAL. UBUNTU+FREEERADIUS..... 161

4.1 ¿POR QUÉ GNU/LINUX? ¿POR QUÉ NO WINDOWS?.....	162
4.2 ¿POR QUÉ FREEERADIUS?.....	163
4.2.1 Características de FreeRADIUS 2.....	165
4.2.2 Aplicación en el mundo real.....	167
4.3 INSTALACIÓN DE UBUNTU SERVER LINUX 8.04.....	169
4.3.1 Descargar y grabar la ISO de Ubuntu.....	169
4.3.2 Instalación de Ubuntu Server 8.04 desde cero.....	170
4.3.3 Nuestro primer arranque.....	184
4.3.4 Configuración de la red.....	186
4.3.5 Actualizar nuestro servidor con los últimos parches.....	188
4.3.6 Algunas teclas básicas del editor nano.....	189
4.4 HERRAMIENTA DE ADMINISTRACIÓN: WEBMIN.....	190
4.4.1 Instalación de Webmin.....	190
4.5 PUTTY COMO CONSOLA REMOTA DE TEXTO.....	194
4.6 SERVIDOR Y CLIENTE NTP.....	196
4.7 PRIMEROS PASOS CON FREEERADIUS.....	198
4.7.1 Instalación de FreeRADIUS 2 desde nuestro DVD.....	199
4.7.2 Cómo compilamos los binarios incluidos en el CD-ROM.....	200
4.7.3 Bloquear FreeRADIUS para que NO se actualice.....	202
4.7.4 Arranque de FreeRADIUS.....	203
4.7.5 Configuración básica de FreeRADIUS.....	206

4.7.5.1	FREERADIUS Y LOS ATRIBUTOS	206
4.7.5.2	ARCHIVOS DE CONFIGURACIÓN.....	207
4.7.5.3	UNLANG. EL LENGUAJE DE FREERADIUS	237
4.7.6	Primer test de funcionamiento	246
4.7.6.1	TEST DE AUTENTICACIÓN SOBRE EL SISTEMA	248
4.7.6.2	TEST DE AUTENTICACIÓN MEDIANTE CHAP	249
4.7.7	Forzar el final de una sesión de usuario conectada	253
4.7.8	Base de datos MySQL	254
4.7.8.1	ADMINISTRACIÓN DEL DAEMON MYSQL	254
4.7.8.2	SENTENCIAS BÁSICAS DE SQL	255
4.7.8.3	PREPARANDO MYSQL PARA FREERADIUS.....	267
4.7.8.4	CONFIGURACIÓN DE SQL EN FREERADIUS	270
4.7.8.5	TEST DE AUTENTICACIÓN SOBRE MYSQL	273
4.7.8.6	REDUNDANCIA Y COPIA DE SEGURIDAD MYSQL.....	278
4.7.9	Introducción a OpenSSL	280
4.7.9.1	INSTALACIÓN DE OPENSLL.....	286
4.7.9.2	CONFIGURACIÓN DE OPENSLL	287
4.7.9.3	CREACIÓN DE MI AUTORIDAD CERTIFICADORA RAÍZ	290
4.7.9.4	OBTENCIÓN DE UN CERTIFICADO DE SERVIDOR	292
4.7.9.5	NOMBRES DE ARCHIVO UTILIZADOS.....	298
4.7.9.6	CONFIGURACIÓN DE CERTIFICADOS EN FREEERADIUS	299
4.7.9.7	OBTENCIÓN DE UN CERTIFICADO DE CLIENTE.....	301
4.7.9.8	REVOCACIÓN DE CERTIFICADOS EN OPENSLL	303
4.7.9.9	OCSP MEDIANTE OPENSLL.....	306
4.7.9.10	CONFIGURACIÓN DE CRL PARA FREERADIUS	315
4.7.9.11	OBTENCIÓN AUTOMÁTICA DE CERTIFICADOS EN FREEERADIUS 2	316
4.7.9.12	TEST DE AUTENTICACIÓN SOBRE EAP	319
4.7.10	Configurando Apache2.....	326
4.7.11	Administrador FreeRADIUS Dialup-Admin.....	331
4.7.11.1	PRIMEROS PASOS CON DIALUP-ADMIN	334
4.7.12	Administrando FreeRADIUS con phpRADmin.....	337
4.7.12.1	INSTALACIÓN Y CONFIGURACIÓN DE PHPRADMIN	338
4.7.12.2	DEPURACIÓN DE ERRORES DE PHPRADMIN	341
4.7.12.3	CONFIGURACIÓN DE PHPRADMIN.....	342
4.7.12.4	CONFIGURACIÓN DE TAREAS DE PHPRADMIN	349
4.7.12.5	GESTIÓN DE CERTIFICADOS DESDE PHPRADMIN	349
4.7.13	Otros administradores para FreeRADIUS.....	352
4.7.14	FreeRADIUS y OpenLDAP	354
4.7.15	FreeRADIUS y Active Directory	366
4.7.16	Clientes Java para RADIUS	366
4.7.17	Suplicante para Linux. Wpa_supplicant.....	368
4.7.18	PAM. Autenticación avanzada en Linux	372
4.8	SERVIDOR DHCP	376
4.8.1	Instalación de DHCP3-Server	377
4.8.2	Configuración de DHCP3-Server.....	377
4.8.3	FreeRADIUS y DHCP.....	378

CAPÍTULO 5. APLICACIÓN REAL: WINDOWS SERVER + IAS	383
5.1 ¿POR QUÉ WINDOWS? ¿POR QUÉ NO LINUX?	384
5.1.1 Windows Server. Introducción	385
5.1.2 Active Directory	386
5.2 MICROSOFT IAS. EL RADIUS DE MICROSOFT	386
5.2.1 Instalación y Configuración de Windows 2003 Server	389
5.2.2 Procedimiento de instalación de Microsoft IAS	396
5.2.3 Configuración de IAS	397
5.2.3.1 CONFIGURACIÓN PRÁCTICA DE IAS	400
5.2.3.2 CREACIÓN DE UN USUARIO DE PRUEBA	415
5.2.4 Primer test de funcionamiento	417
5.2.4.1 TROUBLESHOOTING O SOLUCIÓN DE PROBLEMAS	424
5.2.5 Autoridad Certificadora Raíz de Windows Server	427
5.2.5.1 INSTALACIÓN DE UNA CA RAÍZ DE WINDOWS SERVER	429
5.2.5.2 INSTALACIÓN Y CONFIGURACIÓN DE IIS PARA LA GENERACIÓN DE CERTIFICADOS	437
5.2.5.3 EMISIÓN DE CERTIFICADOS SELF-SIGNED	444
5.2.5.4 COPIA DE SEGURIDAD DE CERTIFICATE SERVER	450
5.2.5.5 REPOSITARIOS DE CERTIFICADOS EN WINDOWS	452
5.2.5.6 IMPORTACIÓN DE CERTIFICADOS. PROCEDIMIENTO	453
5.2.5.7 REVOCACIÓN DE CERTIFICADOS	456
5.2.6 Configuración IAS para clientes Inalámbricos Wi-Fi	457
5.2.6.1 POLÍTICAS DE GRUPO	465
5.2.6.2 CONFIGURACIÓN Y DIVULGACIÓN DE LAS GPO	466
5.2.7 El protocolo 802.1x en Windows	475
5.2.8 Suplicante de Windows. Limitaciones	476
5.2.8.1 PROCEDIMIENTO DE CONFIGURACIÓN Y USO	477
5.2.9 Otras opciones de suplicantes libres y de pago	481
5.2.10 Limitaciones de IAS	485
CAPÍTULO 6. APLICACIÓN REAL. CONFIGURANDO UN NAS.....	487
6.1 TIPOS DE EQUIPOS NAS	487
6.2 CLIENTES DE UN NAS O SUPPLICANTES	490
6.3 CONFIGURACIÓN REAL AP LINKSYS	493
6.4 CONFIGURACIÓN REAL AP CISCO	499
CAPÍTULO 7. SEGURIDAD AVANZADA EN RADIUS.....	505
7.1 VULNERABILIDADES	505
7.1.1 Vulnerabilidades clásicas de RADIUS	506
7.1.2 Vulnerabilidad DoS en RADIUS	508

- 7.1.3 Vulnerabilidad 802.IX 509
- 7.1.4 Vulnerabilidad OpenSSL..... 511
- 7.1.5 Vulnerabilidad en certificados de Windows..... 512
- 7.2 HACKING RADIUS 513
 - 7.2.1 Técnicas utilizadas en los ataques de Hackers 514
 - 7.2.2 Principales tipos de ataques utilizados 516
 - 7.2.3 Hacking MD5 en RADIUS..... 518
 - 7.2.4 Ataque FreeRADIUS-WPE a EAP..... 522
- 7.3 ARQUITECTURA DE RED RECOMENDADA 526
- REFORZANDO A LINUX 528
 - 7.3.1 Los usuarios en Linux..... 529
 - 7.3.2 Los grupos de usuarios en Linux..... 534
 - 7.3.3 Administrando los permisos 535
 - 7.3.4 Permisos especiales 540
 - 7.3.5 IPTables. Cortafuegos..... 543
 - 7.3.5.1 PRIMEROS PASOS..... 543
 - 7.3.5.2 CREANDO EL FIREWALL 548
 - 7.3.5.3 INSTALANDO EL FIREWALL 551
- 7.4 ¿REFORZANDO WINDOWS? 554
 - 7.4.1 Seguridad de infraestructura de red IAS..... 554
 - 7.4.2 Reglas de filtrado de TCP para IAS 557
- 7.5 CONCLUSIÓN..... 558

CAPÍTULO 8. TABLAS Y REFERENCIAS DE VALOR..... 559

- 8.1 LISTA DE ARCHIVOS Y CARPETAS DEL DVD..... 559
- 8.2 GUÍA BÁSICA DE COMANDOS LINUX 563
- 8.3 INSTALACIÓN Y FUNCIONAMIENTO DE VMWARE 569
- 8.4 TIPOS DE PAQUETES DE RADIUS..... 574
- 8.5 DISECCIÓN DE UN PAQUETE DE DATOS RADIUS 574
- 8.6 DISECCIÓN DE UN PAQUETE DE DATOS EAP..... 576
- 8.7 EJEMPLO DE INFORMACIÓN DE ACCOUNTING..... 577
- 8.8 EJEMPLO DE DEBUG TRACE DE FREERADIUS 2..... 577
- 8.9 USUARIOS Y CONTRASEÑAS PARA PRUEBAS..... 583
- 8.10 SECUENCIA EAP-PEAP-MSCHAPV2..... 584
- 8.11 EJEMPLO DE UN CERTIFICADO..... 598
- 8.12 COMANDOS IMPORTANTES OPENSLL 600
- 8.13 COMPARATIVA DE RECURSOS UBUNTU/ WINDOWS..... 602
- 8.14 ARCHIVOS Y DIRECTORIOS DE FREERADIUS 603
- 8.15 ARCHIVOS Y DIRECTORIOS DE OPENSLL 605
- 8.16 ESQUEMA DE LA BASE DE DATOS MYSQL EN FREERADIUS..... 605
- 8.17 EJEMPLOS DE HASHES 608
- 8.18 ATRIBUTOS DE RADIUS 608
 - 8.18.1 AVP estándar de RADIUS 608
 - 8.18.2 Lista alfabética de AVP estándar de RADIUS..... 623
 - 8.18.3 Ejemplo de diccionario de Fabricante. VSA 626

8.19 LISTA DE RFC DE INTERÉS..... 628
8.20 ENLACES DE INTERÉS..... 630
8.21 LISTA DE SERVIDORES 630
ÍNDICE ALFABÉTICO..... 633