«به نام خدا»

Subject : 9531014

Year : Month : Date :

تمرین 4 امنیت

امیرمحمد پیرحسنلو

Threats	consequences
integrity تغییر داده کاربر تغییر حافظه ماشین تغییر ترافیک پیام های در حال ارسال	از دست رفتن داده به خطر افتادن کامپیوتر دروازه برای ورود سایر تهدیدها
confidentiality استراق سمع بسته ها دزدی اطلاعات client ها و server دستیابی به اطلاعات پیکربندی شبکه ~~اطلاعات مربوط به~~ " " فهمیدن این که کدام کاربران با سرور در حال ارتباط هستند.	از دست رفتن اعتبار داده ها " " " حریم شخصی
Denial of service مشغول کردن سرورها با تعداد زیادی request غیرمفید اشباع کردن memory و disk کامپیوتر (server) از دست رس خارج کردن سرور با حمله به DNS	مشغول شدن الکی سرور آزاد client ها جلوگیری از انجام کار معطل client
Authentication شخص دیگر جا زدن خودجای ایجاد داده‌ی ساختگی	اشتباه گرفتن attacker با کاربر اصلی اعتماد کردن به داده های نادرست.

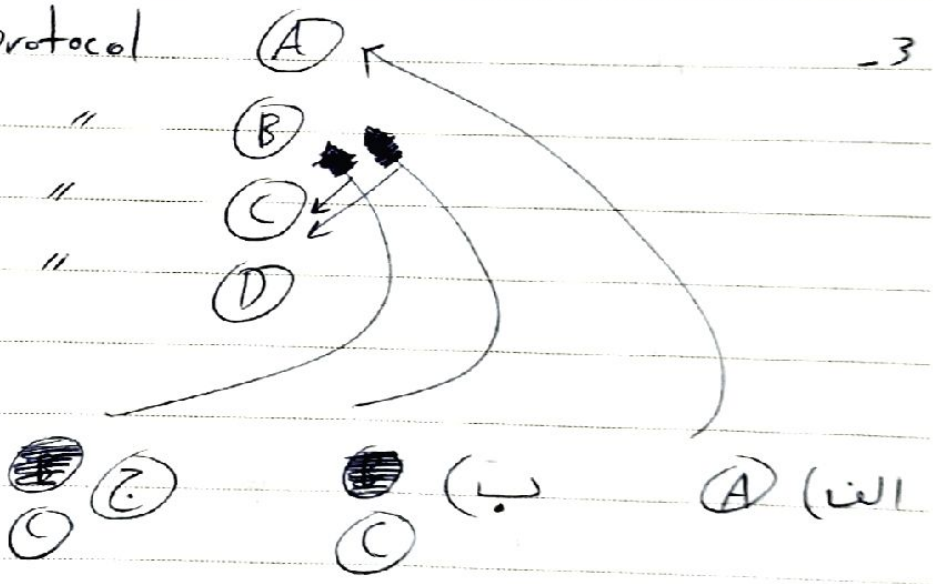
Subject :
Year : | Month : Date :

2- connection : اتصالی که از طریق آن سرویس ارائه می شود. هر connection به یک session مربوط می شود. connection به صورت end to end بین دو peer است.

session : یک ارتباط بین client و server است. با پروتکل hand shake ساخته می شوند. در هر session یک سری پارامترهای رمزنگاری و رمزگشایی وجود دارد که بین connection های یک session به اشتراک گذاشته می شوند.

3-

SSL handshake protocol
" Alert "
" Record "
" change spec "
cipher



4- الف) session ب) X11 ج) direct_tcpip

5- پاسخ صفحه بعد

	Transport Mode	Tunnel Mode
AH	احراز هویت IP payload و قسمت انتخاب شده از هدر IP و هدر های IPV6	احراز هویت هدر + IP payload بسته داخلی + قسمت های انتخابی هدر IP بیرونی و هدر های IPV6 بیرونی
ESP	رمزنگاری IP payload و هدرهای IPV6 و هدرهای ESP	رمزنگاری بسته IP درون

الف) Next Header (8 بیت) : مشخص کردن نوع داده‌ی payload به وسیله ⑥
مشخص کردن اولین هدر در آن payload.

ب) payload length (16 بیت): طول payload برحسب بایت تمامل هدرهای generic را نشان می دهد.

ج) reserved (7 بیت): برای استفاده‌های آتی

د) sequence number (32 بیت): یک شمارنده‌ی افزایشی که برای جلوگیری از replay Attack از آن استفاده می شود.

Year : Month : Date :

7- ⓐ manual : ادمین سیستم دستی کلید های مرسیستم را ست می‌کند.
برای محیط های کوچک مناسب است.

ⓑ automated : یک سیستم خودکار با توجه به تقاضاها ساخت کلید برای SA
ها را برعهده می‌گیرد. برای محیط های در حال رشد و توسعه مناسب است و کار را
ساده می‌کند.

Subject :

Year : Month : Date :

(8) روی هر سه سیستم عامل windows، linux و mac پشتیبانی می شود.
الگوریتم های رمزنگاری موجود در آن به شدت امن هستند.
با SMTP ، نمی توان executable file ارسال کرد.
" " ، داده ی متنی حاوی کاراکترهای زبان های بین المللی (غیر اسکی) را نمی توان ارسال کرد.
سرورهای SMTP ، پیام mail با طول بیشتر از یک مقدار خاص را reject می کنند.
خطای ترجمه هنگام ترجمه EBCDIC به ASCII را گیت وی های SMTP وجود دارد.
پیاده سازی SMTP به صورت کامل مطابق با RFC 821 نیست و مشکلات زیر را دارد:
در قسمت های زیر
(a) تبدیل tab به space
(b) padd کردن خط ها به طول یکسان
(c) حذف کردن space و tab های آخر خط ها
(d) اضافه کردن و پاک کردن کاراکترهای CR و LF

الگوریتم های رمزنگاری مورد استفاده در PGP:
message encryption → CAST - IDEA - 3DES with Diffie-Hellman - RSA
digital signature → DSS - RSA

(9) فشرده سازی : پیام به همراه MAC آن که توسط کلید خصوصی ارسال کننده رمز شده است، فشرده می شود، سپس رمزی می شود. الگوریتم مورد استفاده ZIP است و به طور میانگین حجم داده را نصف می کند.

سازگاری: از آن جایی که خروجی PGP بعد قسمت رمزنگاری حاوی بلاک های داده ی 8 بیتی است، اگر mail system ها اجازه ی عبور داده با

Subject :

Year : Month : Date :

بلاک های حاوی کد ASCII می دهند. با استفاده از الگوریتم Radix64 هر 3 بایت از داده رمزشده را به 4 بلاک 8 بیتی که حاوی کاراکترهای ASCII هستند تبدیل می کنیم. این جا حجم داده ما $\frac{4}{3}$ برابر می شود ولی ZIP کردن داده در ادامه حجم آن را $\frac{1}{2}$ می کند.