بنام خدا

تمرین سری ۲ درس امنیت شبکه (صیاد)

۱. طرح Diffie-Hellman را با q=11 و α=7 در نظر بگیرید.

30% الف) اگر کاربر A قسمت عمومی کلید اش $Y_A=3$ باشد، کلید خصوصی وی (X_A) چیست؟ آیا روش ساده ای برای این کار در حالت کلی وجود دارد؟

30% ب) اگر قسمت عمومی کلید کاربر B $Y_B=5$ باشد، کلید مشترک K_{AB} چیست؟

40% ج) اگر α=3 باشد، در صورت امکان مساله را با مقادیر فوق حل کنید، در غیر اینصورت توضیح دهید.

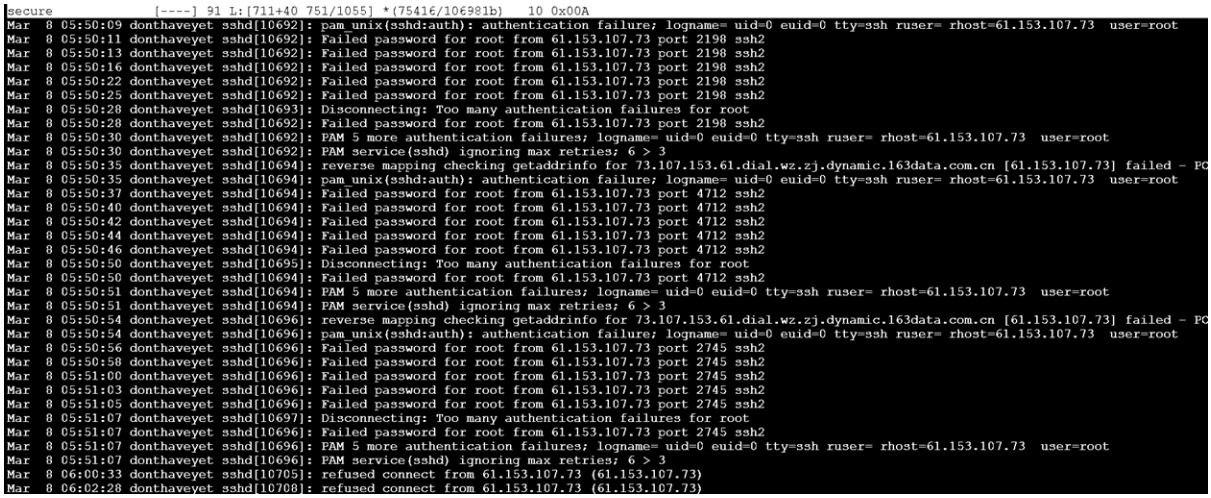
۲. آنچه در این مساله میبینید یک سناریوی واقعی است! این log یک سرور است که یک وبسایت را روی سیستم عامل CentOS میزبانی میکند. دسترسی به این سرور از راه دور با ssh امکانپذیر است و بنابراین پورت آن برای استفاده باز گذاشته شده است. هرچند برای اتصال به آن باید احراز هویت شد.

40% الف) ۱) با بررسی log اول بگویید چه اتفاقی در حال رخ دادن است؟ ۲) آیا میتوانید بگویید حمله از کدام کشور انجام شده است؟ (از سرویس whois برای IP استفاده کنید).

30% ب) بنظر شما برای افزایش امنیت و مقابله با حمله چه میتوان کرد؟

```
secure            [----] 89 L:[935+40  975/1055] *(99416/106981b)   10 0x00A
Mar  8 22:11:52 donthaveyet sshd[11294]: reverse mapping checking getaddrinfo for host.mayl.ir [179.43.144.2] failed - POSSIBLE BREAK-IN ATTEMPT!
Mar  8 22:11:52 donthaveyet sshd[11294]: Invalid user jhow from 179.43.144.2
Mar  8 22:11:52 donthaveyet sshd[11295]: input_userauth_request: invalid user jhow
Mar  8 22:11:52 donthaveyet sshd[11294]: pam_unix(sshd:auth): check pass; user unknown
Mar  8 22:11:52 donthaveyet sshd[11294]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=179.43.144.2.
Mar  8 22:11:54 donthaveyet sshd[11294]: Failed password for invalid user jhow from 179.43.144.2 port 46870 ssh2
Mar  8 22:11:54 donthaveyet sshd[11295]: Received disconnect from 179.43.144.2: 11: Bye Bye
Mar  8 22:11:56 donthaveyet sshd[11296]: reverse mapping checking getaddrinfo for host.mayl.ir [179.43.144.2] failed - POSSIBLE BREAK-IN ATTEMPT!
Mar  8 22:11:56 donthaveyet sshd[11296]: Invalid user larissa from 179.43.144.2
Mar  8 22:11:56 donthaveyet sshd[11297]: input_userauth_request: invalid user larissa
Mar  8 22:11:56 donthaveyet sshd[11296]: pam_unix(sshd:auth): check pass; user unknown
Mar  8 22:11:56 donthaveyet sshd[11296]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=179.43.144.2.
Mar  8 22:11:58 donthaveyet sshd[11296]: Failed password for invalid user larissa from 179.43.144.2 port 47523 ssh2
Mar  8 22:11:58 donthaveyet sshd[11297]: Received disconnect from 179.43.144.2: 11: Bye Bye
Mar  8 22:12:01 donthaveyet sshd[11298]: reverse mapping checking getaddrinfo for host.mayl.ir [179.43.144.2] failed - POSSIBLE BREAK-IN ATTEMPT!
Mar  8 22:12:01 donthaveyet sshd[11298]: Invalid user larisa from 179.43.144.2
Mar  8 22:12:01 donthaveyet sshd[11299]: input_userauth_request: invalid user larisa
Mar  8 22:12:01 donthaveyet sshd[11298]: pam_unix(sshd:auth): check pass; user unknown
Mar  8 22:12:01 donthaveyet sshd[11298]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=179.43.144.2.
Mar  8 22:12:03 donthaveyet sshd[11298]: Failed password for invalid user larisa from 179.43.144.2 port 48013 ssh2
Mar  8 22:12:04 donthaveyet sshd[11299]: Received disconnect from 179.43.144.2: 11: Bye Bye
Mar  8 22:12:09 donthaveyet sshd[11300]: reverse mapping checking getaddrinfo for host.mayl.ir [179.43.144.2] failed - POSSIBLE BREAK-IN ATTEMPT!
Mar  8 22:12:09 donthaveyet sshd[11300]: Invalid user wulei from 179.43.144.2
Mar  8 22:12:09 donthaveyet sshd[11301]: input_userauth_request: invalid user wulei
Mar  8 22:12:09 donthaveyet sshd[11300]: pam_unix(sshd:auth): check pass; user unknown
Mar  8 22:12:09 donthaveyet sshd[11300]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=179.43.144.2.
Mar  8 22:12:10 donthaveyet sshd[11300]: Failed password for invalid user wulei from 179.43.144.2 port 48891 ssh2
Mar  8 22:12:11 donthaveyet sshd[11301]: Received disconnect from 179.43.144.2: 11: Bye Bye
```

30% ج) ما یک مکانیزم امنیتی با استفاده از iptables به سرور افزوده ایم که اثر حمله را تخفیف دهد. Log بعدی نیز مورد مشکوکی را نشان میدهد و عکس العمل این مکانیزم هم در آن دیده میشود. ۱) می توانید حدس بزنید چه اتفاقی در حال رخ دادن بوده و این مکانیزم اضافه شده چه بوده است؟ ۲) آیا میتوانید مشخص کنید که حمله از سمت کدام کشور شده است؟



شما اولین ماموریت جرم شناسی رایانه ای خود را انجام دادید!

۳. شبکه ای را در نظر بگیرید که در آن کاربران همگی به سرور S متصل می شوند تا برای ارتباط با همدیگر از سرور S کلید مسترک مخفی بگیرند. هر کاربر x با سرور یک کلید کشترک مخفی به نام K_x دارد. تمام پیغام های بن کاربران و سرور با این کلید مشترک K_x رمز می شود.

فرض کنید کاربر A میخواهد با کاربر B پیغام M را به صورت رمز شده بفرستد. برای این کار نیاز به کلید مشترک R بین خود و B دارد. این کلید طبق پروتکل زیر تولید می شود.

A -> S: A,B,E(K_a , R)

S -> A: E(K_b , R)

A -> B: E(K_b , R), E(R,M)

40% الف) توضیح دهید هر خط از این پروتکل به چه دلیل انجام می شود؟

60% ب) آیا هکر Z قادر است به پیغام M دسترسی پیدا کند؟ در صورت پاسخ مثبت مراحل حمله را بنویسید و در صورت پاسخ منفی توضیح دهید چرا نمیتواند.

۴. پروتکل زیر را که به A و B اجازه میدهد کلید جلسه (Session key) تازه ای مانند K'_{AB} بسازند در نظر بگیرید. فرض میکنیم که ایندو کاربر قبلا کلید بلند مدت K_{AB} را با هم بطور مشترک داشته اند.

1. $A \rightarrow B: A, N_A$
2. $B \rightarrow A: \mathrm{E}(K_{AB}, [N_A, K'_{AB}])$
3. $A \rightarrow B: \mathrm{E}(K'_{AB}, N_A)$

30% الف) ابتدا سعی میکنیم تا مقصود طراح پروتکل را بفهمیم.

- چرا A و B در انتهای اجرای پروتکل فکر میکنند که کلید K'_{AB} را با طرف مقابلشان به اشتراک گذاشته اند؟
- چطور فرض میکنند که این کلید جدید (Fresh) است؟

در هر دو حالت باید هم برای A و هم برای B استدلال ارائه کنید. به شکل زیر:

A فکر میکند که با B کلید K'_{AB} را به اشتراک گذاشته چراکه .....

B فکر میکند که با A کلید K'_{AB} را به اشتراک گذاشته چراکه .....

A فکر میکند که K'_{AB} جدید است چراکه .....

B فکر میکند که K'_{AB} جدید است چراکه .....

50% ب) حال فرض کنید که کانال intercept شده است و دشمن در میانه راه نشسته است. A میخواهد با B پروتکل را مانند قبل اجرا کند اما C در میانه راه نشسته و پروتکل را از جانب B اجرا کرده و A فکر میکند که کلید جدیدی با B ساخته است در حالی که تنها با C مشغول تراکنش بوده است. اگر هر دو طرف بتوانند از طرف مقابلشان بخواهند که کلید را refresh کند، نشان دهید چگونه مراحل این حمله انجام میشود. از این حمله نتیجه میشود که فرض طرفین در قسمت الف خدشه دار است.

20% ج) تغییری مختصر در پروتکل میتواند این حمله را ناکام بگذارد. راه حلی برای جلوگیری از این حمله پیشنهاد کنید.

۵. یک روش احراز هویت یک طرفه را که بر پایه رمز نگاری نامتقارن بنا نهاده شده است در نظر بگیرید:

$$\begin{aligned} &\mathrm{A} \rightarrow \mathrm{B}: \quad ID_A \\ &\mathrm{B} \rightarrow \mathrm{A}: \quad R_1 \\ &\mathrm{A} \rightarrow \mathrm{B}: \quad \mathrm{E}(PR_a, R_1) \end{aligned}$$

30% الف) پروتکل را توضیح دهید.

70% ب) چه نوع حمله ای به این پروتکل کارگر است؟ (غیر از حملات پایه ای به الگوریتمهای رمزنگاری و DoS)

۶. ۱۶بیت اول hash پیام در امضای PGP بصورت Plaintext کنار امضا منتقل میشوند،

الف) تا چه اندازه این کار امنیت الگوریتم Hash را به مخاطره می اندازد؟ توضیح دهید

ب) تا چه اندازه (با چه احتمالی) این تدبیر، کاری که قرار است انجام دهد را محقق میکند؟ (یعنی کمک کند تا تعیین کنیم که آیا کلید RSA درستی برای بازگشایی hash پیام استفاده شده است یا نه)