禪

تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بینالمللی

آموزش رایگان دوره Network+، امنیت در طراحی شبکهها (بخش 54)

۵۴
Acceptable Use Policy، privileged user agreement، امنیت در طراحی شبکهها، پروکسی سرورها، Access Control List
CompTIA
Network+
شبکه
آموزش رایگان دوره Network+

در شماره گذشته آموزش نتورکپلاس با امنیت فیزیکی، Hashing، پروتکل SHA و خطمشیهای امنیتی مدیریت آشنا شدیم، در این شماره مبحث فوق را خاتمه داده و به سراغ امنیت در شبکهها خواهیم رفت .

برای مطالعه بخش پنجاه و سوم آموزش رایگان و جامع نتورک پلاس **(Network+)** اینجا کلیک کنید

Bring Your Own Device

دستگاه خود را بیاورید **(BYOD)** سرنام **Bring Your Own Device** اشاره به وضعیتی دارد که مردم میتوانند گوشیهای هوشمند، لپتاپها یا سایر تجهیزات هوشمند خود را به منظور انجام کار یا مسئولیتهایی که به عهده دارند به مدرسه یا محیط کار بیاورند . در این زمینه شما با چهار اصطلاح زیر روبرو میشوید :

- نرمافزار خود را بیاورید BYOA □□□□□bring your own application - کارکنان یا دانشآموزان از نرمافزاری که روی کامپیوتر یا گوشی هوشمند ذخیره کردهاند استفاده میکنند .

- ابر خود را بیاورید BYOC سرنام bring your own cloud- کارکنان یا دانشجویان از برنامه ابری یا سرویس ذخیرهسازی خود استفاده میکنند.

• [illegible] BYOT [illegible] bring your own technology – [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] BYO [illegible].

• [illegible] CYOD [illegible] choose your own device -[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible].

[illegible] [illegible] BYOD [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]

.[illegible]

[illegible]

[illegible]

Network Security Devices

[illegible] IDS / IPS [illegible] ACL [illegible]

[illegible]

[illegible] OSI [illegible] (firewall) [illegible]:

[illegible] 1: [illegible].

[illegible] 2: [illegible].

[illegible] 3: [illegible].

[illegible] 4: [illegible] (firewall) [illegible].

[illegible].

Access Control List

Access Control Lists (**ACL**)

- (ICMP או IP כתובת מקור)
- (UDP או TCP כתובת מקור)
- IP כתובת
- UDP או TCP כתובת

• ICMP

access-list acl_2 permit icmp any any

• ICMP

access-list acl_2 deny icmp any any

• TCP 2.2.2.2 5.5.5.5

access-list acl_2 permit tcp host 2.2.2.2 host 5.5.5.5

• TCP 2.2.2.2 3.3.3.3 80 ("www" "equal to" "eq")

access-list acl_2 permit tcp host 2.2.2.2 host 3.3.3.3 eq www

(wildcard) wildcard mask 0 1 0.0.0.255 wildcard 00000000.00000000.00000000.11111111

با آدرس شبکه مطابقت داشته باشد و آخرین اکتت میتواند هر مقداری باشد . دستور زیر به ترافیک TCP اجازه میدهد زمانی که سه اکتت اول یک آدرس آیپی 10.1.1 هستند، صرفنظر از هر مقداری که اکتت آخر دارد، انتقال پیدا کنند .

```
access-list acl_2 permit tcp 10.1.1.0 0.0.0.255
```

توجه داشته باشید که یک فهرست دسترسی بهطور خودکار روی روتر ایجاد نمیشود، زمانی که روتر فاقد ACL باشد، اجازه میدهد ترافیک انتقال پیدا کند . برای اطلاعات بیشتر در خصوص ACL به مقاله **Access Control Lists** مراجعه کنید .

در شماره آینده آموزش نتورکپلاس به سراغ مبحث دیوارهای آتش خواهیم رفت .

نویسنده :
حمیدرضا تائبی
دسته بندی:
فناوری شبکه
تاریخ انتشار :
11:30 - 04/03/1398

برچسب:
آموزش رایگان شبکه - دوره رایگان نتورک پلاس - دوره نتورک پلاس - آموزش نتورک پلاس - آموزش رایگان دوره نتورک پلاس - آموزش دوره نتورک پلاس - آموزش رایگان Bring Your Own+ - Network+ - Network Acceptable Use Policy - Device - پروکسی سرورها - Access Control List - امنیت شبکه - امنیت شبکه بیسیم - امنیت در طراحی شبکه

نشانی
□□□□:https://www.shabakeh-mag.com/networking-technology/15404/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87-network%D8%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%AF%D8%B1-%D8%B7%D8%B1%D8%A7%D8%AD%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7-%D8%A8%D8%AE%D8%B4-54