禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی – 09

آموزش CEH (هکر کلاه سفید): آشنایی با آناتومی پروتکل TCP / IP و ضعفهای امنیتی آن

CEH
TM
CERTIFIED ETHICAL HACKER

TCP / IP پایه و اساس شبکههای مدرن امروزی است. از بسیاری جهات، میتوانید به صراحت اعلام کنید که TCP / IP همگام با اینترنت توسعه پیدا کرده است. تاریخچه این پروتکل به سال 1982 و زمانی باز میگردد که به عنوان استانداردی توسط وزارت دفاع ایالات متحده به تصویب رسید. در ابتدا، مدل TCP / IP به عنوان مجموعهای از پروتکلهای انعطافپذیر و با قابلیت تحمل بالا در برابر خطاها در شبکه تعریف شد. در آن زمان سازمانها به پروتکلی احتیاج داشتند که آستانه تحمل بالایی در برابر خطاها داشته باشد تا گرههای شبکه بتوانند اطلاعات را میان یکدیگر مبادله کنند.

برای مطالعه قسمت قبل آموزش رایگان دوره **CEH** اینجا کلیک کنید.

آناتومی پروتکل TCP / IP

چهار پروتکل اصلی TCP / IP عبارتند از پروتکل اینترنت (IP)، پروتکل کنترل انتقال (TCP)، پروتکل دیتاگرام کاربر (UDP) و پروتکل کنترل پیامهای اینترنتی (ICMP). این پروتکلها زیربنایی هستند و باید توسط هر دستگاهی که قصد دارد اطلاعاتی را در یک شبکه مبتنی بر TCP / IP مبادله کند پشتیبانی شوند. هر پروتکل هدف مشخصی را ارائه میدهد. به همین دلیل لازم است حداقل اطلاعات اولیه در مورد عملکرد این پروتکلها داشته باشید. شکل زیر چهار لایه پشته TCP / IP را نشان میدهد. در شکل زیر لایههای کاربرد، میزبان به میزبان، اینترنت و دسترسی به شبکه را مشاهده میکنید که عملکرد هر یک به شرح زیر است:

.TCP / IP ,ةيلاتلا ةيعرفلا ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه .ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه TCP / IP .ةيلاتلا ةيعرفلا ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه 1982 ذنم ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه TCP / IP .ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه .ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه IP .ةكبشلا ىلع ةيلمعلا ةمظنألا ةعومجم ىلع قلطي حلطصم وه

```
Num   Source Address    Dest Address   Summary
21    192.168.123.101   68.94.156.1    DNS: Standard query A www.hackwire.com

⊞ Frame 21 (76 bytes on wire, 76 bytes captured)
⊞ Ethernet II, Src: 00:09:5b:1f:26:58, Dst: 00:00:94:c6:0c:4f
⊞ Internet Protocol, Src Addr: 192.168.123.101 (192.168.123.101), Dst Addr: 68.94.156.1 (68.94.156.1)
⊞ User Datagram Protocol, Src Port: 1904 (1904), Dst Port: domain (53)
⊞ Domain Name System (query)

0000:  00 00 94 C6 0C 4F 00 09 5B 1F 26 58 08 00 45 00   .....O..[.&X..E.
0010:  00 3E 97 1C 00 00 80 11 00 00 C0 A8 7B 65 44 5E   .>..........{eD^
0020:  9C 01 07 70 00 35 00 2A C6 E4 24 89 01 00 00 01   ...p.5.*..$.....
0030:  00 00 00 00 00 00 03 77 77 77 08 68 61 63 6B 77   .......www.hackw
0040:  69 72 65 03 63 6F 6D 00 00 01 00 01               ire.com.....
```

اجازه دهید به هر یک از چهار لایه TCP / IP نگاهی کرده و مخاطرات امنیتی پیرامون هر لایه و پروتکلهای آنرا بررسی کنیم . چهار لایه TCP / IP به شرح زیر است:

- ■ The application layer
- ■ The transport or host-to-host layer
- ■ The Internet layer
- ■ The network access layer

لایه کاربرد (Application Layer)

لایه کاربرد در بالای پشته این پروتکل قرار دارد . این لایه مسئولیت پشتیبانی از برنامهها را بر عهده دارد . برنامه ها معمولاً نه به نام، بلکه توسط درگاه /پورت مربوطه شناسایی میشوند. پورتها درون بستههای TCP و UDP قرار میگیرند تا برنامه بتواند به پروتکل موردنظر دست پیدا کند . البته این احتمال وجود دارد که یک سرویس خاص دارای پورت اختصاصی باشد، اما سرویسها میتوانند به درگاههای دیگر نیز گوش (listen) دهند. یک نمونه رایج در این زمینه پروتکل ساده انتقال ایمیل (SMTP) است. درگاه اختصاص داده شده به این پروتکل 25 است اما ممکن است شرکت ارائهدهنده خدمات اینترنت یا سازمان پورت 25 را مسدود کرده باشد تا نتوانید یک میلسرور روی کامپیوتر محلی خود داشته باشید، با این حال، راهکار فوق مانع از آن نمیشود تا سرور پست الکترونیکی خود را روی درگاه محلی دیگری اجرا نکنید . دلیل اصلی این موضوع که برخی از سرویسها یک پورتهای خاصی گوش میدهند ایت است که یک کلاینت به سادگی بتواند سرویسی که روی یک میزبان راه دور در حال اجرا است را پیدا کند . به عنوان مثال، سرورهای FTP در پورت 21 فعال هستند، و سرورهای پروتکل انتقال ابرمتن (Hypertext (HTTP) روی پورت 80 فعال هستند. برنامههای کاربردی کلاینتی همچون برنامه یا مرورگر پروتکل انتقال فایل (FTP) بهطور تصادفی از پورتهای اختصاص داده شدهای بزرگتر از 1023 استفاده میکنند . تقریباً 65، 000 هزار پورت وجود دارد که تقسیمبندی آنها به شرح زیر است :

0-1023 : [illegible]

1024-49151: [illegible]

49152-65535: [illegible]

[illegible]

Port	Service	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67/68	DHCP	UDP
69	TFTP	UDP
79	Finger	TCP
80	HTTP	TCP
88	Kerberos	UDP
110	POP3	TCP
111	SUNRPC	TCP/UDP
135	MS RPC	TCP/UDP
139	NB Session	TCP/UDP
161	SNMP	UDP
162	SNMP Trap	UDP
389	LDAP	TCP
443	SSL	TCP
445	SMB over IP	TCP/UDP
514	Syslog	UDP
1433	MS-SQL	TCP

[illegible] Telnet [illegible] SSH [illegible] Secure Shell [illegible]

این چنین نیستند . فهرست زیر کارکردها و مشکلات امنیتی برخی از برنامههای رایج را نشان میدهد :

پروتکل انتقال فایل : FTP پروتکل FTP یک سرویس TCP است و از پورتهای 20 و 21 استفاده میکند . این سرویس برای انتقال فایلها از یک کامپیوتر به کامپیوتر دیگر استفاده شده و از پورت 20 برای انتقال جریان دادهها میان کامپیوتر کلاینت و سرور استفاده میکند . پورت 21 به منظور کنترل جریان و به منظور ارسال فرامین میان کلاینت و سرور FTP استفاده میشود . حمله به سرویس FTP عمدتا به منظور شنود گذرواژههایی که به شکل متن ساده ارسال شدهاند، دسترسی به مجوزهای پوشهای که پیکربندی اشتباهی دارند انجام میشود . FTP یکی از رایجترین سرویسهایی است که هکرها به آن حمله میکنند، به همین دلیل امروزه کمتر از سرویس FTP استفاده میشود .

پروتکل پیکربندی پویای میزبان (DHCP): از DHCP برای اختصاص آدرس آیپی به دستگاههای متصل به یک شبکه استفاده میشود . سرویس فوق از پورت 67 و پورت 68 برای انجام اینکار استفاده میکند . DHCPv4 بر مبنای چهار مرحله کشف، ارائه، درخواست و تأیید فرآیند (DORA) تخصیص آدرس را انجام میدهد.

■: Telnet تلنت یک سرویس TCP است که روی درگاه 23 کار میکند . تلنت به یک کلاینت اجازه میدهد نشستی را با میزبانی که در مکان دیگری قرار دارد برقرار کند . تلنت اطلاعاتی که توسط برنامه کلاینت تایپ شدهاند را برای کامپیوتر میزبان ارسال میکند . اگرچه تلنت میتواند پیکربندی شود تا اتصالات ناشناس را فراهم کند، اما باید به گونهای پیکربندی شود که به نامهای کاربری و گذرواژه نیاز داشته باشد. متأسفانه، حتا پس از انجام اینکار نیز تلنت این اطلاعات را در قالب یک متن عادی ارسال میکند . برنامه های کاربردی مانند SSH باید به عنوان جایگزینی برای تلنت استفاده شوند . SSH جایگزینی مطمئن برای تلنت است، زیرا نام کاربری و گذرواژهها را به شکل متن ساده ارسال نمیکند .

پروتکل انتقال ساده ایمیل **(SMTP)**: یکی دیگر از سرویسهای TCP است که روی پورت 25 کار میکند . سروی فوق برای تبادل ایمیل بین سیستمهای شبکه طراحی شده است. پیامهای ارسال شده از طریق SMTP از دو بخش سرآیند آدرس و متن پیام تشکیل شدهاند. همه کامپیوترها میتوانند با استفاده از SMTP به تبادل پیام بپردازند . جعل و هرزنامه دو آسیبپذیری مرتبط با SMTP هستند.

سامانه نام دامنه (DNS): این سرویس از پورت 53 برای انجام فعالیتهای خود و ترجمه آدرسها استفاده میکند . درست است که گاهی اوقت به درستی نقش DNS را درک نمیکنیم، با اینحال وظیفه سرویس فوق این است که نامهای دامنه کاملاً واجد شرایط (FQDN) را به یک آدرس IP عددی یا آدرسهای IP به FQDN تبدیل میکند . اگر هکری موفق شود عملکرد DNS را مختل کند، اینترنت همچنان به فعالیت خود ادامه میدهد، اما در این حالت کاربران باید آدرس IP هر سایتی که تمایل به بازدید از آنها را دارند حفظ کرده باشند . به همین دلیل عدم وجود DNS در بیشتر موارد باعث غیر قابل استفاده شدن اینترنت میشود .

بانک اطلاعاتی DNS از یک یا چند فایل منطقهای تشکیل شده است. هر منطقه مجموعهای از رکوردهای منابع ساختیافته است . از رکوردهای رایج درون سامانه نام دامنه میتوان به رکورد شروع اعتبار (SOA) سرنام Start Of Authority، رکورد A در پروتکل IPv4 ، □□□□□AAAA در پروتکل IPv6، رکورد CNAME ، رکورد NS، رکورد PTR و رکورد MX اشاره کرد . لازم به توضیح است در هر فایل پایگاه داده منطقهای تنها یک رکورد SOA وجود دارد . رکورد فوق فضای نام منطقهای را توصیف میکند. آخرین ورودی در رکورد SOA مقدار timeout را نشان میدهد . مقدار timeout به هکرها نشان میدهد حمله مسمومسازی DNS چه مدت پایدار بوده است . رکورد A رایجترین رکورد درون سامانه نام دامنه است . رکورد فوق شامل آدرسهای IP و نام میزبان خاص است. رکورد CNAME یک نام مستعار است. رکورد NS آدرس آیپی سایر سرورهای نام را فهرست میکند. یک رکورد MX به رکورد تبادل ایمیل اشاره دارد . این رکورد به آدرس آیپی سرور اشاره دارد، جایی که ایمیل باید به آن ارسال شود . هکرها میتوانند سرورهای DNS را با انواع مختلف از حملات هدف قرار دهند. یکی از این حملهها مسمومسازی کش DNS است. این نوع حمله، ورودیهای جعلی را به یک سرور DNS ارسال میکند تا اطلاعات ذخیره شده در آن را خراب کند . از دیگر حملات پیرامون DNS میتوان به حمله DoS و انتقال به منطقه غیرمجاز اشاره کرد . DNS از پروتکل UDP برای محاورههای DNS و از TCP برای انتقال منطقهای استفاده میکند . به دلیل آسیبپذیریهای موجود در DNS، کارگروه مهندسی اینترنت (IETF) نسخه پیشرفتهای از این سرویس بهنام ضمیمههای امنیتی سامانه نام دامنه (DNSSEC) سرنام Domain Name System Security Extensions را توسعه داد . DNSSEC برای احراز هویت مبدأ دادههای DNS طراحی شده است. Nslookup یکی از ابزارهای رایج خط فرمان است که برای اجرای محاورهها روی سامانه نام دامن و بهدست آوردن نام نام دامنه یا ترسیم آدرس IP از آن استفاده میشود .

در کامپیوترهای لینوکسی میتوان از دستور میزبان برای جستوجوی سوابق DNS استفاده کرد . ترکیب نحوی دستور فوق به شرح زیر است:

```
host [-c class] [-N ndots] [-R number] [-t type] [-W wait] [-m flag] [-4] [-6] {name} [server]
```

نکته : آزمون CEH انتظار دارد درباره دو سرویس مهم DNS بهنامهای name resolvers به سادگی به درخواستها پاسخ میدهد و authoritative servers که رکوردهای DNS را برای یک فضای نام نگهداری میکند اطلاعات کافی داشته باشید . همچنین لازم است درباره رکوردهای عمومی NDS همچون رکوردهای A که مرتبط با آدرسهای IPV4 هستند و رکوردهای AAAA که مرتبط با آدرسهای IPv6 هستند اطلاعات کافی داشته باشید .

پروتکل **TFTP**: پروتکل TFTP سرنام Trivial File Transfer Protocol روی پورت 69 کار میکند . پروتکل فوق را باید نسخه سادهتر و البته چالشیرتر FTP توصیف کنیم، زیرا از UDP برای کاهش سربارهها استفاده میکند . پروتکل فوق نه تنها بدون مدیریت یک نشست که TCP بر مبنای آن کار میکند استفاده میکند، بلکه نیازی به احراز هویت ندارد که میتواند چالش امنیتی بزرگی را به وجود آورد . پروتکل فوق عمدتا توسط تولیدکنندگان روتر برای ارسال فایلهای پیکربندی روتر استفاده میشود .

پروتکل **HTTP**: پروتکل انتقال ابرمتن Hypertext Transfer Protocol یک سرویس TCP است که از پورت 80 استفاده میکند . HTTP یکی از شناختهشدهترین پروتکلهای حال حاضر است که توسط بیشتر برنامهها و برخی از سایتها استفاده میشود . مدل اتصال HTTP به عنوان یک اتصال فارغ -از -حالت است. HTTP از رویکرد درخواست و پاسخ استفاده میکند که در آن کلاینت درخواستی را ارسال میکند و سروری به درخواست پاسخ میدهد. حملاتی که سعی میکنند از پروتکل HTTP سوء استفاده کنند، این توانایی را دارند تا سرور، مرورگر یا اسکریپتهایی که روی مرورگر اجرا میشوند را هدف قرار دهند . Code Red یکی از معروفترین حملاتی بود که وبسرورها را هدف قرار میداد .

پروتکل **SNMP** : پروتکل SNMP سرنام Simple Network Management Protocol یک سرویس مبتنی بر UDP است و از درگاههای 161 و 162 استفاده میکند . کارشناسان پیشبینی میکردند که پروتکل فوق روشی کارآمد و ارزان برای نظارت بر شبکهها باشد . SNMP به سرپرستان شبکه اجازه میدهد تا اطلاعاتی همچون آماری در ارتباط با وضعیت شبکه جمعآوری میکنند و گزارش را برای ایستگاههای مدیریتی ارسال کنند . بیشتر شرکتهای بزرگ به نوعی پروتکل SNMP را برای مدیریت شبکهها پیادهسازی میکنند . برخی از مشکلات امنیتی SNMP ناشی از این واقعیت است که اطلاعات را به شکل متن واضح ارسال میکنند . SNMP نسخه 3 نگارش جدیدتر پروتکل فوق است که امنیت بیشتری را از طریق رمزنگاری اطلاعات ارائه میکند .

نکته : آزمون **CEH** انتظار دارد درباره پروتکلهای فوق و ضعفهای موجود در این پروتکلها اطلاعات لازم را داشته باشید .

در شماره آینده مبحث فوق را ادامه میدهیم .

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره **CEH**

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
11:20 - 03/12/1398
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - آسیبپذیری سرریز بافر - - هک اخلاقی - مدل OSI - پروتکل TCP / IP

□□□□□
https://www.shabakeh-mag.com/security/16595/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-c:□□□□
eh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-
%D8%B3%D9%81%DB%8C%D8%AF-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-
%D8%A8%D8%A7-%D8%A2%D9%86%D8%A7%D8%AA%D9%88%D9%85%DB%8C-
%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-tcp-ip-%D9%88-
%D8%B6%D8%B9%D9%81%E2%80%8C%D9%87%D8%A7%DB%8C-
%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A2%D9%86