禪

آموزش رایگان دوره CEH همگام با سرفصلهای بینالمللی – 19

آموزش CEH (هکر کلاه سفید): سرشماری و هک کردن سامانهها

C|EH™
CERTIFIED ETHICAL HACKER

سرشماری (Enumeration) فرآیند شمارش یا فهرست کردن خدمات، برنامهها و پروتکلها ی موجود در ارتباط با هر یک از کامپیوترهای شناسایی شده است، در حالی که هک سیستم به فرآیند دستیابی، کسب امتیازات، حفظ کنترل و پنهانسازی ردپاها اشاره دارد.

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

اکنون میدانیم که هکرها برای حمله به یک هدف بر مبنای یک برنامه هفت مرحلهای گام بر میدارند که شامل جمعآوری اطلاعات، تعیین محدوده شبکه، شناسایی دستگاههای فعال، یافتن پورتهای باز و نقاط دسترسی، جزییات سیستمعامل، سرویسهای مرتبط با سیستمعامل و نقشهبرداری از شبکه سازمانی است. هرچه اطلاعات بیشتری در ارتباط با هدف جمعآوری شود، شانس موفقیت بیشتر است. ممکن است در این مرحله اطلاعات کافی پیدا کنید که در پیادهسازی حمله موفقیتآمیز باشند. اگر اینگونه نیست، اطلاعات جمعآوری شده را باید به نقطه شروعی برای مراحل بعدی حمله نگهداری کنید. یکی از مباحث مهمی که هکرهای اخلاقمدار باید به آن دقت کنند جمعآوری اسناد و مدارک است. به همین دلیل چند روش برای جمعآوری و مستندسازی اطلاعات معرفی کردیم تا مشکلی از این بابت نداشته باشید. این یادداشتها هنگام تهیه گزارش خود مفید هستند. سرانجام، اطمینان حاصل کنید که سازمان قبل از شروع کار، حتا به منظور شناسایی به شکل کتبی به شما اجازه انجام چنین کاری را داده باشد. تا این بخش از آموزش لازم است درباره کلیدواژههایی که به آنها اشاره کردیم، اطلاعات کافی به دست آورده باشید. برای اطمینان خاطر یکبار دیگر به این کلیدواژهها اشاره میکنیم. توجه داشته باشید که برای تسلط بر این کلیدواژهها باید سطح دانش خود را افزایش دهید.

active fingerprinting، CNAMEs، covert channel، demilitarized zone (DMZ)، denial of service (DoS)، echo reply، echo request، EDGAR database، initial sequence number (ISN)، Internet Assigned Numbers Authority (IANA)، intrusion detection system (IDS)، Nslookup، open source، passive fingerprinting، ping sweep، port knocking، scope creep، script kiddie، Simple Network Management Protocol (SNMP)، social engineering، synchronize sequence number، Time To Live (TTL)، traceroute، war dialing، war driving، Whois، written authorization، and zone transfer

[illegible]

[illegible]

[illegible]

[illegible] 1، [illegible] 72.3.246.59 [illegible] Redirff.com، Redirff.com، Rutgers.edu [illegible]

Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Redriff.com				
Examcram.com				
	72.3.246.59			
Rutgers.edu				

[illegible] 2، [illegible]

[illegible] https://www.whois.net [illegible] 3، [illegible]:

- http:/www.betterwhois.com
- www.allwhois.com
- http://geektools.com
- www.all-nettools.com
- www.dnsstuff.com

[illegible] traceroute [illegible] r- [illegible] 4، [illegible]

[illegible] IANA ، ARIN، RIPE [illegible] 5، [illegible]

[illegible] 6، [illegible]

[illegible]

[illegible]

1) [illegible] Nmap [illegible] https://nmap.org/download.html [illegible]. [illegible] [illegible] 7.30 [illegible].

2) [illegible] Nmap [illegible].

3) [illegible] nmap -h [illegible].

4) [illegible] nmap [illegible].

5) [illegible] UDP [illegible].

6) [illegible] stealth [illegible].

7) [illegible] fingerprint [illegible].

8) [illegible] nmap -sT IP-Address [illegible] IP-Address [illegible].

9) [illegible] stealth [illegible] Nmap - [illegible]. [illegible] sS IP-Address [illegible] IP-Address [illegible].

10) [illegible] UDP [illegible] nmap -sU IP_address [illegible].

11) [illegible] fingerprint [illegible] namp -O IP- [illegible] Address [illegible].

12) [illegible] Nmap [illegible].

[illegible]

■ [illegible] (Enumeration): [illegible].

■ [illegible]: [illegible].

[illegible] CEH [illegible] (OS) [illegible] (Enumeration) [illegible].

انتها نیز به سراغ هک سیستم میرویم که شامل بحث در مورد ابزارها و تکنیکهای مورد استفاده برای دستیابی به سیستمهای کامپیوتری است.

سرشماری

سرشماری را میتوان تحلیل عمیق کامپیوترهای هدف توصیف کرد . سرشماری با اتصال فعال به سامانههایی شناسایی شده مرتبط با حسابهای کاربری، حسابهای سیستمی، خدمات و سایر جزئیات سیستمی انجام میشود . سرشماری فرآیندی است که به شکل فعال محاورههایی را ترتیب داده یا به یک سامانه هدف به منظور جمعآوری اطلاعات از طریق UNIX / Linux ، SNMP ، NetBIOS / LDAP، سرورهای NTP، سرورهای SMTP و DNS انجام میشود .

شماری ویندوز

هدف از شمارش تجهیزات ویندوزی، شناسایی یک حساب کاربری یا یک سیستم برای استفاده احتمالی است. در این مرحله هکر ممکن است به فکر پیدا کردن یک حساب مدیر سیستم باشد، زیرا بالاترین سطح دسترسی را در اختیارش قرار میدهد . در این مرحله، ما و همچنین هکرها فقط به دنبال اطلاعاتی هستیم که اجازه دسترسی به سامانهها و زیرساختها را امکانپذیر کنند . برای هدف قرار دادن بهتر کامپیوترهای ویندوزی باید نحوه عملکرد این سامانهها را درک کنید . ویندوز در هر دو نسخه کلاینت و سرور ارسال میشود. سیستمهای کلاینت که امروزه از سوی کاربران استفاده میشوند به ترتیب ویندوز 10 ، 8 و 7 هستند. در سمت سرور، ویندوزهای 2012 ، 2016 و 2019 توسط مایکروسافت پشتیبانی میشود. هرکدام از این سیستمعاملها هستههای تقریبا مشابهی دارند . سیستمعاملها چگونه میدانند به چه فرد و دستگاهی اعتماد کنند؟ پاسخ در حلقههای محافظتی پیادهسازی شده پیرامون سیستمعامل قرار دارد . این حلقهها اجازه میدهند تا کدها به شکل سلسله مراتب و با محدودیتهای دسترسی اجرا شوند . رویکرد فوق به میزان قابل توجهی نحوه دسترسی به سطوح مختلف سیستمعامل را کنترل میکند. هرچه به سمت مرزهای بیرونی این مدل محافظتی حرکت کنید، سطح اعتماد کاهش پیدا میکند، اما در مقابل کاربر قادر است به مولفههای سیستمعامل دسترسی پیدا کند. شکل زیر مدل پایهای را که ویندوز برای حلقههای محافظتی به کار میگیرد نشان میدهد.

■ Security identifiers (SID)

■ Relative identifiers (RID)

S-1-5-21-1607980848-492894223-1202660629-500

S for security id

1 Revision level

5 Identifier Authority (48 bit) 5 = logon id

21 Sub-authority (21 = nt non unique)

1607980848 SA

492894223 SA domain id

1202660629 SA

500 User id

User ID	Code
Admin	500
Guest	501
Kerberos	502
First user	1000
Second user	1001

Security Account Manager Active Directory SAM Windows / System32 / config SAM HKLM \ SAM LDAP AD NT SAM AD

بیشتری با جستوجوی RFC 2251 دریافت کنید . یکی دیگر از سازوکارهای مهم امنیتی ویندوز خدمات سرور محلی امنیت (LSASS) است. LSASS یک فرآیند حالت کاربر است که مسئول خطمشیهای امنیت سیستم محلی بوده و شامل کنترل دسترسی، مدیریت خطمشیهای گذرواژهها است.

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 :
13:40 - 18/02/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - هک اخلاقی - حمیدرضا تائبی - ابزار Nmap - ابزار SuperScan

---

نشانی
:https://www.shabakeh-mag.com/security/16806/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%B3%D8%B1%D8%B4%D9%85%D8%A7%D8%B1%DB%8C-%D9%88-%D9%87%DA%A9-%DA%A9%D8%B1%D8%AF%D9%86-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7