16 – [illegible] CEH [illegible]

[illegible] CEH [illegible] :(Idle Scan) [illegible]

[illegible] CEH [illegible] (Idle) [illegible].

CEH [illegible].

TCP [illegible] Nmap [illegible] (IDS) [illegible].

TCP Full Connect scan: [illegible] SYN / ACK [illegible] RST / ACK [illegible].

TCP SYN scan: [illegible] TCP [illegible]

TCP FIN scan: In this type of scan, the attacker sends a FIN packet to the target port. If the port is closed, the victim will send a RST packet. If the port is open, the FIN packet will be ignored and the port will enter the open state. This type of scan is also called a stealth scan because it is difficult to log. However, many intrusion detection systems (IDS) can detect it. Another way to identify this scan is to look for packets without any flags enabled. Not all systems follow RFC 793 exactly.

TCP NULL scan: In this type of scan, all header flags are closed (0). If a RST packet is received, the port is closed. If no response is received, the port is open or filtered. The advantage of this scan is that it can sometimes pass through non-stateful firewalls and routers. This scan will not work on systems that comply with RFC 793 because the standard requires that all packets sent to open ports without SYN, RST, or ACK bits set should be discarded and a RST packet returned.

TCP ACK scan: This type of scan is used to map firewall rulesets. It can help determine whether a firewall is stateful or just a packet filter that blocks incoming SYN packets. This scan sends an ACK packet with random sequence and acknowledgment numbers to a port. If there is no response or if an ICMP unreachable error is received, the port is classified as filtered. If a RST is returned, the port is classified as unfiltered. This scan only determines if the port is filtered and cannot be used to find open ports.

TCP XMAS scan: This scan sets the PSH, FIN, and URG flags, lighting up the packet like a Christmas tree. According to RFC 793, a RST packet should be returned for closed ports. No response usually means the port is open. Microsoft implemented its own TCP/IP stack and ignored RFC 793 entirely, so this scan will not work against any Microsoft product. This scan type can sometimes bypass non-stateful firewalls and packet filters.

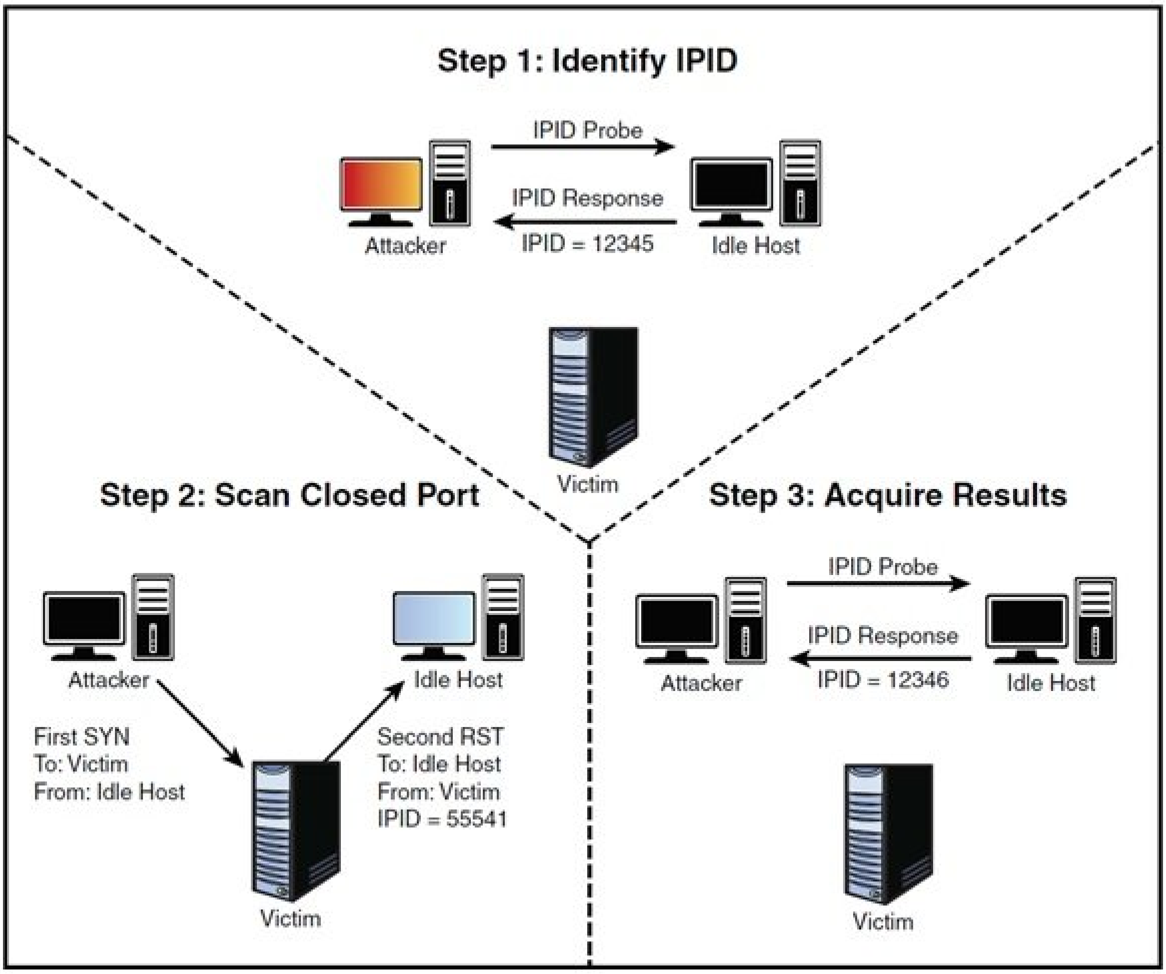
Nmap: Nmap is a free open source utility for network exploration and security auditing. It was designed to rapidly scan large networks, and works against single hosts as well. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap is extremely powerful, flexible, and portable. Nmap supports most operating systems, and both console and graphical versions are available. Nmap is free software, available with full source code under the GNU General Public License as published by the Free Software Foundation.

Idle Scan: This is a sophisticated port scanning technique that takes advantage of the IPID header field in TCP/IP RFCs. It is a blind port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines. The Idle scan is a TCP port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines. The Idle scan is a TCP port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines.

TCP Connect / Full Open: This is the most basic form of TCP scanning. The connect() system call provided by the operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port is not reachable. One strength of this technique is that the user does not need any special privileges. Any user on most UNIX boxes is free to use these calls. Another strength is that this is the fastest scan mechanism available. A full connect to every port of a target machine (65K ports) will take a few minutes at most. Slower machines or networks will take proportionally longer. The big downside to this technique is that it is very easy to detect and filter. The target machine will log the connection and the service will likely log a connection error and record the IP address of the attacker. Most UNIX systems will also add a note to syslog. Stealth scan: This is a sophisticated port scanning technique that takes advantage of the IPID header field in TCP/IP RFCs. It is a blind port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines. The Idle scan is a TCP port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines. The Idle scan is a TCP port scanning technique that allows the attacker to send packets to a target machine using the IP address of a third party machine. This technique can be used to determine which ports are open on the target machine and which services are running on those ports. It can also be used to determine the trust relationships between machines.

TCP Connect / Full Open: This is the most basic form of TCP scanning. The connect() system call provided by the operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port is not reachable. One strength of this technique is that the user does not need any special privileges. Any user on most UNIX boxes is free to use these calls. Another strength is that this is the fastest scan mechanism available. A full connect to every port of a target machine (65K ports) will take a few minutes at most. Slower machines or networks will take proportionally longer. The big downside to this technique is that it is very easy to detect and filter. The target machine will log the connection and the service will likely log a connection error and record the IP address of the attacker. Most UNIX systems will also add a note to syslog.

Step 1: Identify IPID
IPID Probe
IPID Response
IPID = 12345
Attacker
Idle Host
Victim
Step 2: Scan Open Port
Second SYN ACK
To: Idle Host
From: Victim
IPID = 55541
Attacker
Idle Host
First SYN
To: Victim
From: Idle Host
Third RST
To: Victim
From: Idle Host
IPID = 12346
Victim
Step 3: Acquire Results
IPID Probe
IPID Response
IPID = 12347
Attacker
Idle Host
Victim



درست است که روش فوق کامل نیست، اما راهکار فوق مهاجمان را قادر میسازد آدرس واقعی خود پنهان کنند . با این حال، محدودیتهایی در رابطه با پویش idle وجود دارد . اول آنکه، سیستمی که قرار است نقش میزان idle را باز کند باید به معنای واقعی کلمه بیکار باشد . واقعیت دیگری که وجود دارد این است که تمامی سیستمعاملها از رویکرد افزایش IPID استفاده نمیکنند . به عنوان مثال، برخی از نسخههای لینوکس IPID را روی صفر تنظیم میکنند یا مقدار IPID تصادفی تولید میشود. باز طبیعی است در چنین سامانههای عاملی پیادهسازی یک چنین حملاتی شانس موفقیت کمی دارند. در نهایت نباید فراموش کنید که نتایج به دست آمده باید ارزیابی شوند . منظورم این است که برای تأیید صحت نتایج لازم است آزمونهای چندگانهای انجام شوند تا هکر مطمئن شود که حملهخ به سرانجام میرسد . در حالی که مفهوم پویش Idle جالب است، اما روشهای پویش دیگری نیز وجود دارد که به شرح زیر هستند :

ACK scan: در روش فوق یک پروب ACK با شماره دنباله تصادفی ارسال میشود . پاسخهای ICMP نوع 3 کد 13 ممکن است بدان معنا باشند که شبکه هدف از دیوارهای آتش بدون حالت استفاده میکند و بسته RST میتواند از پورتی که فیلتر نشده عبور کرده باشد .

FTP Bounce scan: در روش فوق از سرور FTP استفاده شده و در وضعیت پسیو بستهها ارسال میشوند تا فرآیند ردیابی پویش به سختی امکانپذیر شود .

RPC scan: در این روش تلاش میشود تا این مسئله شمخص شود که آیا پورتهای باز از نوع RPC هستند یا خیر.

Window scan: شبیه به روش پویش ACK عمل میکند، اما گاهی اوقات میتواند درگاههای باز را مشخص کند . در روش مقدار TCP window size بازگردانده شده از بستههای RST بررسی میشود. در برخی از سیستمها، پورتهای باز یک مقدار window size مثبت را بر میگردانند و پورتهای بسته مقدار منفی را برای window size باز میگردانند .

حال بیایید نگاهی به اسکنهای UDP بیندازیم . UDP برخلاف TCP عمل میکند. TCP روی اتصالات محکم

[illegible]

[illegible]

Nmap [illegible]

[illegible]

C:\ nmap-6.25>nmap -h

Nmap 6.25 Usage: nmap [Scan Type(s)] [Options] <host or net list>

Some Common Scan Types ('*' options require root privileges)

* -sS TCP SYN stealth port scan (default if privileged (root))

-sT TCP connect() port scan (default for unprivileged users)

* -sU UDP port scan

-sP ping scan (Find any reachable machines)

-sL list scan that simply does a reverse DNS lookup without actually

scanning

* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)

-sV Version scan probes open ports determining service and app

names/versions

-sR/-I RPC/Identd scan (use with other scan types)

......

......

برای دانلود ابزار فوق می توانید به آدرس زیر مراجعه کنید .

https://nmap.org/book/man.html

همانگونه که در خروجی منوی راهنما در فهرست قبل مشاهده میکنید، Nmap میتواند انواع مختلفی از اسکنها را اجرا کند . Nmap یک ابزار ضروری است که هر کارشناس امنیتی باید نحوه کار با آنرا یاد گرفته باشد . Nmap Scripting Engine یکی از قدرتمندترین و انعطافپذیرترین ویژگیهای Nmap است. قابلیت این امکان را برای کاربران فراهم میکند تا اسکریپتهای سادهای را برای خودکارسازی طیف گستردهای از کارهای شبکه ایجاد و استفاده کنند . Nmap اطلاعاتی در ابتاط با نام سرویسهایی که پورت آنها باز است، پروتکلها و ..... را ارائه میکند . پورتها میتوانند باز، بسته یا فیلتر باشند . اگر پورت باز باشد به این معنا است که دستگاه هدف اتصالات را در آن پورت قبول میکند . یک درگاه بسته اتصالات را قبول نمیکند و یک پورت فیلتر شده به معنی آن است که یک دیوارآتش، فیلتر یا سایر دستگاههای شبکه از درگاه محافظت میکنند و مانع از آن میشوند تا جستوجوی کامل Nmap برای تعیین وضعیت به سرانجام برسد. اگر پورت به عنوان فیلتر نشده گزارش شده باشد به این معنا است که پورت بسته است و به نظر نمیرسد هیچ دیوارآتش یا روتری در تلاش باشند تا خللی در عملکرد Nmap وارد کنند .

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 :
20:20 - 23/01/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - هک اخلاقی - ابزار Nmap

---

نشانی
:□□□□https://www.shabakeh-mag.com/security/16693/%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%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D8%B1%D9%88%D8%B4%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AE%D8%AA%D9%84%D9%81-%D9%BE%D9%88%DB%8C%D8%B4-%D9%BE%D9%88%D8%B1%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A8%D8%A7%D8%B2%D8%8C-%D8%A8%D8%B3%D8%AA%D9%87-%D9%88-%D9%81%DB%8C%D9%84%D8%AA%D8%B1-%D8%B4%D8%AF%D9%87