黑客要攻下一台計算機，一般怎麼做?

黑客技術與網絡安全 今天

以下文章來源於小白學黑客，作者小白哥

小白學黑客

小白也能看懂的網絡安全教程

> **來自公眾號：小白學黑客**

郑重声明：本文仅供技术交流，切勿拿去做违法事情

很多剛剛入門安全的同學可能比較好奇：**黑客到底是如何攻破一個目標的呢?**

這個目標可能是一個網站，也可能是一台個人電腦，還可能是一部智能手機。

這篇文章就來跟大家簡單聊聊這個問題。

網絡攻擊其實是一種電子信息戰爭，看不見摸不著，卻實實在在發生了。

打一場戰爭之前最重要的就是情報收集，所謂知己知彼才能百戰百勝，沒有情報就是瞎搞。

網絡攻擊也一樣，第一步也是情報收集。

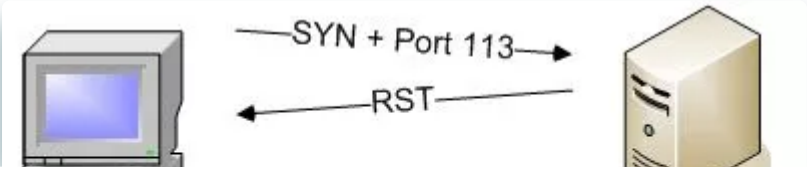
端口掃描

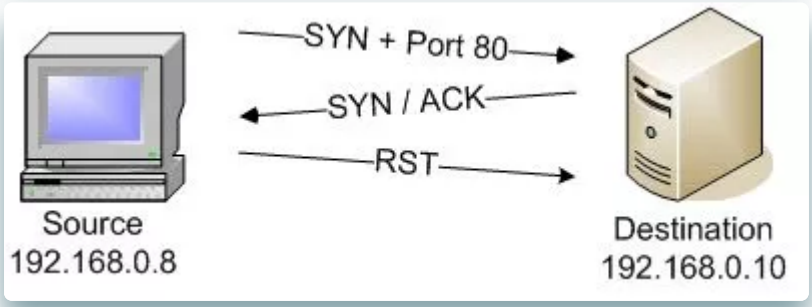
發起網絡攻擊之前，黑客通常會進行端口掃描，檢測目標上開啟了哪些服務。

端口，在計算機網絡協議中，是位於傳輸層的一個概念，當計算機上多個不同的進程都在通信的時候，用端口號來區分它們。

端口是一個16位的整數，總共是65535個端口。

端口掃描的原理，就是依次嘗試向服務器的六萬多個端口發送探測數據包，觀察目標的反應。以TCP為例，如果發送一個TCP的握手包過去，目標返回了第二次握手信息SYN+ACK，則說明在這個端口上，有一個TCP服務存在。





不過，現在的防火牆對於基本的端口掃描行為都能檢測到，如果發現同一個IP地址短時間內嘗試連接大量端口，則很快會被拉入黑名單，導致端口掃描行為無法再進行下去。

所以端口掃描還會更換IP，更換掃描頻率，變的更難識別。

程序識別

掃描到這些端口後有什麼用呢？是用來進行下一步：程序識別。

- 如果發現了80端口，背後可能是一個web服務器。
- 如果發現了53端口，背後可能是一個DNS服務器。
- 如果發現了3389端口，背後可能是一個開放了遠程桌面連接的Windows機器。
- 如果發現了3306端口，背後可能是一個MySQL服務器。
- 如果發現了6379端口，背後可能是一個Redis服務器。
- 如果發現了9200服務器，背後可能是一個ElasticSearch服務器。

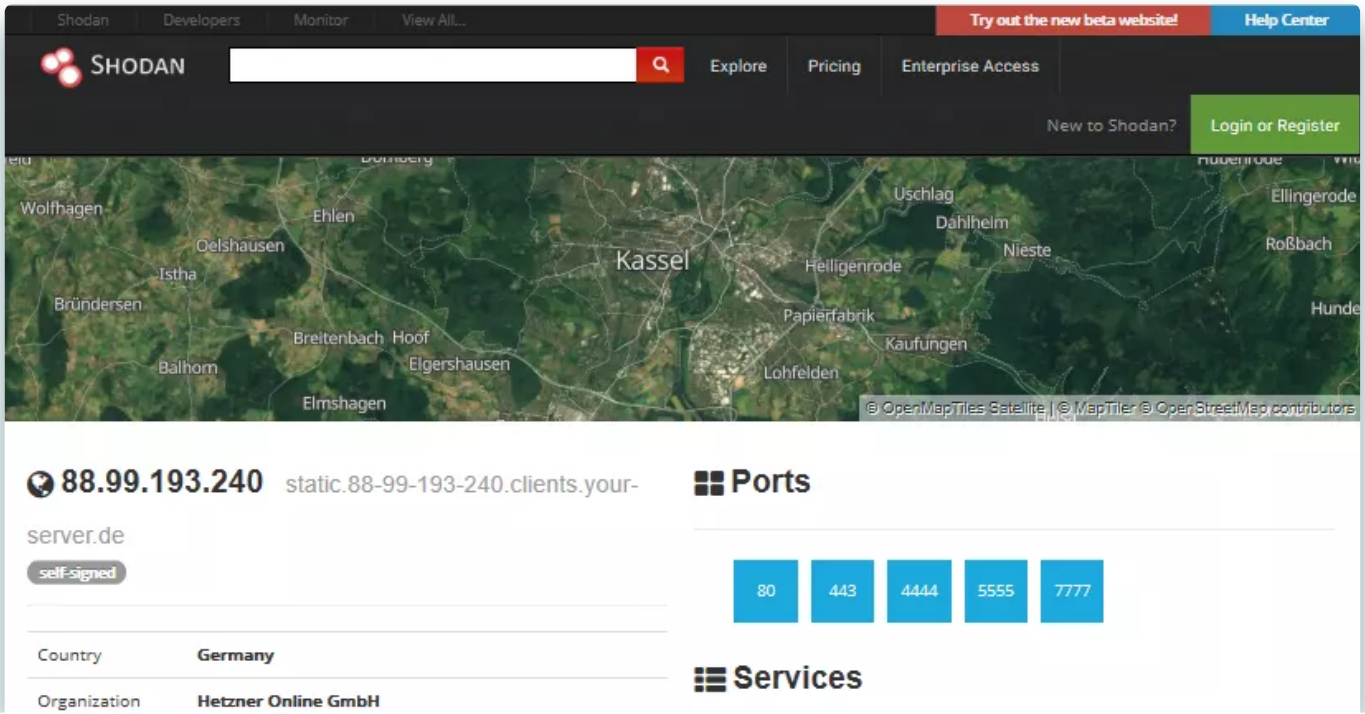
- ...

再進一步，還能識別程序的種類、版本等。

以80端口為例，通過繼續發送HTTP數據包，從服務器的響應中，根據Server字段，還能知道這個web服務器是一個nginx，還是一個Apache或者其他。

甚至通過有些服務，我們還能知道背後是一個Windows還是一個Linux還是一個Android，如果是Linux，內核版本信息也能知道。

端口掃描+程序識別的過程，這些操作已經非常成熟，甚至都不用再自己編程或用工具去探測了。直接用**Shodan**或者**ZoomEye**，輸入IP地址，就能幫我們列出這個IP背後的信息，省去了不少功夫。



漏洞攻擊

識別了程序，接下來關鍵的來了：漏洞攻擊。

像nginx、tomcat、redis、mysql等等這些著名的開源軟件，基本上每年都有不少的漏洞被曝光出來，而許多網站的運營管理人員安全意識並沒有那麼強，不會經常去打補丁升級，就會導致這些對外提供服務的機器上留存有不少的漏洞。

黑客通常都會有一個漏洞武器庫，每個軟件有哪些漏洞他們都清清楚楚，針對每個漏洞還開發了對應的攻擊武器。

此時，黑客可以針對發現的服務器，編寫一個漏洞利用程序，進行遠程攻擊，從而讓遠程服務器執行自己的代碼。

這其中最為人熟知的應該就是**web安全**了，因為web服務佔據了互聯網流量的比重實在太大，有太多的業務都是通過web來提供服務，這就導致黑客把目標聚焦在這一塊。

web服務器後端，一般是C++、Java、PHP、Python這些語言開發的程序，這些語言所攜帶的庫和框架都或多或少的存在這樣那樣的問題，通過向這些後端程序發送一系列精心構造的請求，就可能讓後端服務淪陷。

權限提升

當通過後端服務的漏洞成功入侵，攻擊者可以讓目標服務器執行自己的代碼。但通常來說，操作系統都有一些安全機制，常見的web、mysql、redis、nginx這些，它們也是在一些低權限的進程中運行，就算攻擊者攻破後端服務，也是在這些低權限的進程中執行代碼，很多事情都做不了。所以這個時候，攻擊者一般都需要做一件事：**權限提升**。

接著，他們再通過利用操作系統的一些漏洞，攻擊者可以讓自己的攻擊代碼逃脫低權限的進程，獲得高級權限，比如root權限執行。

開始工作

到這個時候，你的服務器就真的危險了！為了能夠經常登錄你的服務器，攻擊者還會留一些後門，還會添加一些新用戶，以便常回來看看。

如果是一個竊密軟件，它會偷偷把你的重要文件給傳輸出去。

如果是一個搞破壞的，它還會篡改數據，黑掉網站。

如果是一個勒索病毒，它還會加密你的文件。

如果是一個挖礦病毒，那你的CPU和GPU就要辛苦了。

還有些高級攻擊的木馬，並不會立刻對你的計算機做什麼破壞，而是潛伏起來，躲在某個角落等待被喚醒。

安全防禦

以上，就是黑客從信息蒐集到最後拿下服務器的全過程。清楚了敵人的路數，咱們才好對症下藥，做到下面幾件事，防患於未然：

- 防火牆記得開啟，並關閉不需要的端口
- web服務server字段不要洩露任何關於軟件的信息
- 軟件即時打補丁
- 重要數據定時備份
- 使用監控軟件監控服務器CPU、內存的變化，有異常及時告警

看完這篇文章，你有什麼收穫嗎，歡迎轉發分享哦~

--- EOF ---

那些要離職卻被加薪挽留的員工，後來都怎麼樣了?

安曉輝生涯

收藏| 2021某大型活動期間爆出漏洞自查清單

Timeline Sec