公司wifi安全

Black_Hole (/author/Black_Hole) · 2016/02/24 10:11

0x00 前言

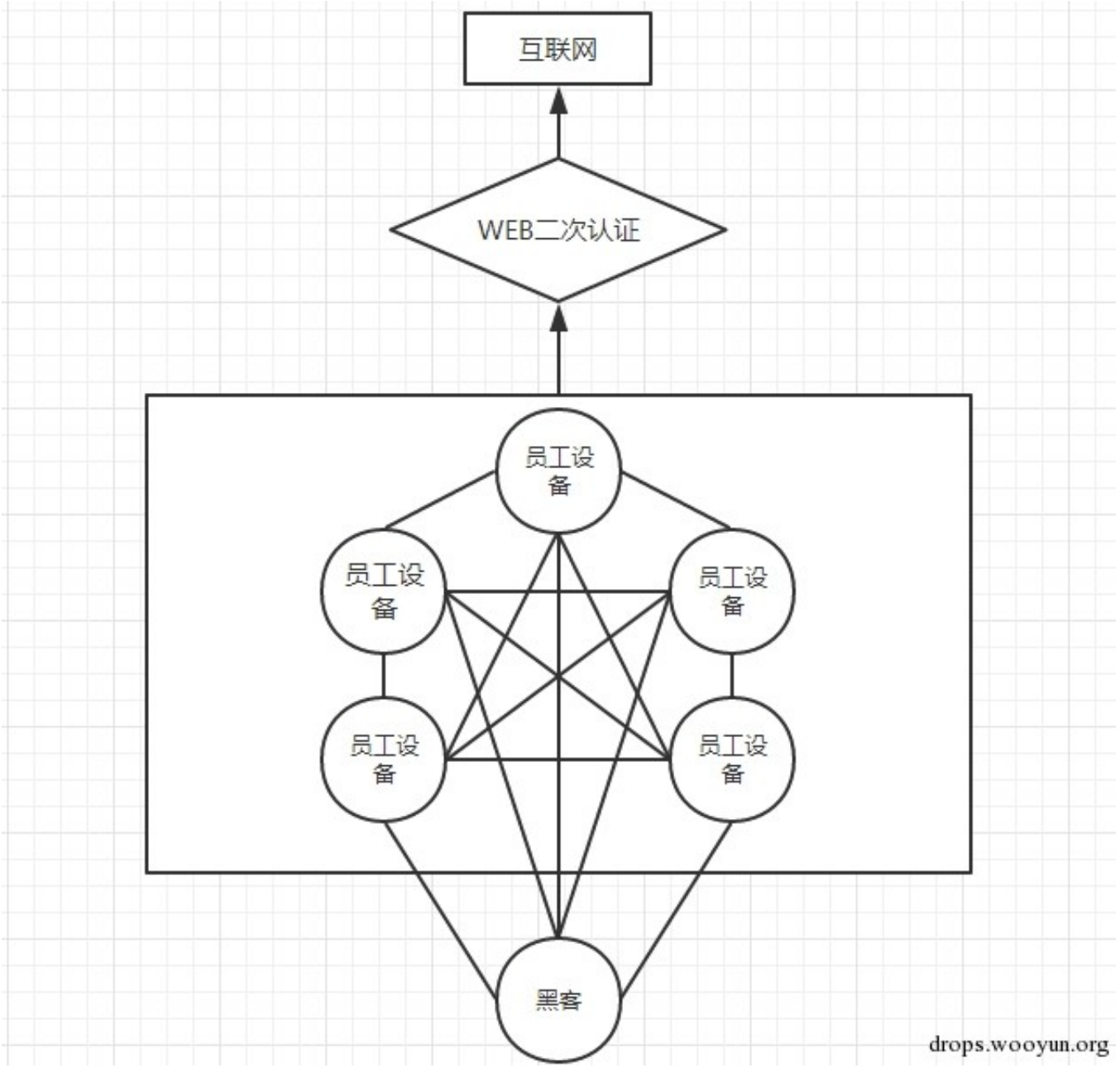
很多的公司都没有安全团队，只有运维来负责整个公司的安全，从而安全问题也大打折扣。我最近一直在给各个公司做安全检测，就把自己的心得写下来，有什么不足之处还望补充。

0x01 无线安全

很多的公司都有不怎么注重公司的无线电安全，有钱的公司买设备，没钱的公司搞人力。但是人的技术在好，没有设备的辅助，人力在牛逼也没有个卵用。一个好的路由器、交换机、IDS就像你装备了 无尽、狂徒、杀人书一样的屌。

很多的公司WIFI认证基本都是WPA/WPA2然后加个WEB二次认证，认为这样就万无一失了，而其实这并没有什么卵用，破解WPA/WPA2，这大家都知道，可以使用aircrack-ng、airmon-ng、airodump-ng、aireplay-ng来实现暴力破解，没有好的密码破解，可以把cap的包发给“549011522”七元一次（本人没破过，不保证绝对不上当）。而大家也都知道有一款神奇叫做“wifi万能钥匙”，可以先去看看wifi万能钥匙能不能解，不能解的话再破。连上WIFI后，将会提示你需要进行WEB二次认证。这里你完全可以弃之不理，因为它并没有什么卵用。WEB二次认证说难听了，屁用没有。因为你是WPA/WPA2的认证方式，你连上WIFI之后，交换机就会马上分配给你一个内网IP（我遇到的是交换机，也可能是路由器）一个黑客要你外网干什么，他需要的是公司的内网资源。连不上网对黑客来说没有什么问题。我给某公司做安全检测的时候，万能钥匙破解—中间人嗅探。不到一分钟拿到了他们公司官网后台管理员的权限。WEB认证在我看来不是针对于黑客的，是针对于员工的，因为黑客不需要外网资源，但是员工需要。

下面是我画的图：



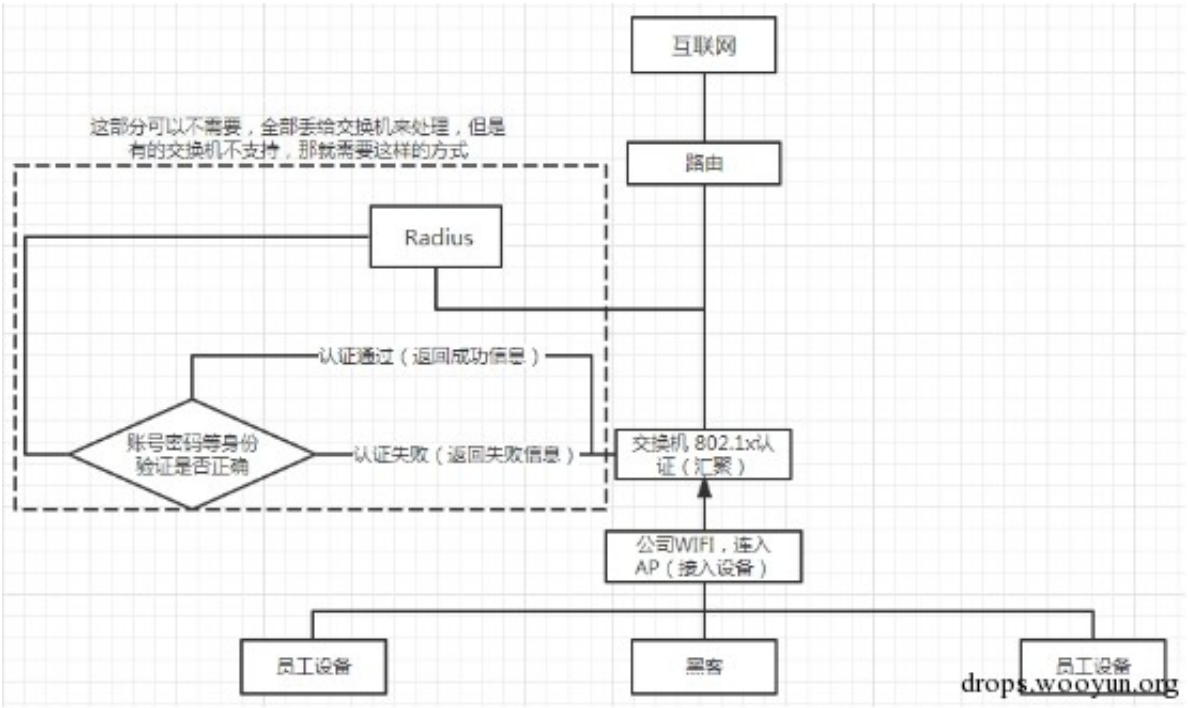
思维导图URL：https://www.processon.com/view/556d3cd0e4b09c41cc41b26e (https://www.processon.com/view/556d3cd0e4b09c41cc41b26e)

黑客连入WIFI后，虽然WEB二次认证不了，但是黑客现在已经处于内网中，他可以访问内网的任何资源。

修复建议：

1. 把WPA/WPA2无线认证换成802.1x认证方式（802.1x无线认证方式需要交换机的支持）
2. 买针对无线检测/防御设备
3. 无线不能访问内网资源，只有有线可以访问内网资源（从物理上隔绝问题）

关于802.1x认证方式，他的原理图是下面这样的:



思维导图URL：http://www.processon.com/view/link/556d5c6be4b09c41cc43c0e3 (http://www.processon.com/view/link/556d5c6be4b09c41cc43c0e3)

黑客即使连上公司WIFI，但是无法通过802.1x认证，导致 公司设备（路由器、交换机）无法分配给你内网IP和外网出口IP的资格。

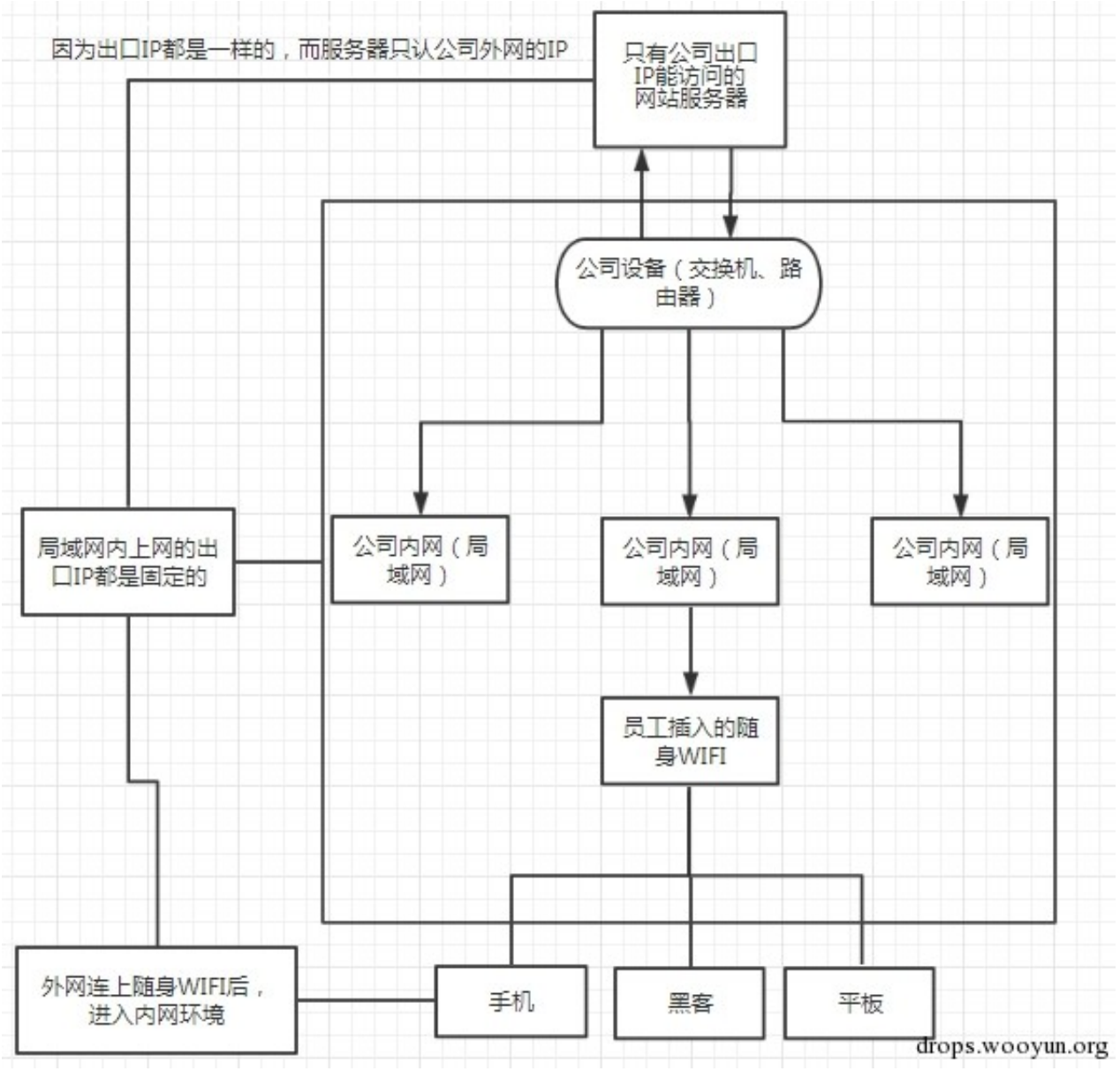
0x02 较为深入无线安全

像上面所讲，只是针对公司开放的WIFI进行管理。而上面的三个解决方案，只有第一个相比之下是比较方便还不用花钱的（机房设备需要支持802.1x无线协议，不支持还是要花钱）。

第二个，公司如果不想花钱是不会选择的，而且买了还要配置，前期工作量特别大。

第三个，工作量大，需要重新架构公司网络。

如果公司不想花钱或者运维不想重新架构的话，第一种是很好的选择，但是这里又有一个问题，360/百度随身WIFI，这个东西的存在，对那些本来就不怎么安全的公司更是雪上加霜。360/百度随身WIFI插入公司电脑后，会开启ICS服务，加上自带的无线网卡AP功能。当你连上这个随身WIFI之后，相当于一个小型的局域网。这时我们可以先入侵那个插了随身WIFI的PC电脑，通过它来入侵整个公司。如果你只需要某个接口，则不需要入侵插了随身WIFI的PC电脑。这里假设下“我需要的是这个网站的后台，可是想要登陆这个网站后台，需要出口IP是这个公司的外网IP”这样的话，我们则不需要入侵插了随身WIFI的PC电脑来。为什么呢？我画了一个图，大家看下。



思维导图URL：https://www.processon.com/view/556d175ee4b0546a904aa2bb (https://www.processon.com/view/556d175ee4b0546a904aa2bb)

黑客连入WIFI后，无需进行WEB二次认证，因为它使用的是员工的网络，员工也肯定认证过了，员工使用的是公司内网，内网有个统一的出口IP，而服务器端也只认这个IP，其他IP连不上服务器。

解决办法，网上很多，可以参考网上的教程。

如果你又更好的解决方案，可以提出来。我个人的思路有限。有不足之处，还望见谅。