3.2 ⅡS 安全

掌握 IIS 的安全点。

3.3 DNS 安全

掌握 DNS 的安全点

0x01 防 DDOS
冗余、负载均衡、防 D 设备

0x02 防欺骗和劫持等
DNS 组件本身的安全性

0x03DNS 服务器本身安全
服务器本身加强防护

3.4 DHCP 安全

0x01DHCP 服务欺骗
0x02ARP 中间人攻击
0x03MAC/IP 欺骗
0x04DHCP 报文泛洪攻击

3.5 AD 域安全

0x01 哈希值传递

这种攻击方法受到 NTLM 架构的限制，NTLM 是微软在 20 世纪 90 年代发布的一种身份验证协议。要登陆到远程主机，需要存储在计算机上的密码哈希值，用于身份验证过程。该哈希值可以从计算机上提取出来。

0x02 Mimikatz

为了实现这一目的，法国的研究者 Benjamin Delpy 在 2014 年开发了 Mimikatz，该实用程序允许从计算机内存中转储明文密码和 NTLM 哈希值。

0x03 暴力破解

如果无法实现从主机提取凭据，那么攻击者也可以选择粗暴但是有效的密码猜测技术。

0x04 net user/domain

在进行攻击之前，攻击者实际上需要一个用户名字典。当任何域成员执行 net user /domain 命令之后，该命令就会返回 AD 域用户的完整列表。

0x05 Kerberoasting 攻击

如果域使用了 Kerberos 作为身份验证协议，那么攻击者就可以尝试进行 Kerberoasting 攻击。在域上进行身份验证的任何用户，都可以请求 Kerberos Ticket，用于访问服务(票证授予服务 Ticket GrantingService)。TGS 使用运行服务用户的密

码哈希值进行加密。攻击者在请求 TGS 后，就可以对 TGS 进行离线的暴力破解，这一暴破过程不会受到任何阻止。如果成功，攻击者将获得运行服务账户的密码，而这一账户通常为特权账户。

0x06 PSEXEC

在攻击者获得所需凭据之后，下一步就是要远程命令执行。使用 Sysinternals 中的 PsExec 实用程序可以轻松实现，这个实用程序非常有效，受到广大 IT 管理员和广大黑客的青睐。

总结：

01.找到服务器或者组件本身的漏洞，根据漏洞本身进行攻击，通过各种漏洞攻击工具实现.最终目的是获得一个域内用户或者得域管理员用户的密码。

02.通过扫描、猜测、暴力破解、渗透提取、钓鱼等多种方式，取得一台服务器的控制权限，然后纵向和横向的不断渗透。