

最后的防线！高级域渗透攻击的分析与检测

@9ian1i

About us

- @9ian1i, 0KEE Team
 - Team Blog: <https://0kee.360.cn/blog/>
 - 擅长安全自动化设计和开发, 关注企业安全防御, 代码审计爱好者
 - DEFCON 27 @ Blue Team Village 演讲者
-
- 微博: @9ian1i
 - Github: @9ian1i



Contents

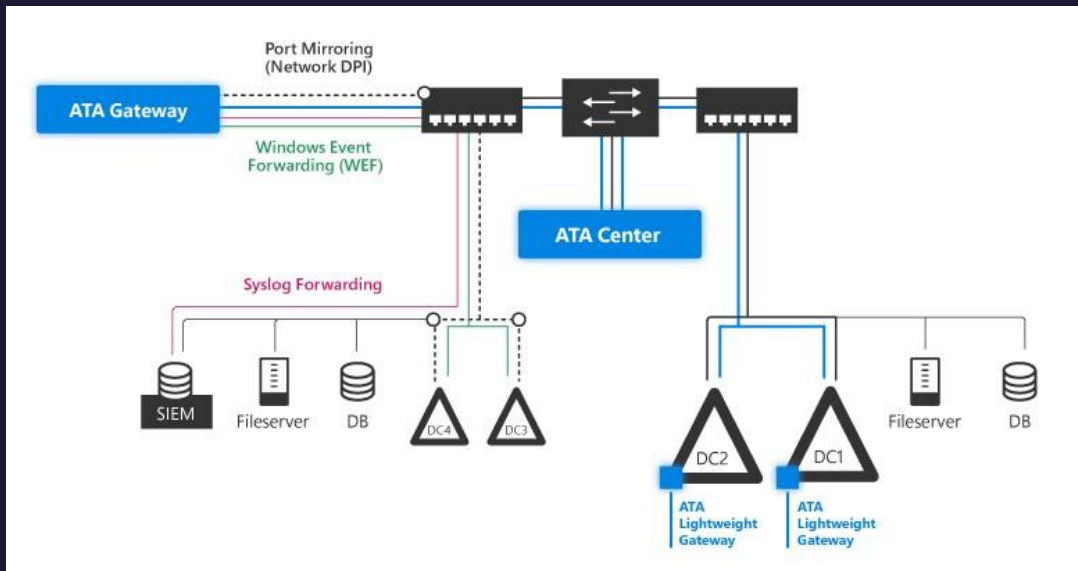


- Background on Subject
- Architecture
- Detections
 - Abnormal Kerberos Protocol
 - Sensitive Actions
 - Logon History
 - Honeypot Account
 - Detect Unknown Threat
- Achievements
- WatchAD
- Thanks

Background on Subject – AD Security



Background on Subject – Microsoft ATA



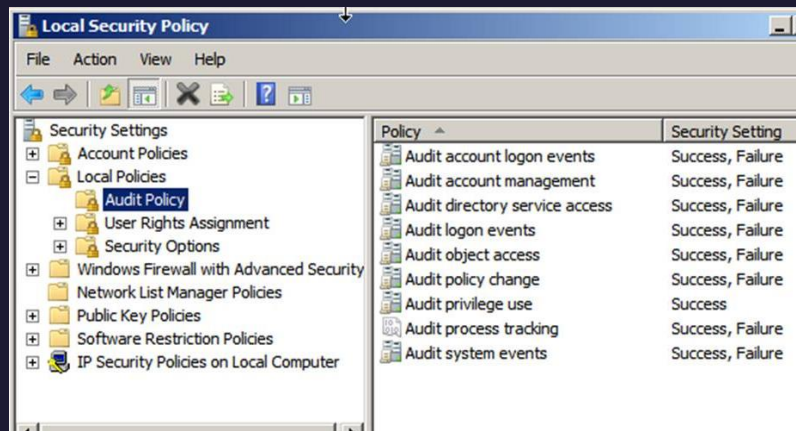
License Options		
	Per user	Per OSE/device
Through Enterprise CAL Suite per-user license	●	
Through Enterprise CAL Suite per-device license		●
Through Enterprise Mobility Suite user subscription license	●	
Through Enterprise Cloud Suite user subscription license	●	
Standalone license – Open L&SA estimated retail price, annualized*	USD \$80	USD \$61.5

* Pricing shown is an estimate only (L&SA = License + Software Assurance), and can vary by country. Please contact your Microsoft reseller or Microsoft representative for a quote.

收费昂贵，以流量为主进行分析，部分检测没有抓住核心原理，容易被针对绕过，且部署在域控上对性能有一定影响。

Background on Subject – event log

- 安全事件日志详细记录了域内所有用户的活动，在所有域控的本地安全策略中开启全部审核选项。
- 安全事件日志适合去分析域渗透攻击所产生的结果，比如敏感用户组变化、特权使用、域内敏感配置更改等。
- 优点是难以混淆绕过，可检测维度多。缺点是信息不够详细，部分攻击有时无法检测。



Background on Subject – event log

- 4624: 记录账户登录事件。
- 4768: 申请TGT时触发该日志。
- 4769: 申请ST时触发该日志。
- 5136: 目录服务对象被修改, 如ACL、账户对象等。
- 4728, 4732, 4756: 向安全组中添加用户。
- 4738: 用户账户被修改, 如添加资源约束委派权限。
- 4672: 特权登录, 管理员权限用户登录时和4624一起触发。
- 4625: 登录失败。

```

<System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-547
  <EventID>4624</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2019-10-25T03:10:26.81250000Z" />
  <EventRecordID>29602552</EventRecordID>
  <Correlation />
  <Execution ProcessID="520" ThreadID="1348" />
  <Channel>Security</Channel>
  <Computer>dc01.adtest.com</Computer>
  <Security />
</System>

<EventData>
  <Data Name="SubjectUserSid">S-1-0-0</Data>
  <Data Name="SubjectUserName"></Data>
  <Data Name="SubjectDomainName"></Data>
  <Data Name="SubjectLogonId">0x0</Data>
  <Data Name="TargetUserSid">S-1-5-21-2858140052-320346861-473137535-
  <Data Name="TargetUserName">CP02$</Data>
  <Data Name="TargetDomainName">ADTEST</Data>
  <Data Name="TargetLogonId">0xd2a67a</Data>
  <Data Name="LogonType">3</Data>
  <Data Name="LogonProcessName">Kerberos</Data>
  <Data Name="AuthenticationPackageName">Kerberos</Data>
  <Data Name="WorkstationName"></Data>
  <Data Name="LogonGuid">{977C63AA-2349-CE7F-F968-669AD8CD...E71}</Data>
  <Data Name="TransmittedServices"></Data>
  <Data Name="LmPackageName"></Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x0</Data>
  <Data Name="ProcessName"></Data>
  <Data Name="IpAddress">192.168.0.24</Data>
  <Data Name="IpPort">26862</Data>
  </EventData>
  
```

来源用户

目标用户

来源主机名

来源IP

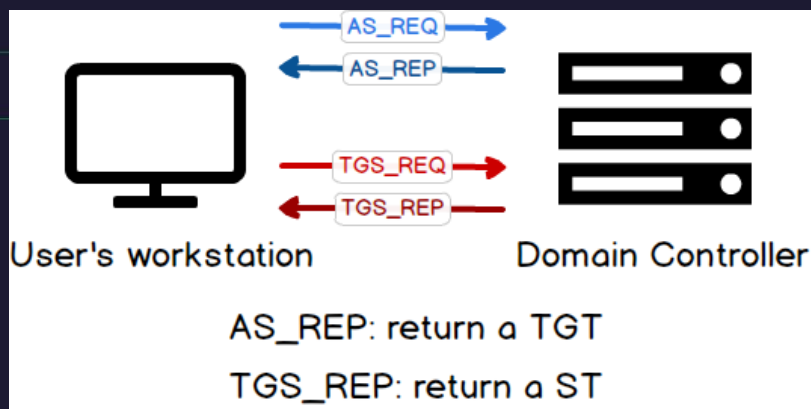
Background on Subject – Traffic of Kerberos

- Kerberos流量包含所有该协议相关的细节，在所有域控上部署流量采集终端收集88端口的流量。
- Kerberos流量适合去分析域渗透攻击的过程，比如利用协议缺陷的提权、伪造票据、匹配工具指纹等。
- 优点是可详细分析攻击特征，分析协议流程。缺点是可被针对绕过，只能用于Kerberos相关攻击检测，其余攻击方式需要额外处理。

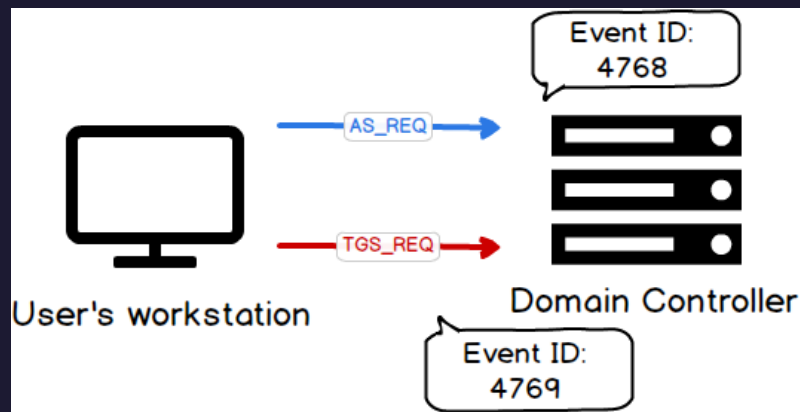
```
▼ Kerberos
  > Record Mark: 274 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▼ padata: 1 item
      > PA-DATA PA-PAC-REQUEST
    ▼ req-body
      Padding: 0
      > kdc-options: 40810010 (forwardable, renewable)
      > cname
        realm: ADTEST.COM
      > sname
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 1120592287
      > etype: 6 items
      > addresses: 1 item CP02<20>
```


Background on Subject – Kerberos Protocol

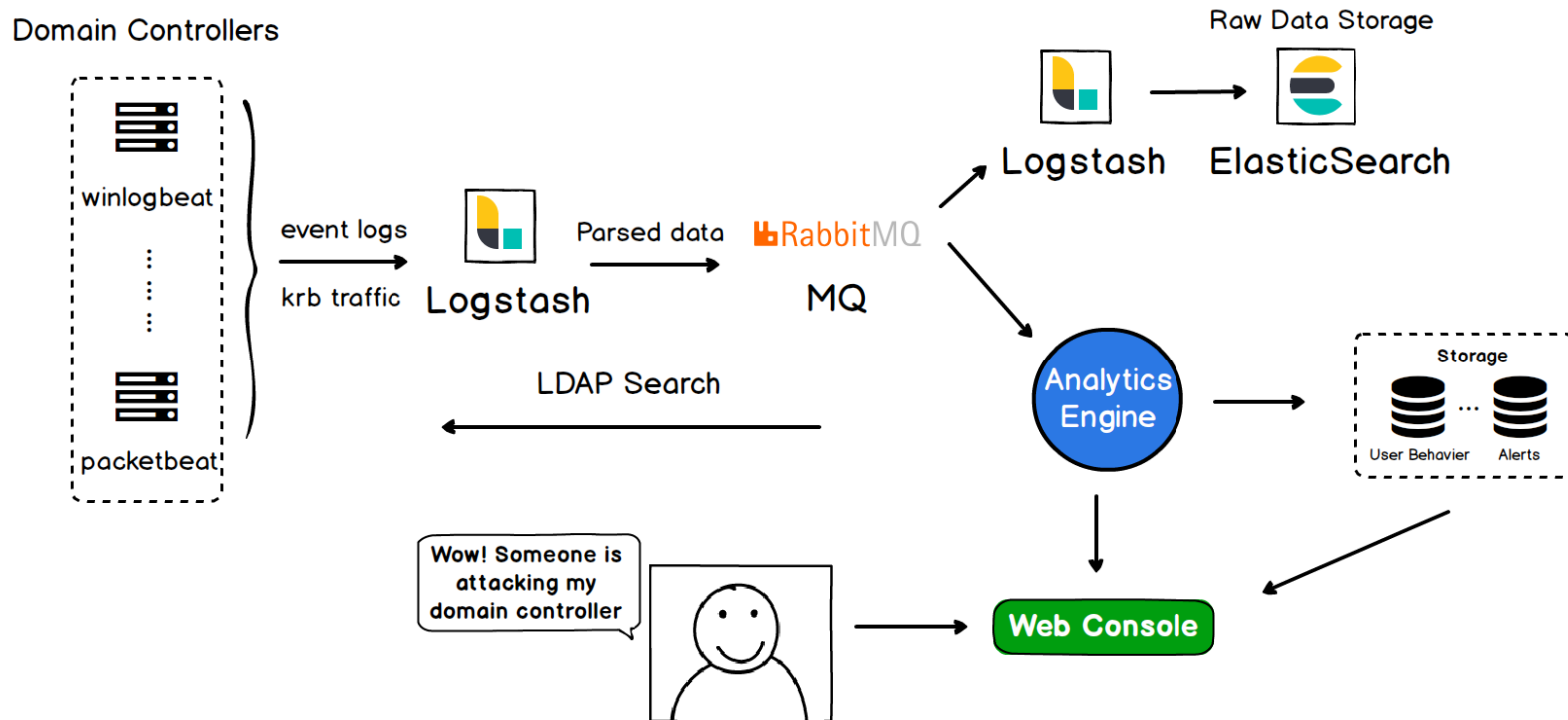
Kerberos协议简要流程



对应触发事件日志



Architecture



Detections



- Abnormal Kerberos Protocol
 - Kerberoast
 - Golden Ticket
 - Tools Fingerprint
- Sensitive Actions
 - Modification of ACL
 - Privileges Granted
 - Constrained Delegation Granted
- Logon History
 - NTLM Relay
- Honeypot Account
 - Honeypot Account Activity
- Unknown Threat Detection
 - Privilege Escalation

Abnormal Kerberos Protocol

Abnormal Kerberos Protocol — Kerberoasting

通过请求某些账户的弱加密(RC4-HMAC)服务票据，本地离线破解密码。

```
Add-Type -AssemblyName System.IdentityModel  
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList  
"MSSQLSvc/adtest.com"
```

如果运气好，碰到一个弱口令账户，那么管理员权限就直接到手了。

只需要打开PowerShell运行命令，然后导出票据进行本地破解，看似悄无声息，与正常域内活动很难区分，传统安全设备更是毫无办法。

很多攻击者也是这么认为，但这真的很难检测吗？

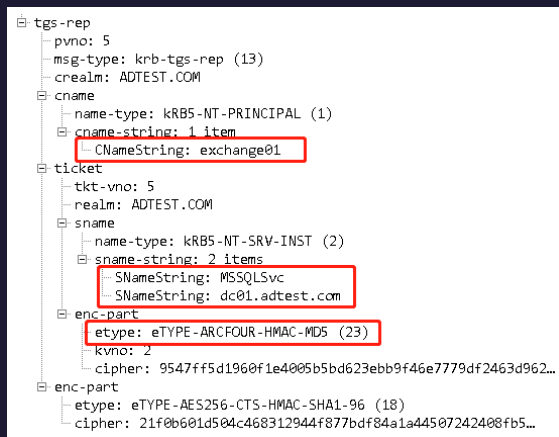
Abnormal Kerberos Protocol — Kerberoasting Detection

从win 2008开始，域内绝大多数的票据加密方式都是AES256，只有极少数情况存在RC4加密。

我们可以：

- 通过对域内的加密方式进行一段时间的统计，排除多数用户使用RC4请求的服务。
- 关注极少出现的RC4服务票据加密方式，同时可结合高风险SPN前缀判断。

TGS-REQ流量分析



4769日志分析



SPN Prefix

MSSQLSvc

MSSQL

FIMService

AGPMServer

exchangeMDB

TERMSERV

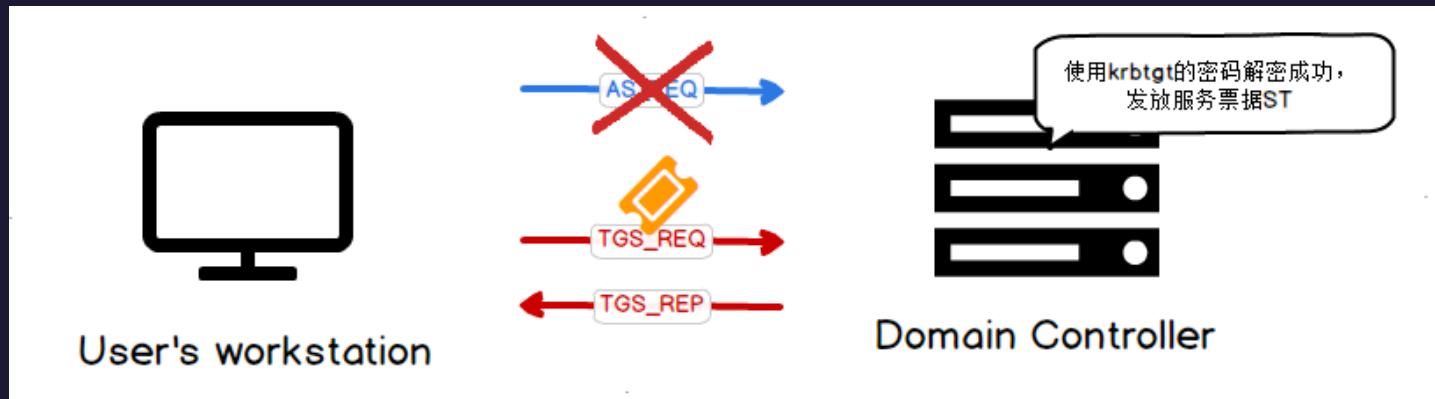
WSMAN

.....

Abnormal Kerberos Protocol — Golden Ticket

TGT使用 `krbtgt` 账户的密码进行加密，如果该密码被攻击者获取，就可以伪造任意身份的TGT，访问任意服务，即**黄金票据**。

因为该TGT是伪造的，所以在Kerberos协议的流程中，缺失了 `AS_REQ` 和 `AS_REP` 的步骤。




Abnormal Kerberos Protocol — Golden Ticket Detection

- AS-REP返回的Ticket字段中，虽然经过krbtgt密码的加密，但我们仍然可以对其计算唯一摘要值。
- 跟踪每一次的AS-REP TGT票据颁发，记录下Ticket Hash，存入列表A。
- 对每一次TGS-REQ中TGT Hash进行确认，判断该值是否存在于已知颁发过的TGT列表A中。如果不存在，则属于伪造的TGT，即黄金票据。
- 列表A的内容可设置过期时间，TGT和ST的默认最大有效期都是10小时。

```

msg-type: krb-tgs-req (12)
✓ padata: 2 items
  ✓ PA-DATA PA-TGS-REQ
    ✓ padata-type: kRB5-PADATA-TGS-REQ (1)
      ✓ padata-value: 6e82058a30820586a003020105a1
        ✓ ap-req
          pvno: 5
          msg-type: krb-ap-req (14)
          Padding: 0
          > ap-options: 00000000
          ✓ ticket
            tkt-vno: 5
            realm: ADTEST.COM
            > sname
            ✓ enc-part
              etype: eTYPE-AES256-CTS-HMAC-SHA
              kvno: 2
              cipher: 7d8a8db269d666870ef8a0068
            > authenticator
  
```

计算Hash



Policy	Security Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Abnormal Kerberos Protocol — Tools Fingerprint

部分安全工具请求Kerberos票据时会有留下一些特殊值，根据这些指纹，了解入侵者使用的工具。

• KDC Options

Normal:

0x40810010、0x40810000、0x60810010

Impacket:

0x50800000

Rubeus、kekeo:

0x40800010

• Domain Format

在正常4769日志中的值:

mimikatz填写/domain字段值为corp:

CORP.QIHOO.NET (固定大写FQDN)

corp (同填写的值)

• Nonce

Normal:

随机值

Kekeo、Rubeus:

1818848256 (硬编码)



Sensitive Actions

Sensitive Actions — Modification of ACL



ACL(**Access Control List**): 定义了在活动目录中谁可以访问哪些对象，拥有什么权限。
SDDL(**Security Descriptor Definition Language**): 描述了ACL中对象和权限的关系。

每一次的ACL修改都会触发事件日志**5136**，内容使用SDDL语法详细描述了权限信息。

```
<Data Name="ObjectDN">CN=Policies,CN=System,DC=360testad,DC=com</Data>
<Data Name="ObjectGUID">{F7D82EAC-DE32-4E96-9ED8-42C5763DE190}</Data>
<Data Name="ObjectClass">container</Data>
<Data Name="AttributeLDAPDisplayName">nTSecurityDescriptor</Data>
<Data Name="AttributeSyntaxOID">2.5.5.15</Data>
<Data Name="AttributeValue">O:DAG:DAD:AI(OA;;CC;f30e3bc2-9ff0-11d1-b603-0000f8
(A;;CCDCLCSWRPWPL0CRRCWDWO;;;DA)(A;;LCRPLORC;;;AI)(A;;CCDCLCSWRPWPDT
00aa006e0529;4828cc14-1437-45bc-9b07-ad6f015e5f28;RU)(OA;CIIOID;RP;4c1642
00aa003049e2;RU)(OA;CIIOID;RP;5f2-2010-79a5-11d0-9020-00c04fc2d4cf;4828cc
9020-00c04fc2d4cf;bf967aba-0de6-11d0-a285-00aa003049e2;RU)(OA;CIIOID;RP;b
```

O:DAG:DAD:AI(OA;CIIO;RP;72e.....3049e2;)(.....)(.....)S:AI(...)(...)

owner_sid group_sid dacl_flags string_ace list sacl_flags string_ace list

```
ace_flags: "CI"
ace_type: "OBJECT ACCESS ALLOWED..."
inherited_object_type: ""
object_type: "bf967a86-0de6-11d0-a285-00aa003
permissions: { ...}
trustee: "S-1-5-21-3942060436-2245087920-1392
user_name: "admin"
```

Sensitive Actions — Modification of ACL Detection

Exchange + NTLM Relay Privilege Escalation Attack

- 通过利用exchange的SSRF漏洞，中继NTLM认证请求到LDAP修改ACL，向某个攻击者控制的账户添加 **Replicating Directory Changes** 和 **Replicating Directory Changes All** 权限，即可使用DCSync进行远程域控密码获取。
- 所以，当我们解析5136日志发现exchange机器账户存在以上行为时，那说明遭受了此类攻击。
- 同时，ACL的修改属于不常见行为，需要监控每一次修改操作。

EventId: 5136
 SubjectUserName: Exchange
 ObjectDN: DC=btv, DC=defcon, DC=org
 ObjectClass: container
 AttributeLDAPDisplayName:
 nTSecurityDescriptor
 AttributeValue: O:DAG:DAD:AI(...)(...)(...)



Exchange add the "Replicating Directory Changes" and "Replicating Directory Changes All" permissions to Hacker.

Sensitive Actions — Privileges Granted Detection



- 添加攻击者控制的账户到一些敏感用户组中，从而维持权限。



Account Operators, Administrators, Backup Operators, Print Operators, Server Operators, Domain Admins, Enterprise Admins, Schema Admins, DnsAdmins, Group Policy Creator Owners, Exchange Trusted Subsystem, etc.

- Event Id: 4728, 4732, 4756

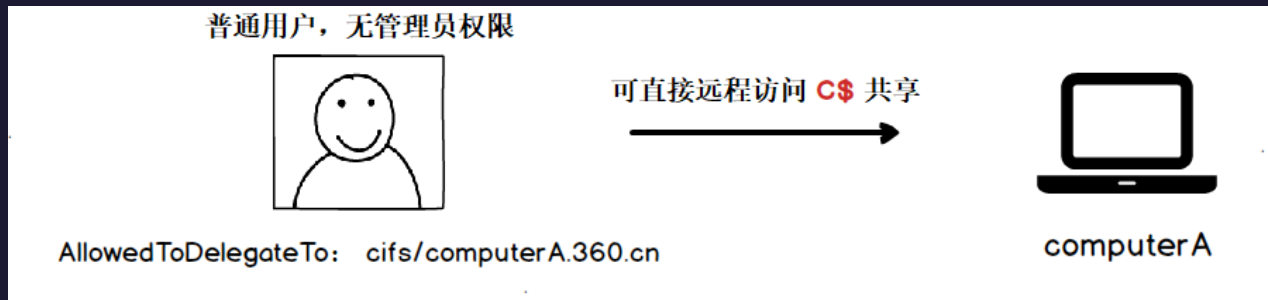
添加账户: **zhushiyu**
用户组: **Domain Admins**

```
- <EventData>
  <Data Name="MemberName">CN=zhushiyu,CN=Users,DC=360testad,DC=com</Data>
  <Data Name="MemberSid">S-1-5-21-2858140052-320346861-478137535-1120</Data>
  <Data Name="TargetUserName">Domain Admins</Data>
  <Data Name="TargetDomainName">360TESTAD</Data>
  <Data Name="TargetSid">S-1-5-21-2858140052-320346861-478137535-512</Data>
  <Data Name="SubjectUserSid">S-1-5-21-2858140052-320346861-478137535-1009</Data>
  <Data Name="SubjectUserName">dcadmin</Data>
  <Data Name="SubjectDomainName">360TESTAD</Data>
  <Data Name="SubjectLogonId">0x15fc6cf9</Data>
  <Data Name="PrivilegeList">-</Data>
```

Sensitive Actions — Constrained Delegation Granted



- Kerberos约束委派允许某个账户访问指定的服务，即使是域控。
- 不同服务名对应不同的服务类型，可以类比白银票据。
- 设置约束委派需要管理员权限。



WMI	HOST RPCSS
PowerShell Remoting	HOST HTTP
WinRM	HOST HTTP
Scheduled Tasks	HOST
Windows File Share (CIFS)	CIFS
LDAP operations including Mimikatz DCSync	LDAP
Windows Remote Server Administration Tools	RPCSS LDAP CIFS

Sensitive Actions — Constrained Delegation Granted Detection

- 通过对攻击者控制的账户设置目标为DC的**约束委派**，从而维持权限。
- 设置约束委派需要修改账户属性，会在域控上触发 **4738** 事件日志。
- 日志中 **AllowedToDelegateTo** 字段的值表明委派的对象，我们重点关注是否存在**敏感计算机**和**敏感服务**。

EventId: **4738**

TargetUserName: **hacker**

AllowedToDelegateTo: LDAP/DC.defcon.org
cifs/DC.defcon.org
HOST/DC.defcon.org

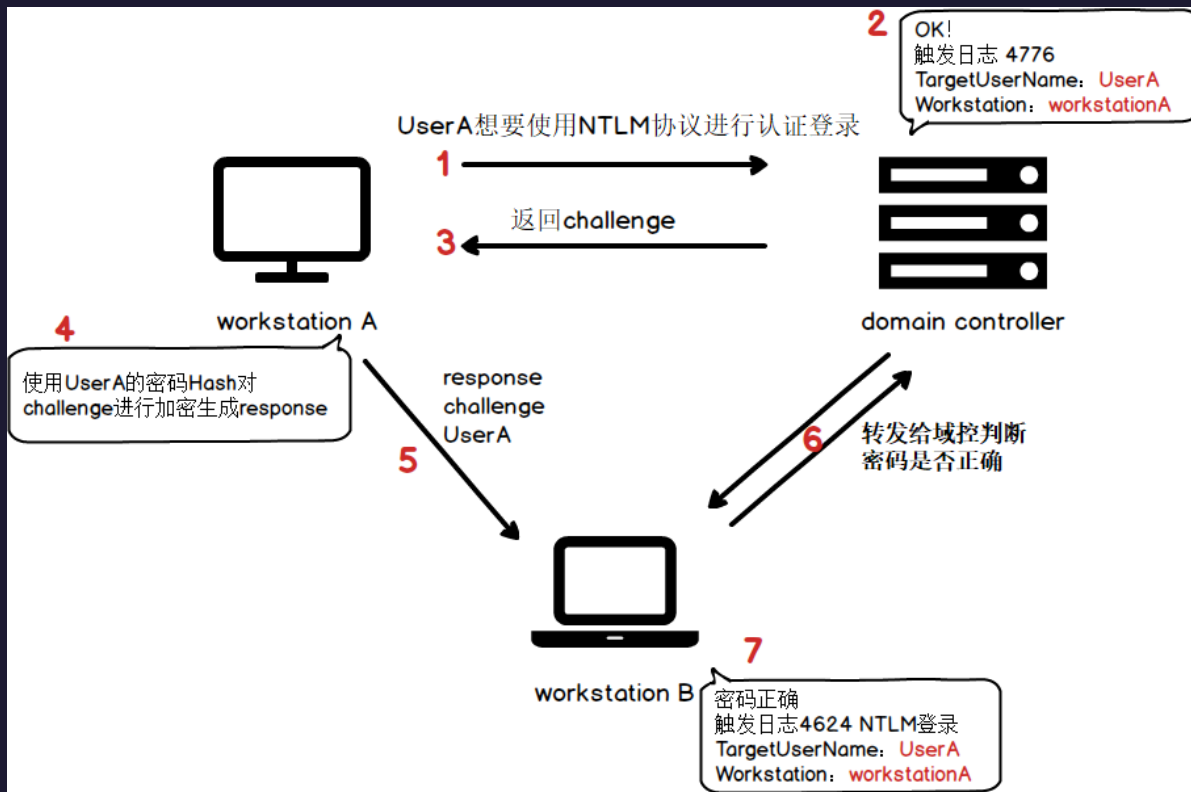
LDAP管理权限
对DC执行DCSync

访问DC上的文件共享

可远程访问DC任何Windows服务

Logon History

Logon History — NTLM Introduction



Logon History — NTLM Relay

- NTLM中继的本质是**中间人攻击**，代替来源计算机与目标机器进行认证交互。
- 通过对高权限账户的NTLM认证请求进行中继，从而暂时获得目标账户的高权限。
- 我们检测的依据是事件日志，虽然登录会留下日志，但存在一个问题：

4624事件日志属于**本地登录行为**，只在目标机器上触发。我们只收集了域控的事件日志，当中继的目标不是域控，我们无法感知。



Logon History — NTLM Relay Detection targeting to DC



- 域控上4624 事件日志记录了每一次目标为域控NTLM登录行为。
- 统计聚合登录相关的事件日志，可以得到域账号、主机名和IP的近期对应关系。
- 被中继的NTLM登录在日志中会留下一些痕迹：“ **IpAddress**” 值为**中继者IP**
- 检查所有4624 NTLM登录日志，关注敏感来源主机的IP发生变化的情况。



4624 NTLM登录日志
WorkstationName: **EXCHANGE**
IpAddress: **192.168.1.3**

Honeypot Account



HoneyPot Account — HoneyPot Account Activity

让我们站在入侵者的角度思考，如何简单快速的提升域内权限：

- 首先找高权限账户，属性adminCount = 1，或者属于管理员组
- 能不能离线票据破解，最好SPN里面有MSSQLSvc这种前缀最好
- Kerberos身份预认证关闭的账户，可以ASREP-Roasting
- 查找拥有约束委派权限的账户，可以直接访问域控
-

以上操作，有些工具都已经能够自动化完成。

我们可以投其所好，针对以上条件，在域内设置一些蜜罐账户，密切监视该账户相关的活动。

Event Id: 4768, 4769, 4770, 4771, 4776, 4624, 4625, 4648等各种活动。

正常情况下，这些账户没有任何域内活动，我们可以假定蜜罐账户所有活动都是入侵者触发的。

HoneyPot Account — Add HoneyPot Account



1. 创建一个足够吸引人的账户，要逼真，比如：

```
username: backup-admin
adminCount: 1
description: 用于临时备份的管理员账户, backupadmin123abc!
memberOf: Domain Admins
SPNs: MSSQLSvc/dc01.360.cn
AllowedToDelegateTo: cifs/dc02.360.cn
                        ldap/dc02.360.cn
```

2. 完善设置

- (1) 设置一个足够复杂的密码，防止被离线破解。
 - (2) 不要使用该账户进行登录或者其它操作，避免在其它地方留下票据等认证缓存。
- > **蜜罐账户的作用是吸引入侵者，设置要小心，不能让账户真的被利用。**

3. 等入侵者上钩

监控相关活动，就算只是 `net user backup-admin /domain`，我们也能感知。

Unknown Threat Detection

Unknown Threat Detection — Privilege Escalation

4672: Special privileges assigned to new logon.

(注意：4672是一个本地事件，即只会在被登录目标上留下事件日志)

接下来我们需要了解，谁会触发**特权登录**事件日志：

- **域管理员组成员**登录
- **本地管理员**登录
- 账户属性 **adminCount = 1** 的账户登录

如果除了这些，一个**陌生账户**也触发了该日志，那么极大可能是**提权成功后的登录**。

Unknown Threat Detection — Privilege Escalation

One of the MS14-068 Detections



- 普通账户通过MS14-068提权之后，当前登录会话期间暂时拥有了管理员权限。
- 如果当前登录的目标是域控，则会在域控上触发4672特权登录事件。
- 我们检查 4672 日志中显示的用户名，判断是否为已知的管理员。

EventId: 4672
SubjectUserName: peter
SubjectUserSid: S-1-2-5-21-.....



Who is peter ?!
Why can he leave
the 4672 log ?!



Conclusion



- 检测逻辑编写时需要了解每种**攻击背后原理**，如DCShadow是“影子域控”，攻击时会伪装成域控发送同步请求，所以检测重点关注**非已知域控计算机执行域控专属的操作**，这样才不会有误报同时也难以绕过。
- 事件**日志** + **流量**能检测绝大部分攻击手法，覆盖几乎所有**关键变动**，要想绕过检测提权，除非不使用任何的域特性，比如：MS17-010直接打域控。
- 既然检测**域渗透活动**并不是那么困难，那为什么你家域的大门常打开？

Achievements — What can WatchAD do?



- **加固内网防御** —— 日益增多的钓鱼直入内网，帮你及时发现内网威胁。
- **红蓝对抗** —— 想完全绕过WatchAD，不触发任何异常，将极大增加红队攻击成本。
- **“护网”利器** —— 自定义设置，将关键资产添加到敏感实体列表中，监控异常活动。
- **高级威胁分析** —— 当针对公司的渗透活动利用域相关特性进行攻击，可检测相关威胁。

Achievements — Detection In 360



该系统已在360内部上线运行半年，监控办公网主域的**所有域控**，分析引擎依靠一台**8核服务器**，每天处理日志超过**100G**，日均误报不超过**10条**。

部分成果：

- 内部红队**RedTeam**域渗透**攻击演习**多次捕获，无关键手法漏报。
- 某员工机器感染恶意软件**攻击域控**。
- 某杀毒软件在域环境下异常**信息查询**行为。
- 某员工办公网违规调试程序执行域**信息扫描**。

... ..

- 相关技术点议题入选 **DEFCON 27 @ BTV**



Detections — Based on Event logs



信息探测:

- 使用SAMR查询敏感用户组
- 使用SAMR查询敏感用户
- 蜜罐账户活动
- PoLoggedOn信息收集

横向移动:

- 账户爆破
- 显式凭据远程登录
- 目标域控的远程代码执行
- 未知文件共享名

凭证盗取:

- AS-REP Roasting
- 远程Dump域控密码

防御绕过:

- 域控事件日志被清空
- 域控事件日志服务被关闭

Detections — Based on Event logs



权限提升:

- ACL修改
- MS17-010攻击检测
- 新增组策略监控
- NTLM 中继检测
- 基于资源的约束委派权限授予检测
- 攻击打印机服务 SpoolSample
- 未知权限提升

权限维持:

- AdminSDHolder对象修改
- DCShadow攻击检测
- DSRM密码重置
- 组策略委派权限授予检测
- Kerberos约束委派权限授予检测
- 敏感用户组修改
- 域控新增系统服务
- 域控新增计划任务
- SIDHistory属性修改
- 万能钥匙-主动检测

Detections — Based on Kerberos traffic



基于流量检测：

Kerberoasting

Kerberos票据加密方式降级

异常的Kerberos票据请求

MS14-068攻击检测

Kerberos约束委派滥用

万能钥匙-被动检测

黄金票据

WatchAD Web Platform — Threat Activities



WatchAD — AD Security Intrusion Detection System

DashboardThreat ActivitiesInvasionsConfiguration

Search users, computers and groups ...

Fast Filter

All (195)

auto_ignore (22)

ignore (16)

pending (157)

All (157)

medium (21)

high (17)

low (119)

09-11 21:27

Abnormal constrained delegation activity 权限提升 待处理

来自于 10.1.1.1 使用身份 ya... 通过约束委派获得了目标 Administrator 对于计算机... 的身份权限, 对应的服务为 cifs.

2019-09-11 21:27:23

09-09 22:40

Abnormal constrained delegation activity 权限提升 待处理

来自于 10.1.1.1 使用身份 2个用户 通过约束委派获得了目标 Administrator 对于计算机... 的身份权限, 对应的服务为 cifs.

从 2019-09-09 19:14:52 至 2019-09-09 22:40:23

09-09 22:27

Suspicious access print server 权限提升 待处理

域控 6个域控 收到了来自于 10.1.1.1 (3个计算机) 身份为... 的主动认证发起请求, 该行为一般用于诱导域控发起NTLM认证, 经恶意目标中继而提升权限.

从 2019-09-09 11:07:58 至 2019-09-09 22:27:08

09-09 11:23

Suspicious access print server 权限提升 待处理

域控 10.1.1.1 收到了来自于 10.1.1.1 身份为 y... 主动认证发起请求, 该行为一般用于诱导域控发起NTLM认证, 经恶意目标中继而提升权限.

2019-09-09 11:23:26

Field Select

Select field

Time Select

Start time

End Time

Level

High Medium Low

Threat Types

Select threat type

Status

pending

Filter

WatchAD Web Platform — Invasions



WatchAD — AD Security Intrusion Detection System

Dashboard

Threat Activities

Invasions

Configuration

Search users, computers and groups ...



09-12 05:27

来自于10 [redacted] 的入侵事件

Encryption Downgrade activity

横向移动

待处理

来自于 [redacted] 请求了目标账户 [redacted] 的弱加密票据。服务名称为 krbtgt，加密方法降级为 rc4-hmac，而正常加密方法为 aes256-cts-hmac-sha1-96。通常这伴随着 OverPassHash、PassTheTicket、GoldenTicket等攻击的发生，或者是其它与票据相关的攻击行为。
2019-09-15 23:06:23

Encryption Downgrade activity

横向移动

待处理

来自于 [redacted] 请求了目标账户 [redacted] 的弱加密票据。服务名称为 evservice，加密方法降级为 rc4-hmac，而正常加密方法为 aes256-cts-hmac-sha1-96。通常这伴随着 OverPassHash、PassTheTicket、GoldenTicket等攻击的发生，或者是其它与票据相关的攻击行为。
2019-09-15 23:05:48

Abnormal constrained delegation activity

权限提升

待处理

来自于 [redacted] 使用身份 ya [redacted] 通过约束委派获得了目标 Administrator 对于计算机 [redacted] 的身份权限，对应的服务为 cifs。
2019-09-12 05:27:23

Encryption Downgrade activity

横向移动

待处理

来自于 10 [redacted] 请求了目标账户 YAN [redacted] 的弱加密票据。服务名称为 krbtgt，加密方法降级为 rc4-hmac，而正常加密方法为 aes256-cts-hmac-sha1-96。通常这伴随着 OverPassHash、PassTheTicket、GoldenTicket等攻击的发生，或者是其它与票据相关的攻击行为。
2019-09-12 05:26:58

Suspicious access print server

权限提升

待处理

域控 E [redacted] 收到了来自于 10 [redacted] 身份为 ya [redacted] 的主动认证发起请求，该行为一般用于诱导域控发起NTLMAuth，经恶意目标中继后提升权限。
2019-09-09 19:23:26

09-10 03:14

来自于 [redacted] 的入侵事件

WatchAD Web Platform — Threat Details



WatchAD — AD Security Intrusion Detection System

DashboardThreat ActivitiesInvasionsConfiguration

Search users, computers and groups ...

Abnormal constrained delegation activity 权限提升 待处理

来自于 10... (-) 使用身份 2个用户 通过约束委派获得了目标 Administrator 对于计算机 1... 的身份权限, 对应的服务为 cifs.

从 2019-09-09 19:14:52 至 2019-09-09 22:40:23

使用身份 2个可疑账户 Administrator 对该计算机的权限


时间	来源IP	来源计算机	使用身份	target_computer	目标用户	target_service
2019-09-09 19:14:52	10...	1...	11\$	1...	Administrator	cifs
2019-09-09 22:40:23	10...	1...	11\$	1...	Administrator	cifs

原始日志


时间	名称	事件ID	处理域控	日志编号	操作	展开详情
2019-09-09T06:18:49.493Z	Kerberos 服务票证操作	4769	1...	9332508530	格式化	>
2019-09-09T09:28:05.085Z	Kerberos 服务票证操作	4769	1...	9340711851	格式化	>

处理建议

WatchAD Web Platform — Entry Activities


WatchAD — AD Security Intrusion Detection System

[Dashboard](#)
[Threat Activities](#)
[Invasions](#)
[Configuration](#)



朱思

安全中心

员工编号

域账号

所属域

邮箱

上级

活动

域内的相关活动记录

1

详细信息

具体的活动目录信息

威胁活动

1

访问实体

0

登录IP

21

使用计算机

1

Search sensitive group using SAMR

信息探测

已忽略


来自 10.10.10.10 (10.10.10.10) 的账户 zh 使用SAMR查询了敏感组 Domain Admins 的信息。

从 2019-05-05 22:26:25 至 2019-05-08 18:32:55

请选择


存在 1 个相关的威胁活动

共查询到 0 条相关的域内活动记录




无相关域内活动记录

WatchAD Web Platform — Entry Details

 WatchAD — AD Security Intrusion Detection System

DashboardThreat ActivitiesInvasionsConfiguration

Search users, computers and groups ...



zhusiyu1

zh...@360.cn

员工编号

Q0...

域账号

Zh...

所属域

CORP

邮箱

zh...@360.cn

上级

活动

域内的相关活动记录

1

详细信息

具体的活动目录信息

账号信息

SAM 名称 zhusiyu1

SID S-1-5-21-39420604...

UPN zh...@360.cn

DN CN=...

SPNs

创建于 2017-11-16 09:14:52

约束委派

用户访问控制

禁用账户

允许空密码

允许保存文本密码

密码永不过期

要求智能卡

可无约束委派

该账户无法被委派

只能使用DES加密

不要Kerberos预身份认证

密码已过期

用户组信息

直属用户组 (8)

g26

g26

F

递归用户 (3)

e360 2nd

sd 2nd


brain 2nd

组织架构

上级/经理

直接下属 (0)

WatchAD Web Platform — Settings

 WatchAD — AD Security Intrusion Detection System

[Dashboard](#)[Threat Activities](#)[Invasions](#)[Configuration](#)

System

- Domain List
- DC Name List
- LDAP Setting
- Raw Data Expire

Detection

- Sensitive Entry
- HoneyPot Account
- Kerberos**
- Exclusions

Notifications and Reports

- Alarms Merge
- Notifications
- Mail Server

Other

- About

Kerberos

Ticket Lifetime

TGT maximum lifetime hours

ST maximum lifetime mins

High Risk SPN Prefix

MSSQLSvc

×

MSSQL

×

FIMService

×

AGPMService

×

exchangeMDB

×

TERMSERV

×

WSMAN

×

Microsoft Virtual Console Service

×

STS

×

enter spn prefix

Add

High Risk Delegation Prefix

ldap/

×

http/

×

HOST/

×

cifs/

×

krbtgt/

×

mssqlsvc/

×

enter delegation pre

Add

Save

WatchAD

— AD Security Intrusion Detection System

Talk is cheap, 开源!

- **检测引擎** — 基于事件日志检测的完整代码

<https://github.com/0Kee-Team/WatchAD>

- **Web平台** — 前后端完整代码

<https://github.com/0Kee-Team/WatchAD-Web>

THANKS

欢迎大家踊跃提交 issue 和 PR !

