بسمه تعالی


**سازمان فناوری اطلاعات ایران**

**معاونت امنیت فضای تولید و تبادل اطلاعات**

**مرکز ماهر**

# بررسی حملاتCLDAP Amplification و راه‌های مقابله با آن

**تیرماه ۹۸**

فهرست مطالب


**۱ چکیده ..... ۱**
**۲ تاثیر آسیب پذیری ..... ۱**
**۳ اسکن آسیب پذیری ..... ۱**
**۴ مشخصه های حمله ..... ۳**
**۵ جزییات حمله ..... ۴**
**۶ پیاده سازی حمله ..... ۶**
۶-۱ شبیه سازی حمله ..... ۷
**۷ اقدامات جهت کاهش شدت آسیب پذیری ..... ۱۰**
**۸ جمع بندی و نتیجه‌گیری ..... ۱۱**
**۹ منابع ..... ۱۲**

# ۱ چکیده

برای نخستین بار در سال ۲۰۱۶، مرکز عملیات امنیتی شرکت Akamai، یک حمله انکار سرویس توزیع شده بازتابی (DDoS) را شناسایی کردند که از پروتکل سبک[۱] و غیراتصال‌گرای[۲] دسترسی مسیر (CLDAP[۳]) بهره‌برداری می‌کرد. این روش جدید بازتاب و تقویت، می‌توانست باعث تولید حملات انکار سرویس توزیع شده (DDoS) با سرعت حداکثر ۷۰ برابر شود.

مانند بسیاری از دیگر حملات بازتابی و تقویتی، در صورتی که فیلترینگ ورودی به طور مناسب انجام گیرد، امکان این حمله وجود نخواهد داشت. در ادامه به بررسی بیشتر این حمله و روش‌های جلوگیری از آن خواهیم پرداخت.

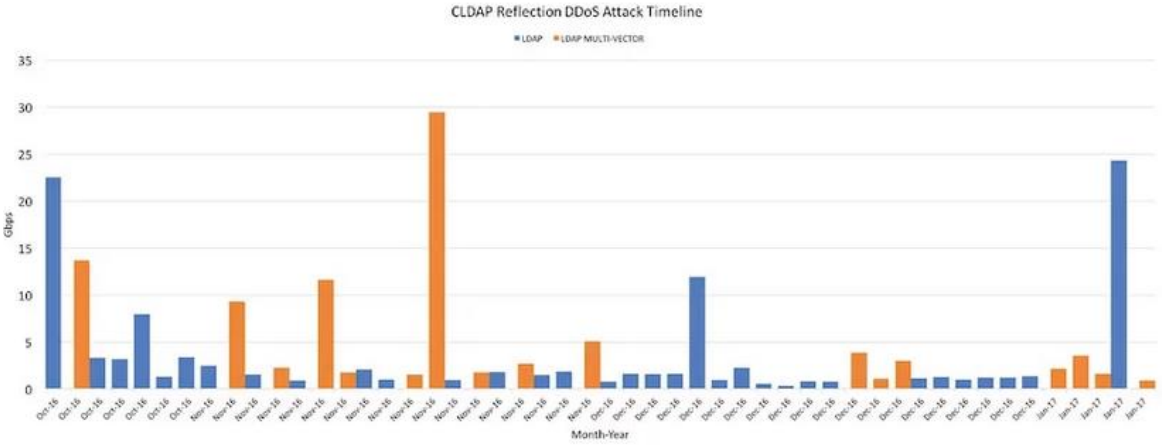
# ۲ تاثیر آسیب‌پذیری

مهاجمان می توانند از پهنای باند و اعتماد نسبی سرورهای بزرگ که پروتکل های UDP ارائه می‌دهند، استفاده کنند و قربانیان را با سیلی از ترافیک ناخواسته مواجه کرده و یک حمله DDoS ایجاد کنند. سطح این آسیب‌پذیری، متوسط گزارش شده است.

# ۳ اسکن آسیب‌پذیری

با استفاده از اسکن اینترنت و فیلتر کردن پورت مقصد ۳۸۹ پروتکل UDP می‌توان میزبان‌های بالقوه‌ای برای این حمله را پیدا کرد. مرکز عملیات امنیتی شرکت Akamai در مجموع ۷،۶۲۹ بازتابنده حمله منحصر به فرد CLDAP را بر اساس منابع جمع آوری شده در طی ۵۰ حمله بازتابی[۴] واقعی CLDAP صورت گرفته از ۱۴ اکتبر ۲۰۱۶ تا ۱۳ ژانویه ۲۰۱۷ شناسایی کرده است؛ اگرچه هم‌اکنون لیست بازتابنده‌های این حمله بیشتر از این مقدار تخمین زده می‌شود.

[۱] Lightweight
[۲] connection-less
[۳] Connection-less Lightweight Directory Access Protocol
[۴] Reflection




**شکل ۱: حملات بازتاب CLDAP صورت گرفته از ۱۴ اکتبر ۲۰۱۶ تا ۱۳ ژانویه ۲۰۱۷. میله‌های نارنجی نشان‌دهنده حملاتی هستند که علاوه بر CLDAP از بردارهای حمله دیگری نیز استفاده کرده‌اند.**

اکثریت قریب به اتفاق این حملات (۳۳ مورد از ۵۰ حمله)، حملاتی هستند که فقط از یک بردار حمله استفاده کرده‌اند، به این معنی که همه درخواست های فرستاده شده از نوع CLDAP خالص بوده و هیچ پروتکل دیگری استفاده نشده است. این غیر معمول است، زیرا بیشتر حملات DDoS از پروتکل های متعددی برای عبور از سیستم‌های حفاظت DDoS استفاده می‌کنند.

باتوجه به موفقیت آمیز بودن حملات DDoS انجام شده با این روش، تعداد این حملات از زمان پیدایش اولین حمله، در حال افزایش بوده است. از طرفی پیدا کردن منابع CLDAP برای حمله، تنها نیازمند یک اسکن برای پورت‌های باز udp 389 است. دلایل افزایش این حملات را می‌توان موارد زیر دانست:

- شرکت‌ها پروتکل CLDAP (پورت ۳۸۹ از udp) را روی تمام ترافیک‌های وروی و خروجی شبکه خود فیلتر نمی‌کنند.
- ارائه‌دهندگان خدمات اینترنت (ISPها) پورت مربوط به CLDAP را در لیست پورت‌های فیلتر شده برای جلوگیری از بهره‌برداری[۵] قرار نمی‌دهند (حتی برخی از ISP ها لیستی برای فیلتر کردن پورت‌ها ندارند.)
- فراهم‌کنندگان ابر[۶] به مشتریانشان اجازه می‌دهند تا بتوانند نمونه‌های جدیدی با پورت CLDAP باز تولید کنند و به این ترتیب هر نمونه می‌تواند یک بازتابنده CLDAP برای انجام حمله DoS باشد.

[۵] exploit
[۶] cloud

## ۴ مشخصه های حمله

در ۷ ژانویه سال ۲۰۱۷، یکی از بزرگترین حمله های DDoS که با استفاده از بازتاب cldap به عنوان عامل اصلی انجام شده بود توسط akamai مشاهده و مقابله شد. ویژگی های این حمله عبارت بودند از:

- زمینه صنعت: اینترنت و مخابرات
- اوج پهنای باند: ۲۴ گیگابیت در ثانیه
- بیشترین تعداد بسته ها در هر ثانیه: ۲ میلیون بسته در هر ثانیه
- مسیر حمله: CLDAP
- پورت منبع: ۳۸۹
- پورت مقصد: تصادفی

```
CLDAP Reflection Attack – Largest Observed Response is 3,662 Bytes:

17:35:25.728099 IP A.A.A.A.389 > Z.Z.Z.Z.46414: UDP, bad length 3006 > 1472
17:35:25.728102 IP B.B.B.B.389 > Z.Z.Z.Z.38980: UDP, bad length 3662 > 1472
17:35:25.728106 IP A.A.A.A > Z.Z.Z.Z: ip-proto-17
17:35:25.728110 IP A.A.A.A > Z.Z.Z.Z: ip-proto-17
17:35:25.728115 IP B.B.B.B > Z.Z.Z.Z: ip-proto-17
17:35:25.728127 IP B.B.B.B > Z.Z.Z.Z: ip-proto-17
```

**شکل ۲: نمونه حمله بازتاب CLDAP با ۳،۰۰۶ و ۳،۶۶۲ تا از داده‌های پاسخ مربوطه**

شکل ۲، نشان می دهد که این حمله توانایی فشرده‌سازی قابل توجهی دارد. پس از اولین حملات با استفاده از CLDAP، Akamai SIRT[۷] توانست پرس‌وجوهای بازتابی[۸] نمونه‌های مخرب CLDAP را به دست آورد. حجم پرس وجو فقط ۵۲ بایت است. این بدان معنی است که فاکتور تقویت پایه (baf) برای بارگیری اطلاعات ۳۶۶۲ بایتی و بارگیری پرس‌وجوی ۵۲ بایتی، ۷۰ برابر بود (یعنی طول پاسخ هر پرس‌وجو حدود ۷۰ برابر طول پرس‌وجو بود)، اگر چه فقط یک میزبان، این میزان پاسخ را برگردانده است. تجزیه و تحلیل حمله پس از آن نشان داد که فاکتور تقویت متوسط در طول این حمله، ۵۶،۸۹ برابر بوده است.

[۷] Security incident response team

[۸] reflection queries

این حمله ۲۴ گیگابایت بر ثانیه برآورد شده است. در مقابل، کوچکترین حمله مشاهده شده ۳۰۰ مگابیت بر ثانیه بوده، و پهنای باند متوسط حمله CLDAP برابر 3 Gbps بوده است.

## ۵ جزییات حمله

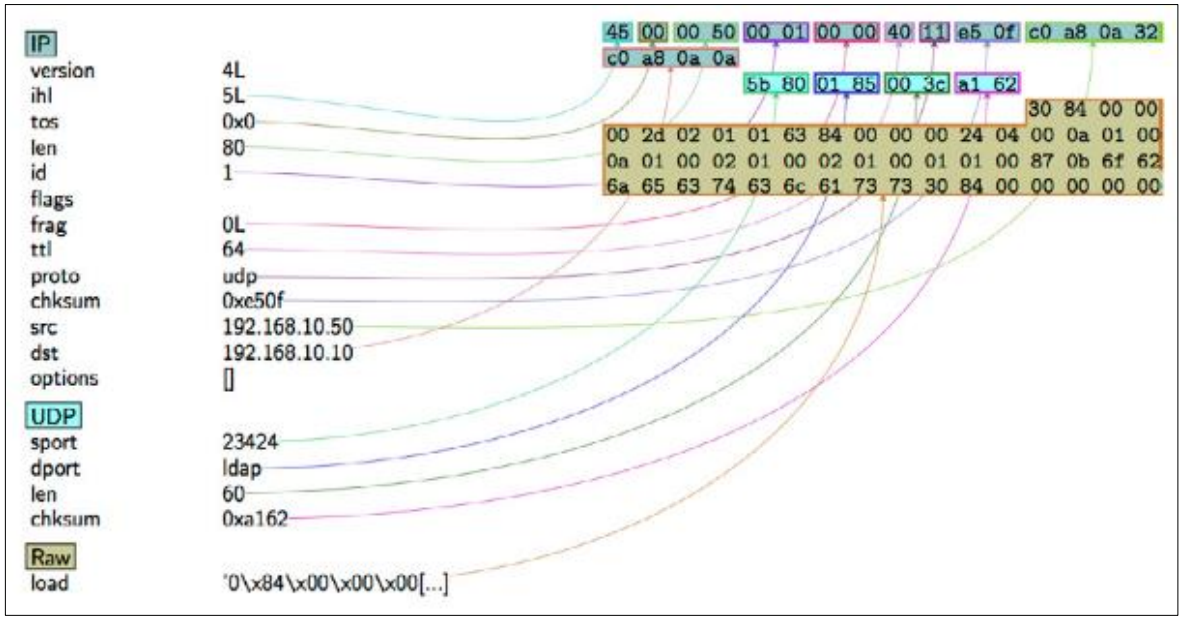
پروتکل CLDAP دارای قابلیت‌های اضافی است که توسط مایکروسافت به آن افزوده شده است و یک جایگزین کارآمد برای پرس‌وجوهای LDAP است که با پروتکل TCP انجام می‌شوند، اما CLDAP از همه ویژگی‌های موجود در LDAP پشتیبانی نمی‌کند. LDAP یکی از پروتکل‌هایی است که بیشترین استفاده را برای دسترسی به اطلاعات نام کاربری و رمز عبور در پایگاه داده‌هایی مانند Active Directory در بسیاری از سرورهای آنلاین دارد. یک سرور Active Directory که سرویس CLDAP در آن نادرست پیکربندی شده باشد، این سرویس را از طریق اینترنت در دسترس قرار می‌دهد، که این باعث آسیب‌پذیر شدن سرور در برابر حملات DDoS می‌شود.

در مراحل ابتدایی این حمله، Akamai SIRT پرس‌وجوهای مخرب CLDAP را که در تلاش بودند تا داده‌های پاسخ LDAP را به اهداف (URLها) مختلف بازتاب کنند، مشاهده کرد. شکل ۳ پرس‌وجوهای مشاهده شده در طی یک حمله واقعی بازتابی CLDAP را نشان می‌دهد. اینها شامل تعداد انگشت شماری از سرورها (اهداف مورد نظر) برای چند میزبان LDAP هستند.

```
13:55:57.962697 IP X.X.X.X.57852 > X.X.X.X.389: UDP, length 52
13:55:57.963784 IP X.X.X.X.33850 > X.X.X.X.389: UDP, length 52
13:55:57.964392 IP X.X.X.X.47097 > X.X.X.X.389: UDP, length 52
13:55:57.965226 IP X.X.X.X.47728 > X.X.X.X.389: UDP, length 52
```

**شکل ۳: پرس و جوهای مخرب CLDAP فرستاده شده به پورت مقصد ۳۸۹ که هر پرس‌وجو فقط شامل ۵۲ بایت داده است.**

با استفاده از بارگیری داده‌های مشابه شکل ۳، این پرس و جو می‌تواند به راحتی با استفاده از ابزاری مانند Scapy بازتولید شود. آزمون‌های آزمایشگاهی با استفاده از یک نمونه مجازی از ویندوز سرور و لینوکس با Scapy انجام شده است. ارسال پرس و جو از میزبان لینوکس به سرور ویندوز در ابتدا هیچ پاسخی نداشت. با این حال، هنگامی که سرور ویندوز به عنوان کنترل کننده دامنه راه اندازی شد و شروع به گوش دادن روی پورت ۳۸۹ udp و tcp کرد، تراکنش شکل ۴ ثبت شد.

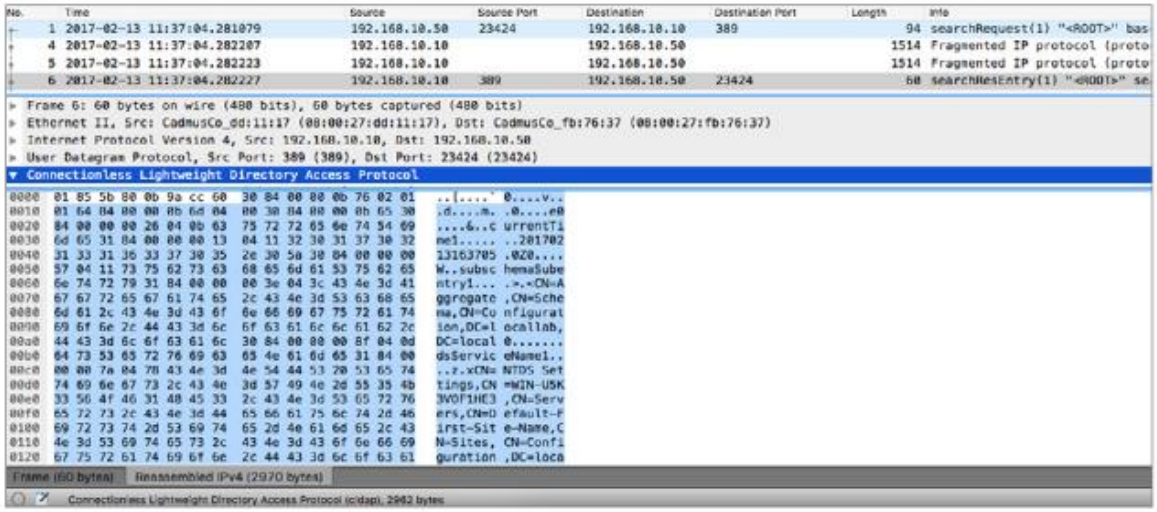



**شکل ۴: بسته پرس و جوی CLDAP**

```
CLDAP  Query Test and Response in a Lab Test

11:37:04.281079 IP linux_host.23424 > windows_server.389: UDP, length 52
11:37:04.282207 IP windows_server.389 > linux_host.23424: UDP, bad length 2962 > 1472
11:37:04.282223 IP windows_server > linux_host: ip-proto-17
11:37:04.282227 IP windows_server > linux_host: ip-proto-17

CLDAP Sample of Printable Response Text

Packet 1
2[`0vdm0e0&currentTime120170213163705.0Z0WsubschemaSubentry1><CN=Aggregate,CN=Schema,CN=Configu-
ration,DC=locallab,DC=local0
dsServiceName1zxCN=NTDS
Settings,CN=WIN-U5K3VOF1HE3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,D-
C=locallab,DC
<snip>

Packet 2
<snip>
WIN-U5K3VOF1HE3.locallab.local0GldapServiceName10.locallab.local:win-u5k3vof1he3$@LOCALLAB.LOCAL0{
serverName1igCN=WIN-U5K3VOF1HE3,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=locall
ab,DC=local0supportedCapabilities11.2.840. 113556.1.4.8001.2.840.113556.1.4.16701.2.840.113556.1.4.17911.2.840.
113556.1.4.19351.2.840.113556.1.4.20801.2.840.113556.1.4.22370isSynchronized1TRUE0"isGlobalCatalogReady1TR
UE0domainFunctionality160forestFunctionality160(domainControllerFunctionality160e
```

**شکل ۵: پرس و جوی CLDAP از ویندوز سرور ۲۰۱۲ با ۲,۹۶۲ بایت پاسخ**

payload دو پاسخ نخست، حاوی بیشترین میزان داده‌ها با اندازه ۱۴۷۲ بایت و ۱۴۸۰ بایت بودند و آخرین قطعه حاوی ۱۰ بایت باقیمانده بود. این نسخه، نمونه جدیدی از ویندوز سرور ۲۰۱۲، بدون هیچ گزینه یا تنظیم دیگری است. نسخه های دیگر ممکن است اندازه‌های مختلف پیلود را تولید کنند.




**شکل ۶: payload پاسخ ۲,۹۶۲ بایتی CLDAP تولید شده در آزمایشگاه**

اندازه پیام و محتویات آن می‌تواند از آنچه در طی این حملات مشاهده شده، متفاوت باشد. این شامل پارامترهای پیکربندی سرور و سایر تنظیمات می‌شود.

حملات بازتابی دیده شده با استفاده از "اسکریپت‌های حمله" راه‌اندازی می‌شوند. این اسکریپت‌های حمله معمولاً با استفاده از زبان برنامه‌نویسی C نوشته می‌شوند و از یک بردار حمله به بردار دیگر، بسیار شبیه هستند. گزینه‌هایی که معمولاً با این اسکریپت‌های حمله قابل دسترسی هستند، عبارتند از IP هدف، پورت هدف، لیست بازتابنده ها و محدودیت زمانی. زمانی که این اسکریپت‌ها اجرا می‌شوند، IP هدف، منبع بارگیری همه ۵۲ بایت پرس‌وجو می‌شود. سپس آنها به سرعت به هر سرور در لیست بازتابنده ارائه می‌شوند. از آنجا، سرورهای CLDAP همانطور که طراحی شده اند، به پرس و جو پاسخ می‌دهند. در نتیجه، هدف این حمله باید با سیل پاسخ درخواست‌های CLDAP مقابله کند.

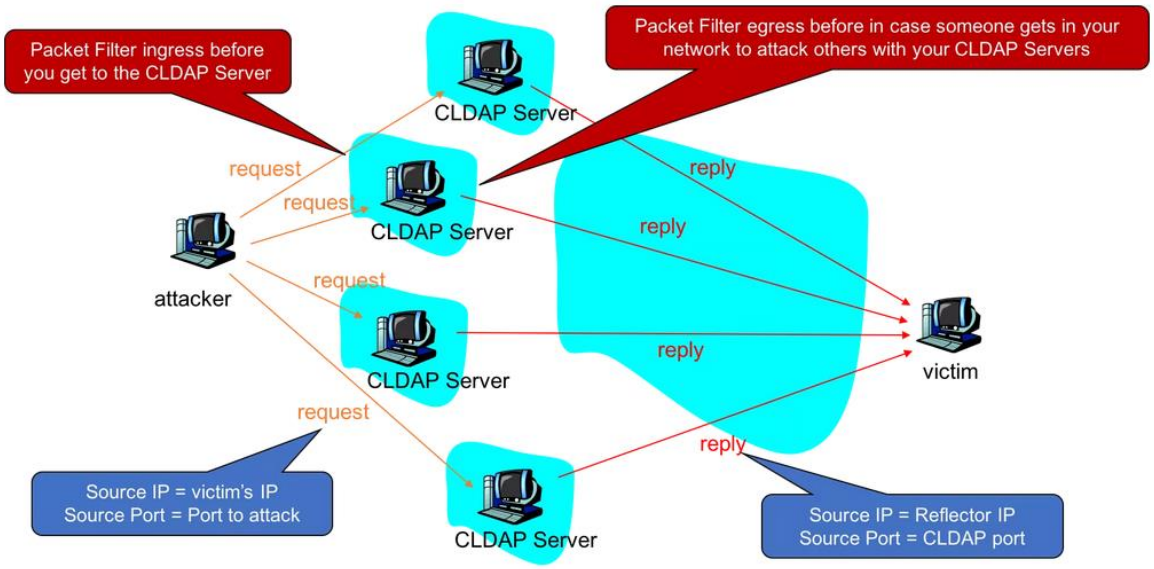
## ۶ پیاده سازی حمله

CLDAP از پروتکل غیراتصال‌گرای UDP استفاده می‌کند. این پروتکل برای اختصاص آدرس‌های IP به میزبان های جدید متصل شده به شبکه، استفاده می‌شود و مهاجمان می‌توانند از سرورهای متخلف برای تولید تعداد زیادی درخواست CLDAP به منظور غلبه بر یک سیستم هدف استفاده کنند.

حمله بازتابی جدید DDoS روی CLDAP ، یک عامل تقویت کننده تا ۷۰ برابر دارد که آن را یکی از معروفترین پروتکل های قابل سوء استفاده UDP کرده است.

در این حمله، مهاجم از زیرساخت CLDAP درخواست بازیابی تمام کاربران ثبت شده در Active directory را می‌کند. از آنجا که مهاجم این پرس و جو را طوری می‌سازد که به‌نظر برسد قربانی آن را فرستاده، آدرس IP

فرستنده درخواست را با IP قربانی جایگزین می‌کند؛ سپس سرویس CLDAP جواب را به قربانی ارسال خواهد کرد. در نتیجه، سیستم قربانی با اطلاعاتی که درخواست نکرده، بمباران می شود.




**شکل ۷: شمایی از حمله بازتابی CLDAP**

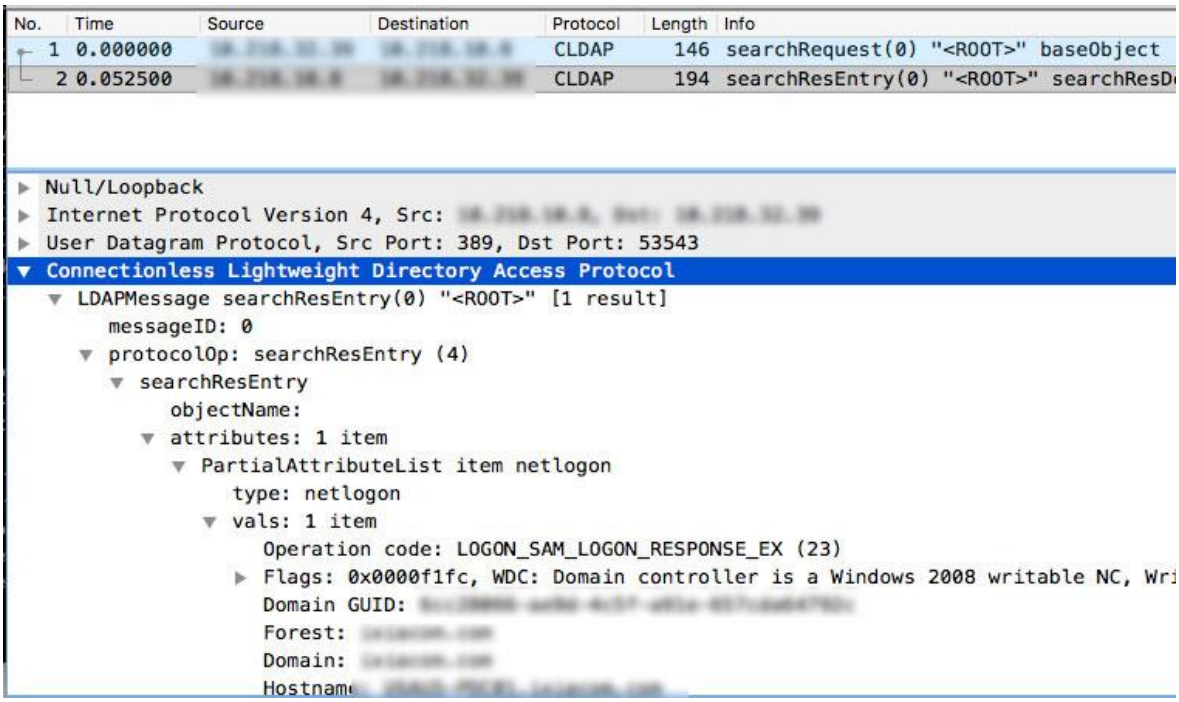
## ۶-۱ شبیه‌سازی حمله

از معمول‌ترین استفاده‌های CLDAP برای کاربردی است که پرس‌وجوی Netlogon نامیده و با عنوان "AD ping" نیز شناخته می شود که به عنوان یک مکانیزم اولیه کشف، توسط میزبان‌های ویندوزی مورد استفاده قرار می‌گیرد. برای شبیه‌سازی این حمله می‌بایست یک ابزار برای بازسازی این پینگ پیدا کنیم و بتوانیم برخی از پاسخ های این پرس‌وجو را تقویت کنیم.

پس از جستجو در اینترنت، به قطعه کدی از تیم سامبا می‌رسیم. این کد، یک پرس‌وجو از یک کنترل‌کننده دامنه است و به عنوان یک درخواست RootDSE یا "Netlogon" ارسال می‌شود. در شکل ۸ و ۹، تصویری از خروجی CLI و آنچه Wireshark نشان می‌دهد، آمده است.

```
$perl ./cldap.pl -d
Information for Domain Controller:

Response Type: SAMLOGON
GUID:
Flags:
        Is a PDC:                                       no
        Is a GC of the forest:                          yes
        Is an LDAP server:                              yes
        Supports DS:                                    yes
        Is running a KDC:                               yes
        Is running time services:                       yes
        Is the closest DC:                              yes
        Is writable:                                    yes
        Has a hardware clock:                           no
        Is a non-domain NC serviced by LDAP server:     no
Forest:
Domain:
Domain Controller:
Pre-Win2k Domain:
Pre-Win2k Hostname:
Unk:
Server Site Name:
Client Site Name:
NT Version:             5
LMNT Token:             ffff
LM20 Token:             ffff
```

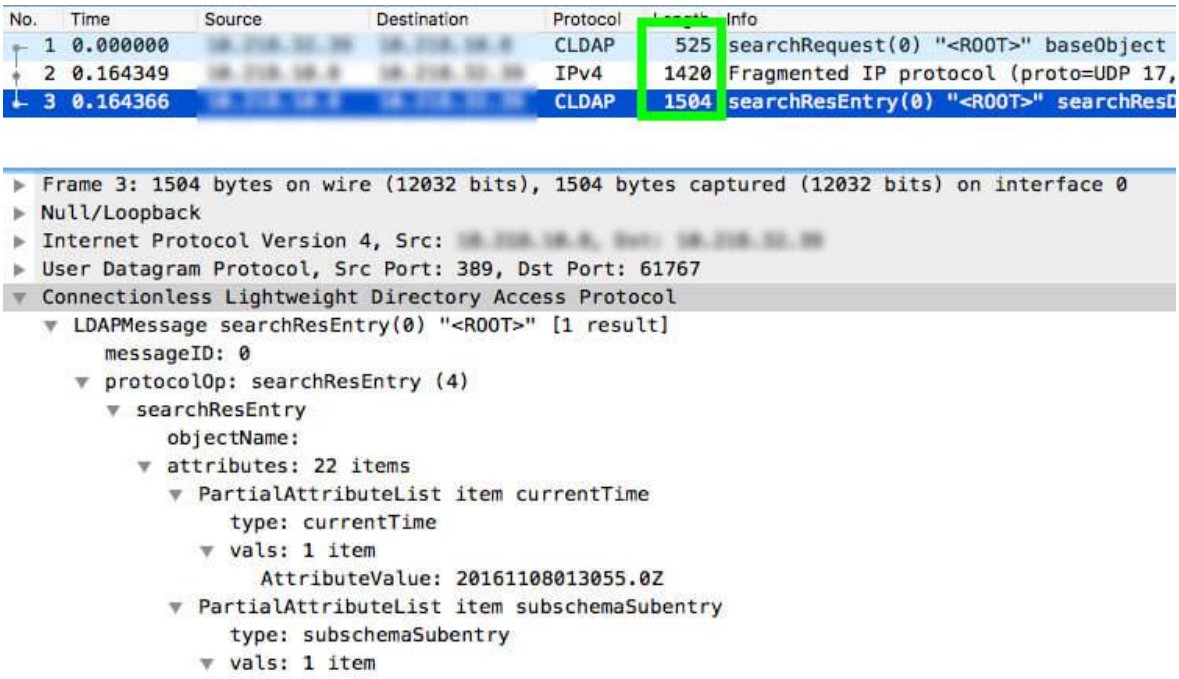
**شکل ۸: خروجی CLI**




**شکل ۹: خروجی نمایش داده شده در وایرشارک**

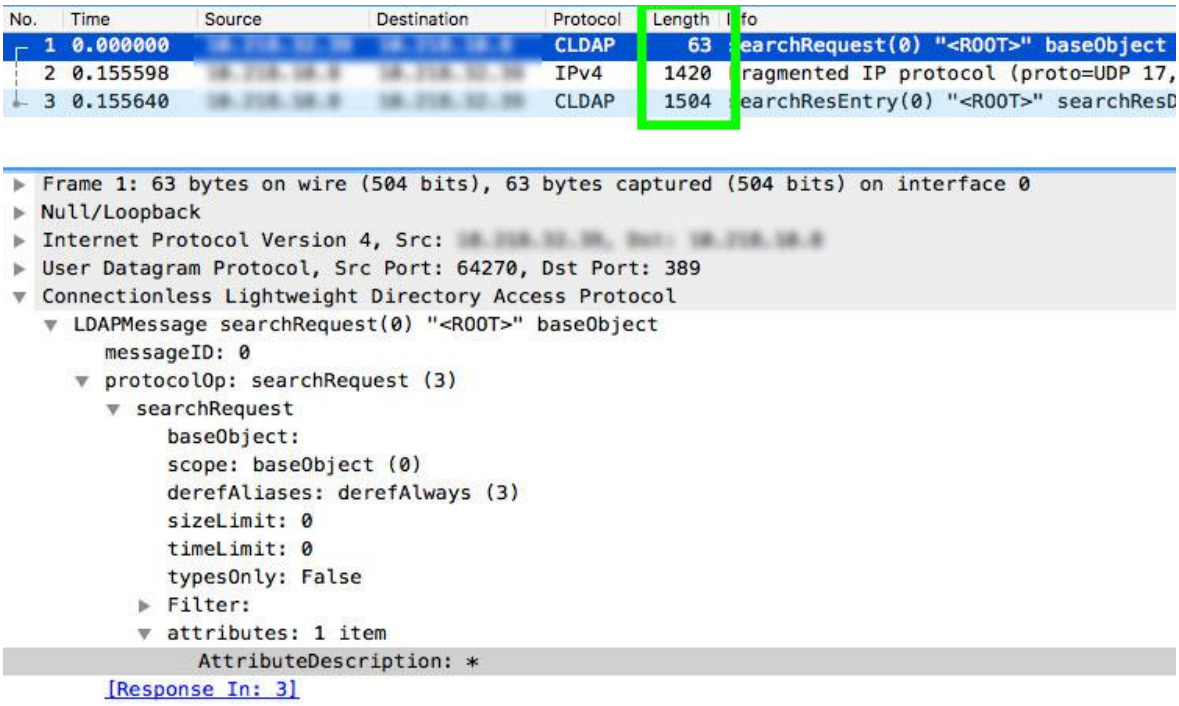
همانطور که در شکل ۹ دیده می‌شود، اندازه پاسخ فقط ۰,۷۵ بزرگتر از اندازه درخواست است و این اندازه تقویت برای یک مهاجم DDoS، ارزش لازم را ندارد. بنابراین باید ببینیم چگونه می‌توان فاکتور تقویت را افزایش داد.

در این مرحله، سعی می‌کنیم ویژگی هایی از Netlogon را به دست آوریم که می‌توانند بدون احراز هویت از یک سرور LDAP درخواست شوند. برای این منظور، به سایت مایکروسافت و لیست ویژگی‌های rootDSE موجود برای پرس‌وجو نگاه می‌کنیم. پر کردن تمام این صفات در اسکریپت AD Ping نمونه سامبا کمی کار می‌برد، اما بعد از مدتی با گرفتن و ضبط بسته پاسخ، به نتیجه نشان داده شده در شکل ۱۰ می‌رسیم:




**شکل ۱۰: نتیجه ضبط پاسخ برای درخواست فرستاده شده حاوی ویژگی‌های Netlogon**

در این حالت به پاسخی با اندازه ۵,۵ برابر بسته درخواست رسیدیم. حال سعی می‌کنیم اندازه بسته درخواست را کاهش دهیم تا فاکتور تقویت بزرگتر شود. برای این کار به‌جای نشان دادن بیست و دو ویژگی ممکن LDAP در درخواست، از * استفاده می‌کنیم.




**شکل ۱۱: نتیجه ضبط بسته پاسخ پس از کاهش اندازه بسته درخواست**

همانطور که در شکل ۱۱ مشاهده می‌شود، توانستیم تنها با ۶۳ بایت از بسته درخواست، بسته پاسخ با اندازه قبلی را دریافت کنیم. اکنون یک فاکتور تقویت کننده ۴۶ برابری ایجاد کرده ایم! حال کافی است نتیجه فوق را به عنوان گزینه‌ای برای آزمایش ابزارهای مقابله با DDoS معرفی کنیم.

## ۷ اقدامات جهت کاهش شدت آسیب‌پذیری

ساده ترین راه برای حل این مسئله، این است که فایروال را بر روی سرور خود فعال کنید تا دسترسی به پورت LDAP ۳۸۹ را از طریق UDP مسدود کند. LDAP اغلب در سرورهای ویندوز با استفاده از سرویس‌های Active directory مورد استفاده قرار می‌گیرد. اگر برنامه ای دارید که از طریق UDP از سرویس LDAP سرور دیگر استفاده می‌کند، باید یک استثناء در فایروال قرار دهید که به این برنامه اجازه ادامه کارش را بدهد یا آن برنامه را طوری تغییر دهید که از طریق TCP از LDAP استفاده کند. LDAP همچنین می‌تواند با رمزنگاری (LDAPS) روی پورت ۶۳۶ اجرا شود، اما این پروتکل تنها توسط TCP پشتیبانی می‌شود.

برای غیرفعال کردن دسترسی به LDAP از طریق UDP، در صورتی که سروری نداشته باشید که به این سرویس دسترسی داشته باشد، این مراحل را دنبال کنید:

۱. بر روی start راست کلیک کنید، سپس روی Run کلیک کرده و "wf.msc" را تایپ کرده و OK را بزنید.
۲. روی گزینه "Inbound Rules" در سمت چپ پنجره کلیک کنید.
۳. قاعده "Active Directory Domain Controller - LDAP (UDP-In)" را تعیین کنید.
۴. روی قاعده کلیک راست کرده و گزینه "Disable Rule" را انتخاب کنید.

اگر نیاز می‌دانید که دسترسی به LDAP از سرورهای دیگر را مجاز کنید، این مراحل را دنبال کنید:

۱. بر روی start راست کلیک کنید، سپس روی Run کلیک کرده و "wf.msc" را تایپ کرده و OK را بزنید.
۲. روی گزینه "Inbound Rules" در سمت چپ پنجره کلیک کنید.
۳. قاعده "Active Directory Domain Controller - LDAP (UDP-In)" را تعیین کنید.
۴. روی قانون کلیک راست کرده و Properties را انتخاب کنید.
۵. روی زبانه "Scope" کلیک کنید.
۶. در قسمت "Remote IP address" گزینه "These IP addresses:" را انتخاب کنید.
۷. برای هر آدرس یا محدوده IP که باید دسترسی داشته باشند، روی «Add…» کلیک کنید و محدوده های درست را وارد کنید.
۸. پس از وارد کردن تمام محدوده هایی که باید دسترسی داشته باشند، برای حفظ این قانون، روی OK کلیک کنید.

اگر می‌خواهید LDAP را بر روی TCP یا سرویس LDAP امن را به دلایل امنیتی محدود کنید، ممکن است بخواهید این قواعد را با استفاده از مراحلی مشابه مراحل بالا تغییر دهید:

- Active Directory Domain Controller - LDAP (TCP-In)
- Active Directory Domain Controller - Secure LDAP (TCP-In)

اگر شما سرویس LDAP را در لینوکس اجرا می‌کنید، باید تنظیمات سرور LDAP خود را مطابق با مستندات آن تغییر دهید تا LDAP را از طریق UDP غیرفعال یا محدود سازید، یا فایروال سیستم خود را پیکربندی کنید.

## ۸ جمع بندی و نتیجه‌گیری

اخیرا شاهد افزایش قابل توجهی در گزارشات حملات تقویتی که از پروتکل LDAP بر روی UDP استفاده می‌کنند، بوده‌ایم. این حمله درخواستی را به سرورهای LDAP با استفاده از آدرس منبع جعلی ارسال می‌کند. این درخواست باعث می‌شود که پاسخ به آدرس جعلی برگردد و در نتیجه مقدار زیادی داده به رایانه‌ای که آن را درخواست نکرده، ارسال می‌شود. این اثر، زمانی که با هزاران سرور LDAP مورد استفاده قرار گیرد، مقدار بسیار زیادی از ترافیک را روی یک IP سبب می‌شود و یک حمله توزیع شده موثر روی هدف انجام می‌دهد.

اکثر سرورها و مشتریان LDAP از پروتکل TCP استفاده می‌کنند که به دلیل برقراری ارتباط سه مرحله‌ای در پروتکل TCP که ابتدا منبع را تأیید می‌کند و سپس منبع و مقصد می‌توانند با یکدیگر ارتباط برقرار کنند، مانع تقویت می‌شود. UDP این تأیید را انجام نمی‌دهد، بنابراین سرور LDAP می‌تواند ترافیک را به مقصدی که تأیید نشده، ارسال کند.

حملات بازتاب مبتنی بر UDP به طور مداوم شامل بیش از ۵۰ درصد از همه حملات است. با بردارهای حمله جدید که به طور مرتب کشف می‌شوند و بسیاری از آنها سال‌ها ادامه پیدا می‌کنند، این مشکل به زودی قابل حل نخواهد بود. راه‌حل‌های اصلی برای پیشگیری از این حمله از طریق پروتکل CLDAP، مسدود کردن دسترسی غیر ضروری به این سرویس بر روی اینترنت توسط سرویس دهنده است.

## ۹ منابع

[1] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/CLDAP-threat-advisory.pdf

[2]https://www.plixer.com/blog/network-security/how-to-monitor-CLDAP-traffic-with-netflow/

[3]https://support.steadfast.net/Knowledgebase/Article/View/119/0/preventing-LDAP-amplification-attacks

[4]https://www.bleepingcomputer.com/news/security/cldap-protocol-allows-ddos-attacks-with-70x-amplification-factor/

[5] https://www.senki.org/cldap-reflection-attack-are-increasing/

[6]https://www.ixiacom.com/company/blog/following-crumbs-deconstructing-cldap-ddos-reflection-attack