باسمه تعالی

حملات تقویت شده DDOS از طریق سوءاستفاده از پروتکل LDAP

مقدمه

LDAP یک پروتکل لایه کاربرد است که برای دسترسی به سرویس دایرکتوری در شبکه مورد استفاده قرار گرفته و امکان دسترسی و جستجو در فهرست اطلاعات کاربران، سیستم‌ها، شبکه‌ها، سرویس‌ها و برنامه‌های کاربردی را میسر می‌سازد. این پروتکل به‌طور پیش فرض از شماره پورت ۳۸۹ پروتکل‌های TCP و UDP استفاده می‌کند. این پروتکل در صورت تنظیم نامناسب و در نظر نگرفتن ملاحظات امنیتی می‌تواند مورد سوء استفاده قرار گرفته و در حمله DDOS شرکت داده شود. OPEN-LDAP یک نرم‌افزار آزاد و منبع باز است که پروتکل LDAP[1] را پیاده‌سازی کرده است و نسخه‌های گوناگون آن در سیستم‌عامل‌های مختلف مورد استفاده قرار می‌گیرد. در این مستند نگاهی کوتاه به حمله LDAP reflection-amplification DDoS شده و ملاحظاتی به منظور امن‌سازی آن بیان می‌گردد.

LDAP reflection-amplification DDoS

استفاده از روش تقویت ترافیک (Amplification)، شیوه‌ای برای اجرای حمله DDOS می‌باشد. اساس این روش، ارسال یک درخواست با طول کم به یک سرویس‌دهنده آسیب‌پذیر و دریافت پاسخ با طول زیاد می‌باشد. حمله‌کننده با قرار دادن آدرس IP جعلی فرد قربانی و ارسال درخواست‌های متوالی با طول کم به یک و یا چندین سرور موجب ارسال حجم زیادی ترافیک به سمت قربانی می‌شود. نکته کلیدی، طول پاسخ بازگردانده شده از سوی سرور می‌باشد. هرچه اندازه پاسخ نسبت به درخواست ارسال شده بیشتر باشد، ترافیک نهایی به سمت قربانی نیز بیشتر می‌شود.

به عبارتی دیگر، در برخی از پروتکل‌ها همچون پروتکل LDAP، ارسال یک درخواست کم حجم مناسب که آدرس IP فرد قربانی به جای آدرس مبداء قرار گرفته است، می‌تواند یک پاسخ خروجی که اندازه آن بسیار بزرگتر از درخواست اولیه می‌باشد را تولید کند. این ترافیک تقویت شده می‌تواند به دفعات برای فرد قربانی ارسال شود. نسبت حجم ترافیک دریافتی توسط فرد قربانی به ترافیک ارسالی فرد حمله‌کننده به عنوان شاخص تقویت حملات انعکاس DDoS[2] شناخته می‌شود. برای پروتکل LDAP معمولاً این مقدار بیش از ۴۵ بوده که رقمی بسیار قابل توجه است.

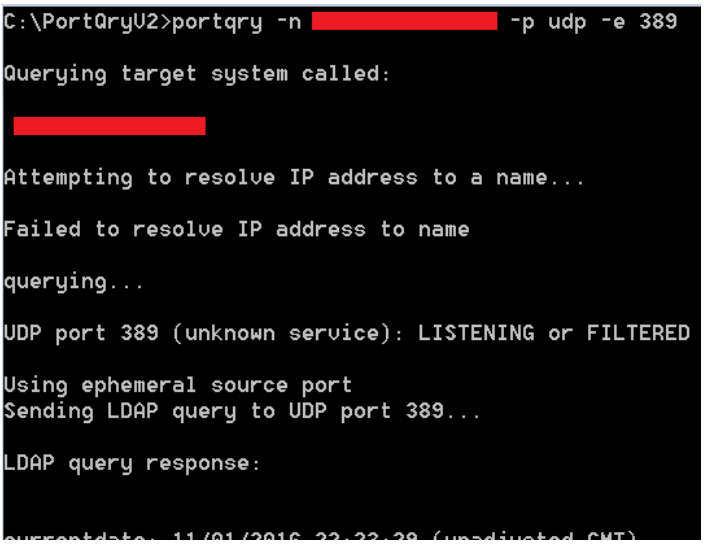
---

[1] Lightweight Directory Access Protocol
[2] reflection DDoS attack's amplification factor

درنتیجه برای سوءاستفاده از این آسیب‌پذیری، کافی است فرد مهاجم فهرستی از آدرس‌های IP قابل دسترس از طریق شبکه اینترنت که سرویس LDAP بر روی آن‌ها فعال است را یافته و به روش فوق از آن‌ها سوءاستفاده نماید (به خاطر ماهیت بدون اتصال بودن ارتباطات UDP، معمولاً به دنبال یافتن پورت‌های UDP/389 هستند).

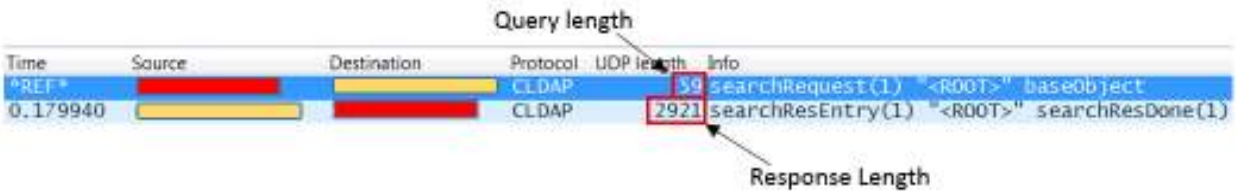
فاکتور تقویت در حملات Amplification

فاکتور تقویت به میزان کارآمدی حمله و مقدار داده‌ای اشاره دارد که به سمت هدف ارسال می‌شود. این فاکتور با تقسیم طول پاسخ سرور LDAP به طول درخواست مهاجم محاسبه می‌شود. می‌توان با استفاده از اسکنر پورت PortQry کوئری LDAP روی UDP تولید کرد (شکل ۱).



شکل ۱ . تولید کوئری درخواست LDAP

سپس می‌توان با استفاده از وایرشارک طول کوئری پاسخ را محاسبه کرد (شکل ۲).



شکل ۲ . دریافت کوئری پاسخ

در مثال نوعی فوق مشاهده می‌شود که طول پاسخ ۲۹۲۱ بایت و سایز کوئری ارسالی ۵۹ بایت است، بنابراین فاکتور تقویت ۴۹ است. این تست نشان می‌دهد که LDAP amplification attack می‌تواند به‌اندازه‌ی DNS amplification attack قوی و مخرب باشد.

در جدول زیر، فاکتور تقویت تعدادی از پروتکل‌های آسیب‌پذیر جهت مقایسه آورده شده است.

پروتکل	فاکتور تقویت
NTP	556.9
CharGEN	358.8
QOTD	140.3
RIPv1	131.24
Quake Network Protocol	63.9
LDAP	**46-55**
DNS	28-54
SSDP	30.8
Portman (RCPhind)	7-28
Kad	16.3
Multicast DNS (mDNS)	2-10
SNMPv2	6.3
Stream Protocol	5.5
NetBIOS	3.8
BitTorrent	3.8

بررسی‌های انجام گرفته توسط مرکز ماهر نشان می‌دهد که سرویس LDAP بر روی تعدادی از آدرس‌های IP قابل دسترس از طریق اینترنت آن مجموعه فعال است (لیست پیوست). اکیداً توصیه می‌گردد که راهبران شبکه مطمئن شوند که بر روی هیچ یک از آدرس‌های Valid IP تحت کنترل آن‌ها، سرویس LDAP قابل دسترس

نمی‌باشد (بایستی دسترسی به پورت tcp/udp 389 کلیه ماشین‌ها محدود به آدرس‌های IP مجاز شده و سایر ترافیک‌ها به سمت این پورت بر روی فایروال مسدود گردد). درصورت لزوم فعال بودن LDAP بر روی برخی از آدرس‌های Valid IP، به‌روزرسانی ماشین سرویس‌دهنده و هچنین امن‌سازی سرویس (به عنوان مثال، مطابق با موارد مطرح شده در آدرس https://www.openldap.org/doc/admin24/security.html) الزامی است.