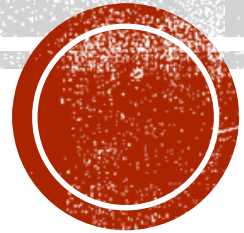
CLDAP 反射攻擊



ASOC

童鵬哲

389 PORT (CLDAP、LDAP)

- LDAP (Lightweight Directory Access Protocol) 為AD上利用 TCP 389 PORT進行傳輸的協定。

- CLDAP (Connection-less Lightweight Directory Access Protocol)為AD上利用 UDP 389 PORT 進行傳輸的協定。

- Windows AD 的rootDSE，預設情況下是不需要權限，即可存取。

CLDAP 服務主機(攻擊協助者)

- 不少北區ASOC轄下學校，皆加入DDOS攻擊的清單。

學校IP	學校名稱		服務PORT	
)1.197.2	宜蘭	學(12	389	LDAP
1.130.1	宜蘭	民小	389	LDAP
1.159.6	宜蘭	民小	389	LDAP
4.67.76	國立	.4.0.0	19	Chargen Service
4.67.77	國立	.4.0.0	0	
4.71.159	國立	.4.0.0	389	LDAP
2.184.165	國立	40.12	389	LDAP
6.120.68	私立	6.12(	389	LDAP
2.16.100	國立	63.22	389	LDAP
2.21.127	國立	63.22	389	LDAP
2.6.1	國立	63.22	389	LDAP
).0.163	桃園	(163.	389	LDAP
).112.2	桃園	民小	389	LDAP
2.135.200	臺北	農職	389	LDAP
.3.13	國立	業學	389	LDAP
40.62.130	花蓮	民小	389	LDAP
40.62.132	花蓮	民小	0	
43.8.200	臺北	學(21(	389	LDAP
).7.119	財團	高級	389	LDAP
).7.2	財團	高級	389	LDAP
).55.111	玄奘	)-210.	389	LDAP

透過SHODAN

View Raw Data

self-signed

City	Taipei
Country	Taiwan
Organization	Taiwan Academic Network
ISP	Taiwan Academic Network (TANet) Information Center
Last Update	2018-07-29T23:54:07.000192
ASN	AS18047

Web Technologies

- Bootstrap
- Chart.js
- FlexSlider

Ports

53 80 88 123 389 443 636 5985

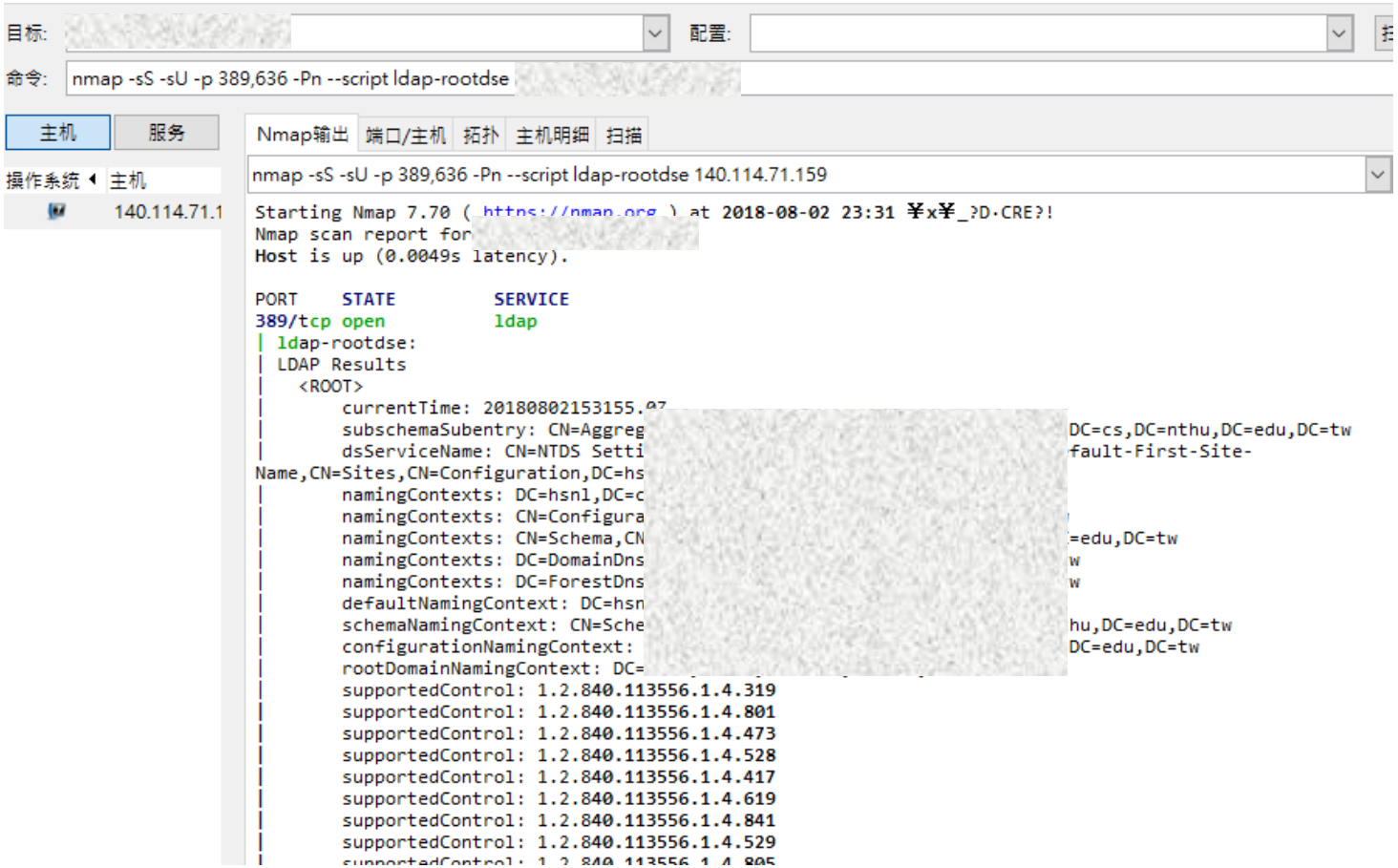
Services

80
tcp
http

Microsoft IIS httpd Version: 7.5

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 09 Apr 2014 13:10:57 GMT
Accept-Ranges: bytes
ETag: "96982425f553cf1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Thu, 19 Jul 2018 11:29:42 GMT
Content-Length: 34823
```

利用NMAP進行查詢


目标:
配置:
命令: nmap -sS -sU -p 389,636 -Pn --script ldap-rootdse
主机
服务
操作系统
主机
140.114.71.1
Nmap输出
端口/主机
拓扑
主机明细
扫描
nmap -sS -sU -p 389,636 -Pn --script ldap-rootdse 140.114.71.159
Starting Nmap 7.70 (https://nmap.org) at 2018-08-02 23:31 ¥x¥_?D·CRE?!
Nmap scan report for
Host is up (0.0049s latency).
PORT STATE SERVICE
389/tcp open ldap
| ldap-rootdse:
| LDAP Results
| <ROOT>
| currentTime: 20180802153155.0Z
| subschemaSubentry: CN=Aggreg DC=cs,DC=nthu,DC=edu,DC=tw
| dsServiceName: CN=NTDS Setti fault-First-Site-
Name,CN=Sites,CN=Configuration,DC=hs
| namingContexts: DC=hsn1,DC=c
| namingContexts: CN=Configura
| namingContexts: CN=Schema,CN =edu,DC=tw
| namingContexts: DC=DomainDns w
| namingContexts: DC=ForestDns w
| defaultNamingContext: DC=hsn
| schemaNamingContext: CN=Sche hu,DC=edu,DC=tw
| configurationNamingContext: DC=edu,DC=tw
| rootDomainNamingContext: DC=
| supportedControl: 1.2.840.113556.1.4.319
| supportedControl: 1.2.840.113556.1.4.801
| supportedControl: 1.2.840.113556.1.4.473
| supportedControl: 1.2.840.113556.1.4.528
| supportedControl: 1.2.840.113556.1.4.417
| supportedControl: 1.2.840.113556.1.4.619
| supportedControl: 1.2.840.113556.1.4.841
| supportedControl: 1.2.840.113556.1.4.529

CLDAP攻擊封包

不到100 bytes的封包，可以造成3000 bytes的回應封包，放大率大於30倍。

69336	2018-04-11 14:58:14.983375		59.126.5.132	1		182.51	IPv4	1506 F
69337	2018-04-11 14:58:14.983377	1221	59.126.5.132	389	1	182.51	3779 CLDAP	60 s
69338	2018-04-11 14:58:14.983484		61.216.151.118	1		182.51	IPv4	1514 F
69339	2018-04-11 14:58:14.983486	1088	61.216.151.118	389	1	182.51	33951 CLDAP	1071 s
69340	2018-04-11 14:58:14.983488		61.218.81.226	1		182.51	IPv4	1514 F
69341	2018-04-11 14:58:14.983490	927	61.218.81.226	389	1	182.51	39743 CLDAP	1021 s
69342	2018-04-11 14:58:14.983492		60.250.121.199	1		182.51	IPv4	1143 F
69343	2018-04-11 14:58:14.983537		59.124.239.20	1		182.51	IPv4	1514 F

```
Source: 59.126.5.132
Destination:
[3 IPv4 Fragments (2966 bytes): #69333(1472), #69336(1472), #69337(22)]
   [Frame: 69333, payload: 0-1471 (1472 bytes)]
   [Frame: 69336, payload: 1472-2943 (1472 bytes)]
   [Frame: 69337, payload: 2944-2965 (22 bytes)]
   [Fragment count: 3]
   [Reassembled IPv4 length: 2966]
   [Reassembled IPv4 data: 01850ec30b966ef5308400000b72020101648400000b6904...]
```

預防

- 使用者可架設防火牆進行ACL的控管
- AD 應盡量避免暴露於Internet
- 於設定檔中關閉**Anonymous Access**