BÁO CÁO

Dò quét thông tin lỗ hổng bảo mật hệ thông

THEO HỒ SƠ

I Thông tin về dò quét

1.1 Thông tin tiến trình dò quét

1.1.1 Lần quét 1

_id	Name	Target	Date_Create	Date_Stop	Status
614993f0f2ecf62470b071af	test_running	192.168.133.181	21/09/2021T15:12:32	21/09/2021T15:18:16	StatusSuccess
61494be0b3cfb4d777eb9576	test_running	192.168.133.198	21/09/2021T10:05:04	21/09/2021T10:05:30	StatusSuccess

1.2 Thông tin đối tượng dò quét

1.2.1 IP

TT	IN_IP
1	192.168.133.181

1.2.2 DOMAIN

TT	IN_DOMAIN
1	http://WIN-BT5LUHIQRIP

1.2.3 DESCRIBE

TT	IN_DESCRIBE
1	windows server - exchange

1.2.4 NAME

TT	IN_NAME
1	windows-server-old

1.2.5 AUTHEN

<table>
<tr><th>TT</th><th>IN_AUTHEN</th></tr>
<tr><td>1</td><td><table><tr><td><b>username</b></td><td></td></tr><tr><td><b>password</b></td><td></td></tr></table></td></tr>
</table>

II Thu thập, dò quét thông tin

2.1 SERVICES

TT	name	product	version	port	protocol
1	smtp	Microsoft Exchange smtpd	0	25	tcp
2	domain	Simple DNS Plus	0	53	tcp
3	http	Microsoft IIS httpd	10.0	80	tcp
4	http	Microsoft IIS httpd	10.0	81	tcp
5	kerberos-sec	Microsoft Windows Kerberos	0	88	tcp
6	msrpc	Microsoft Windows RPC	0	135	tcp
7	netbios-ssn	Microsoft Windows netbios-ssn	0	139	tcp
8	ldap	Microsoft Windows Active Directory LDAP	0	389	tcp
9	http	Microsoft IIS httpd	10.0	443	tcp
10	http	Microsoft IIS httpd	10.0	444	tcp
11	microsoft-ds	0	0	445	tcp
12	kpasswd5	0	0	464	tcp
13	smtp	Microsoft Exchange smtpd	0	465	tcp
14	smtp	0	0	475	tcp
15	smtp	0	0	476	tcp
16	smtp	0	0	477	tcp
17	smtp	Microsoft Exchange smtpd	0	587	tcp
18	ncacn_http	Microsoft Windows RPC over HTTP	1.0	593	tcp
19	ldap	Microsoft Windows Active Directory LDAP	0	636	tcp
20	smtp	Microsoft Exchange smtpd	0	717	tcp
21	ccproxy-http	0	0	808	tcp
22	mc-nmf	.NET Message Framing	0	890	tcp
23	msmq	0	0	1801	tcp
24	msrpc	Microsoft Windows RPC	0	2103	tcp
25	msrpc	Microsoft Windows RPC	0	2105	tcp
26	msrpc	Microsoft Windows RPC	0	2107	tcp
27	smtp	Microsoft Exchange smtpd	0	2525	tcp
28	ldap	Microsoft Windows Active Directory LDAP	0	3268	tcp
29	ldap	Microsoft Windows Active Directory LDAP	0	3269	tcp
30	http	Microsoft HTTPAPI httpd	2.0	3800	tcp
31	mc-nmf	.NET Message Framing	0	3801	tcp
32	mc-nmf	.NET Message Framing	0	3803	tcp
33	mc-nmf	.NET Message Framing	0	3823	tcp
34	mc-nmf	.NET Message Framing	0	3828	tcp
35	mc-nmf	.NET Message Framing	0	3843	tcp
36	mc-nmf	.NET Message Framing	0	3863	tcp
37	mc-nmf	.NET Message Framing	0	3867	tcp
38	msexchange-logcopier	Microsoft Exchange 2010 log copier	0	3875	tcp
39	http	Microsoft HTTPAPI httpd	2.0	5985	tcp
40	ncacn_http	Microsoft Windows RPC over HTTP	1.0	6001	tcp
41	msrpc	Microsoft Windows RPC	0	6400	tcp
42	msrpc	Microsoft Windows RPC	0	6401	tcp
43	msrpc	Microsoft Windows RPC	0	6402	tcp
44	msrpc	Microsoft Windows RPC	0	6403	tcp
45	ncacn_http	Microsoft Windows RPC over HTTP	1.0	6405	tcp
46	msrpc	Microsoft Windows RPC	0	6406	tcp
47	msrpc	Microsoft Windows RPC	0	6408	tcp
48	msrpc	Microsoft Windows RPC	0	6411	tcp
49	msrpc	Microsoft Windows RPC	0	6421	tcp
50	msrpc	Microsoft Windows RPC	0	6457	tcp
51	msrpc	Microsoft Windows RPC	0	6475	tcp
52	msrpc	Microsoft Windows RPC	0	6482	tcp
53	msrpc	Microsoft Windows RPC	0	6527	tcp
54	msrpc	Microsoft Windows RPC	0	6536	tcp
55	msrpc	Microsoft Windows RPC	0	6537	tcp
56	msrpc	Microsoft Windows RPC	0	6539	tcp
57	msrpc	Microsoft Windows RPC	0	6544	tcp
58	msrpc	Microsoft Windows RPC	0	6547	tcp
59	msrpc	Microsoft Windows RPC	0	6548	tcp
60	msrpc	Microsoft Windows RPC	0	6550	tcp
61	msrpc	Microsoft Windows RPC	0	6552	tcp
62	msrpc	Microsoft Windows RPC	0	6558	tcp
63	msrpc	Microsoft Windows RPC	0	6559	tcp
64	msrpc	Microsoft Windows RPC	0	6582	tcp

TT	name	product	version	port	protocol
65	msrpc	Microsoft Windows RPC	0	6600	tcp
66	msrpc	Microsoft Windows RPC	0	6603	tcp
67	msrpc	Microsoft Windows RPC	0	6619	tcp
68	msrpc	Microsoft Windows RPC	0	6626	tcp
69	msrpc	Microsoft Windows RPC	0	6692	tcp
70	msrpc	Microsoft Windows RPC	0	6707	tcp
71	msrpc	Microsoft Windows RPC	0	6760	tcp
72	msrpc	Microsoft Windows RPC	0	6763	tcp
73	msrpc	Microsoft Windows RPC	0	6766	tcp
74	msrpc	Microsoft Windows RPC	0	6780	tcp
75	msrpc	Microsoft Windows RPC	0	6789	tcp
76	msrpc	Microsoft Windows RPC	0	6792	tcp
77	msrpc	Microsoft Windows RPC	0	6795	tcp
78	msrpc	Microsoft Windows RPC	0	6833	tcp
79	msrpc	Microsoft Windows RPC	0	6841	tcp
80	msrpc	Microsoft Windows RPC	0	6855	tcp
81	msrpc	Microsoft Windows RPC	0	6939	tcp
82	msrpc	Microsoft Windows RPC	0	6947	tcp
83	msrpc	Microsoft Windows RPC	0	6967	tcp
84	http	Microsoft IIS httpd	10.0	8172	tcp
85	mc-nmf	.NET Message Framing	0	9389	tcp
86	mc-nmf	.NET Message Framing	0	9710	tcp
87	msrpc	Microsoft Windows RPC	0	11183	tcp
88	msrpc	Microsoft Windows RPC	0	11187	tcp
89	msrpc	Microsoft Windows RPC	0	11204	tcp
90	msrpc	Microsoft Windows RPC	0	17705	tcp
91	msrpc	Microsoft Windows RPC	0	17785	tcp
92	http	Microsoft HTTPAPI httpd	2.0	47001	tcp
93	msexchange-logcopier	Microsoft Exchange 2010 log copier	0	64327	tcp
94	mc-nmf	.NET Message Framing	0	64337	tcp

2.2 PORTS

TT	RECON_PORTS
1	25
2	53
3	80
4	81
5	88
6	135
7	139
8	389
9	443
10	444
11	445
12	464
13	465
14	475
15	476
16	477
17	587
18	593
19	636
20	717
21	808
22	890
23	1801
24	2103
25	2105
26	2107
27	2525
28	3268
29	3269
30	3800
31	3801
32	3803
33	3823

TT	RECON_PORTS
34	3828
35	3843
36	3863
37	3867
38	3875
39	5985
40	6001
41	6400
42	6401
43	6402
44	6403
45	6405
46	6406
47	6408
48	6411
49	6421
50	6457
51	6475
52	6482
53	6527
54	6536
55	6537
56	6539
57	6544
58	6547
59	6548
60	6550
61	6552
62	6558
63	6559
64	6582
65	6600
66	6603
67	6619
68	6626
69	6692
70	6707
71	6760
72	6763
73	6766
74	6780
75	6789
76	6792
77	6795
78	6833
79	6841
80	6855
81	6939
82	6947
83	6967
84	8172
85	9389
86	9710
87	11183
88	11187
89	11204
90	17705
91	17785
92	47001
93	64327
94	64337

2.3 OS

TT	RECON_OS
1	windows
2	linux

2.4 WEBAPP

TT	RECON_WEBAPP
1	http://192.168.133.181:80
2	http://192.168.133.181:81
3	http://192.168.133.181:3800
4	http://192.168.133.181:5985
5	http://192.168.133.181:47001
6	https://192.168.133.181:443
7	https://192.168.133.181:444
8	https://192.168.133.181:8172

III Thông tin lỗ hổng bảo mật

3.1 POCS

<table>
<tr><th>TT</th><th>result</th><th>app_name</th><th>created</th></tr>
<tr><td>1</td><td><table><tr><td><b>ShellInfo</b></td><td><table>
<tr><td><b>url</b></td><td>https://192.168.133.181:443</td></tr>
<tr><td><b>email</b></td><td>Administrator@demo.local</td></tr>
<tr><td><b>shell</b></td><td>https://192.168.133.181:443/aspnet_client/ulcmzutebcvemlqu.aspx</td></tr>
<tr><td><b>info</b></td><td>proxyshell RCE</td></tr>
</table></td></tr></table></td><td>exchange-proxyshell-cve-2021-34473</td><td>2021-09-21 16:01:14</td></tr>
<tr><td>2</td><td><table><tr><td><b>ShellInfo</b></td><td><table>
<tr><td><b>dc_name</b></td><td>WIN-BT5LUHIQRIP</td></tr>
<tr><td><b>dc_ip</b></td><td>192.168.133.181</td></tr>
<tr><td><b>username</b></td><td>Administrator</td></tr>
<tr><td><b>password</b></td><td>aad3b435b51404eeaad3b435b51404ee:
714ae77627375ec5b7a997f7567dd415</td></tr>
<tr><td><b>url</b></td><td>• 192.168.133.181</td></tr>
</table></td></tr></table></td><td>windows-cve-2020-1472</td><td>2021-09-21 16:01:32</td></tr>
</table>

IV Lịch sử khai thác lỗ hổng