candor PROTECT

Penetration Test
Detailed Report

Jun. 30, 2022 | Candor Protect: Sample Black Box Penetration Test

Candor Protect automated penetration test report summarizes the vulnerabilities, exploit achievements and remediation action items recommended in your network based on the latest ethical hacking pen-testing techniques

Candor provides the Candor Protect™ service and report "As Is", without any warranty of any kind. Candor makes no warranty that the information contained in this report is complete or error - free.

Table Of Contents

Detailed Report

Appendix

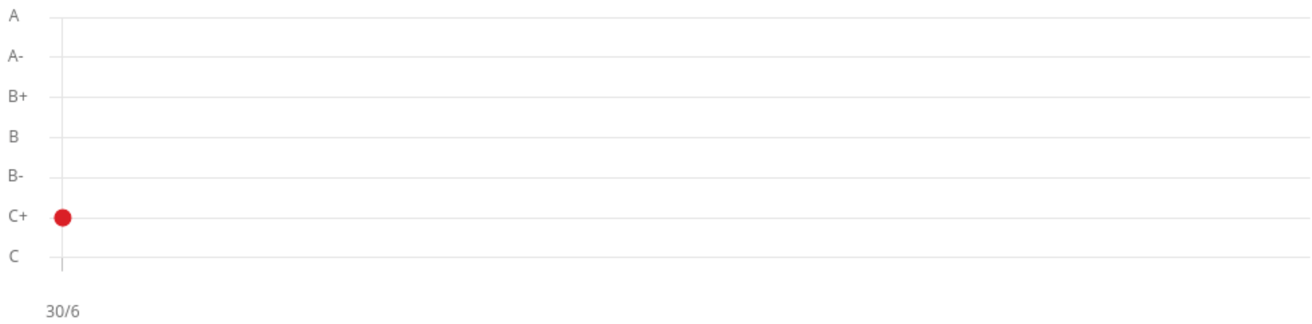
Executive Summary

✓ Completed successfully

Cyber Resilience Score & Settings

Name:	**Candor Protect: Client Demo**
Description:	Simulated Black Box Senario
Type:	**Penetration Testing (Black Box)**
Time & Duration:	Jun 30 2022 14:23 - Jun 30 2022 16:24, 02:00
Included IP Range(s):	**192.168.4.1 - 192.168.4.254, 192....** 3 Ranges
Action Approval Score:	64 / 69 - 92%
User Input:	**1 - IP Range(s)**

Resilience Score Over Last 1 Tasks



Resilience Score Card

Critical Assets	No critical assets are defined in Candor	
Credentials and Account Takeover	Gained access to 2 accounts: 2 Domain user(s)	Critical
Sniffing	Sniffed 3 credentials and performed 2 relay attacks	High
Password Strength	Cracked 102 out of 104 passwords: 102 easy	Critical
Lateral Movement	Congratulations! Candor wasn't able to perform lateral movement in your network	
Accessible Data	Gained access to 2 Hosts (with complete access)	Critical
Host Takeover	Candor was able to 'take over'[1] 2 out of 32 hosts (6%): 1 Windows Workstation(s) and 1 Windows Server(s)	Critical
AV/EDR Bypass	Congratulations! Candor wasn't able to bypass your Antivirus/EDR solutions	Critical

69 Total Action Approvals

● 64 Approved (93%) ● 5 Not Approved (7%)

883 Total Actions

● 390 Successful (45%) ● 493 No-results (55%)

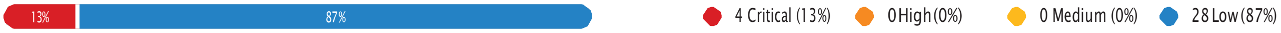
[1] Gain complete access to a host's hardware, software and files.

Host Findings

32 Discovered Hosts

Candor identified 32 live hosts across 5 device categories, 4 were affected by critical vulnerabilities

Vulnerability Severity Distribution

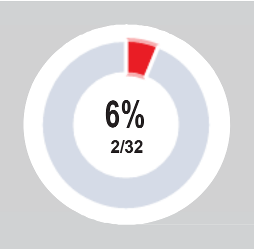


8	2	1	20	0	1
Windows Workstation	Windows Server	Windows	Linux	Network Devices	Other

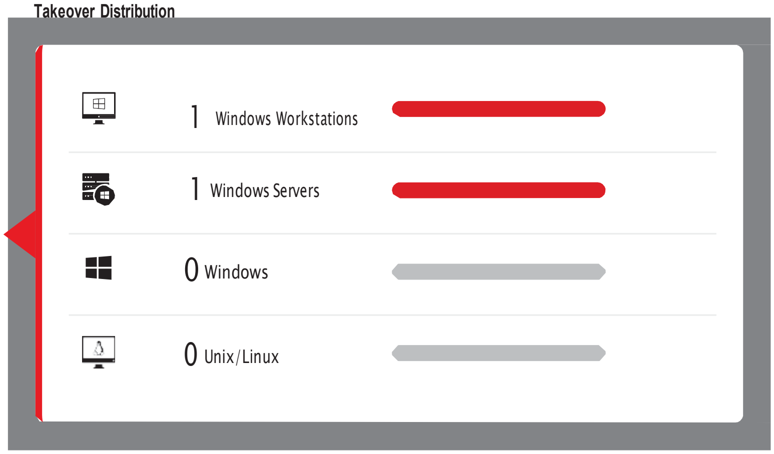
6% Host Takeover[1]

Out of 32 live hosts, Candor took over 2 hosts

Takeover Percentage



Takeover Distribution



[1] Host Takeover refers to the state when an attacker achieves complete control of a remote host's operating system, installed software, hardware and files

Live Hosts Table

(Listing 32 of 32 hosts).

Host	OS Version	Takeover	Details
TECH-PC.CLIENT.CORP **00:15:5D:05:0A:0C** **Microsoft**	**Win7 (D)**		Domain/Workgroup: CLIENT.CORP
DABOSS-PC.CLIENT.CORP **00:15:5D:05:0A:06** **Microsoft**	**Win7 (D)**		Domain/Workgroup: CLIENT.CORP
STAFF-01.CLIENT.CORP **00:15:5D:05:0A:0B** **Microsoft**	**Win7 (D)**	▲	Logged on user(s): User: administrator Domain/Workgroup: CLIENT.CORP
CLIENT-SVR-2012.CLIENT.CORP **00:15:5D:05:0A:08** **Microsoft**	**Win2012R2 (D) Server**	▲	Domain/Workgroup: CLIENT.CORP
_gateway			

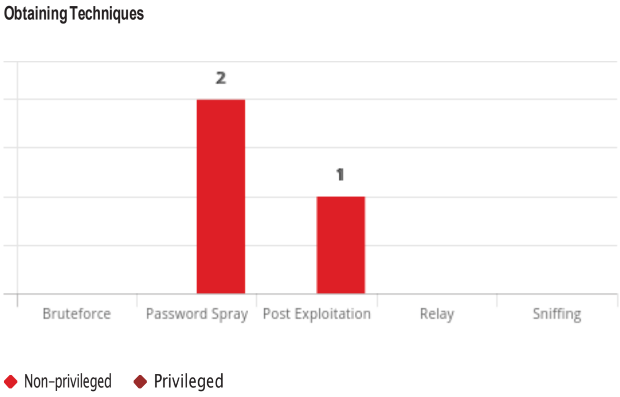
192.168.4.7	🖥	**Linux**	
192.168.4.8	🖥	**Linux**	
192.168.4.29	🖥	**Linux**	
192.168.4.18	🖥	**Linux**	
192.168.4.19	🖥	**Linux**	
192.168.4.3	🖥	**Linux**	
192.168.4.4	🖥	**Linux**	
ACCOUNTING-PC.CLIENT.CORP **00:15:5D:05:0A:09** **Microsoft**	🖥	**Win10 (D)**	Domain/Workgroup: CLIENT.CORP
192.168.4.16	🖥	**Linux**	
DESKTOP-KK865F1	🖥	**Win10**	Domain/Workgroup: DESKTOP-KK865F1
192.168.4.17	🖥	**Linux**	
192.168.4.14	🖥	**Linux**	
192.168.4.9	🖥	**Linux**	
CAN-DEMO-HV **B8:CA:3A:92:C5:33** **Dell**	🖥	**Win10**	Domain/Workgroup: CAN-DEMO-HV
CLIENT-SVR-WIN2022.CLIENT.CORP **00:15:5D:05:0A:0D** **Microsoft**	🗄	**Win10 (D) Server**	Domain/Workgroup: CLIENT.CORP
192.168.4.41	🖥	**Linux**	
192.168.4.53	🖥	**Linux**	
192.168.4.5	🖥	**Linux**	
192.168.4.6	🖥	**Linux**	
192.168.4.1	🖥	**Linux**	
DESKTOP-QU21GJG	🖥	**Win10**	Domain/Workgroup: DESKTOP-QU21GJG
192.168.4.12	🖥	**Linux**	

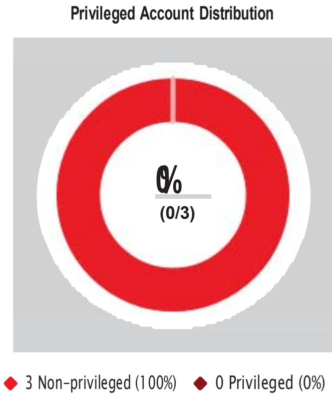
192.168.4.13	🖥	**Linux**	
192.168.4.10	⊞	**Windows**	
192.168.4.11	🖥	**Linux**	
192.168.4.15	🖥	**Linux**	
desktop-9lvldr5.CLIENT.CORP **00:15:5D:05:0A:0E** **Microsoft**	🖥	**Win10(D)**	Domain/Workgroup: CLIENT.CORP

Credentials & Passwords

3 Compromised Accounts[1]

Candor 'obtained access' to 3 accounts out of 3 using 2 techniques

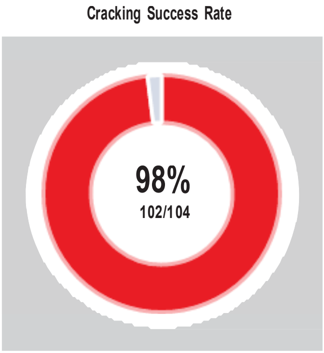

Obtaining Techniques

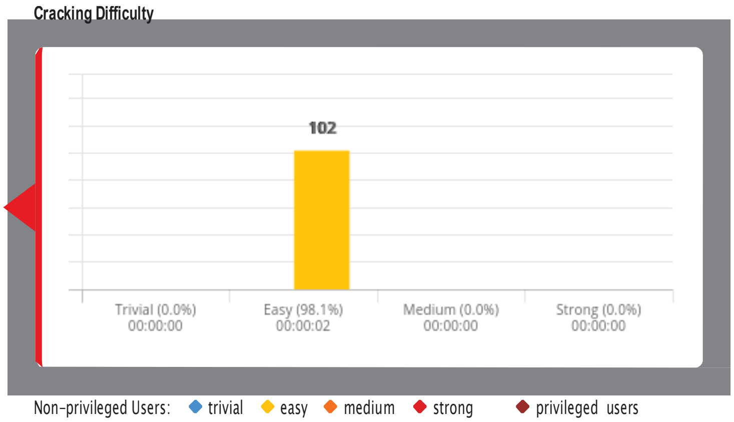

Privileged Account Distribution

[1] Refers to the state when Candor was able to access an account's plaintext password, password hash (that can be used without cracking) or credentials successfully used in a relay attack.

102 Passwords Cracked

29% of your passwords were cracked in under 30 minutes, a total of 102 accounts were cracked by Candor in 2 hours.


Cracking Success Rate


Cracking Difficulty

Compromised Accounts Table

(Listing 50 of 104 items¹).

Username	Type	Obtained	Password Cracking Difficulty	Host / Domain Name
ablad1991	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
adaund1981	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
administrator	Local User	PasswordSpray, Cracking	Easy 🕒 (avg. 00:00:02)	192.168.5.100
administrator	Local User	Exploit, Memory		192.168.5.102

Username	Type	Obtained	Password Cracking Difficulty	Host / Domain Name
administrator	Domain User	Msv, Memory		CLIENT
afruldeste	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
aliver	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
alksomed	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
apping	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
artudistrums	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
awaseen	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
awking	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
beanind	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
beary1971	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
beestre	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
biry1966	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
ceitheart1993	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
chme1974	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
ciancel61	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
citiold1966	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
comefultall1987	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
compled	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
coor1992	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
dadogiag	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
daunded1995	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
debectiand	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
dend1963	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
diesequan	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
dowerent60	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
duceir	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
effor1982	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP
equescam	Domain User	Exploit	Easy 🕒 (avg. 00:00:02)	CLIENT.CORP

Username	Type	Obtained	Password Cracking Difficulty	Host / Domain Name
eusive	Domain User	Exploit	Easy ◷ (avg. 00:00:02)	CLIENT.CORP
fasithater	Domain User	Exploit	Easy ◷ (avg. 00:00:02)	CLIENT.CORP
firessin	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
fivereclums	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
floace	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
forideare	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
fulta1953	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
gnalluggive88	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
gothis	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
goverrestat	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
guest	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
hamelf	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
hereinitoor	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
herson54	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
herus1960	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
hignisfat67	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
hingiverack	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP
hinte1958	Domain User	Exploit	Easy ◷(avg. 00:00:02)	CLIENT.CORP

Detailed Report
164 Vulnerabilities

111 Critical | 6 High | 2 Medium | 45 Low

Candor identified a total of 164 vulnerability occurrences across 4 severity levels

Listing 19 of 19 items.

#1 | 4.7

Priority[1]

Host can be forced to authenticate by a rogue server

1 occurrences

In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them. Since those are a broadcast protocols, anyone can respond to the query. An attacker may refer the request to a machine in his control using a man-in-the-middle attack, And obtain sensitive data such as username and password hash.

`CLIENT.CORP`

#2 | 5.8

Priority[1]

SMB server on endpoint does not validate clients

1 occurrences

`CLIENT.CORP`

#3 | 5.5

Priority[1]

EPP/EDR allowed writing malicious payload to disk

2 occurrences

An attacker may write a malware to disk for persistence on compromised hosts. A malware written to disk is one step before successful malware infection. Such a malware can perform various actions desired by the attacker, such as information collection, file encryption, or backdoor communication.

`192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)` `192.168.5.100 (STAFF-01.CLIENT.CORP)`

#4 | 8.8

Priority[1]

AV did not block malicious payload

2 occurrences

An attacker may inject a malware in order to run commands and control the host in various ways. An updated and fully capable AV/EDR security layout is required to ensure the safety of the network.

`192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)` `192.168.5.100 (STAFF-01.CLIENT.CORP)`

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements

8.1

NTLM hashed credentials stored in the memory

1 occurrences

Priority[1]

After a user logs on, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. This is meant to facilitate single sign-on (SSO), ensuring a user isn’t prompted to input credentials each time resource access is requested. The credential data may include Kerberos tickets, NTLM password hashes, LM password hashes, and even clear-text passwords (WDigest and SSP authentication protocols). An attacker with administrative access to a host can extract NTLM hashed credentials from the memory and use them to connect to hosts using an attacked called pass-the-hash, and possibly take-over those hosts.

```
192.168.5.100 (STAFF-
01.CLIENT.CORP)
```

8.3

Cleartext credentials stored in the memory

1 occurrences

Priority[1]

After a user logs on, a variety of credentials are generated and stored in the Local Security Authority Subsystem Service (LSASS) process in memory. An attacker with administrative access to a host can extract clear text credentials from the host's memory and proceed his attack into the organizational network. With these credentials he could possibly access different services and assets in the domain and steal or manipulate sensitive information.

```
192.168.5.100 (STAFF-
01.CLIENT.CORP)
```

9.3

MS17-010

1 occurrences

Priority[1]

An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability the attacker will get a high privileged shell (with SYSTEM access) on a host, getting the attacker a foothold in the organization's network. This vulnerability was used by several ransomware attacks to takeover hosts across the network and spread their malware.

```
192.168.5.102 (CLIENT-SVR-
2012.CLIENT.CORP)
```

9.8

BlueKeep (CVE-2019-0708)

3 occurrences

Priority[1]

An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability the attacker could crash the target (Denial of Service) or get a high privileged shell (with SYSTEM access) on a host with no need for authentication at all, getting the attacker a foothold in the organization's network.

```
192.168.5.100 (STAFF-          192.168.5.104 (DABOSS-          192.168.5.103 (TECH-PC.CLIENT.CORP)
01.CLIENT.CORP)                PC.CLIENT.CORP)
```

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements

8.6

Remediation Priority[1] Severity

Using empty password(s)

101 occurrences

Succeeded in cracking the password using an empty password

```
tobounce
sayinten
wasto1967
punkling
shapied82
guest
hereinitoor
herus1960
spead1968
biry1966
comefultall1987
chme1974
pland1989
citiold1966
letuarespin
thelismor
hingiverack
awaseen
housbady
ling1982
equescam
fasithater
meable
wilgre1966
herson54
thwitere63
firessin
apping
sterve
beanind
reastill
daunded1995
gnalluggive88
Go to Candor for 51 more...
woull1990
aliver
diesequan
alksomed
forideare
murne1963
morgilizeed
latim1969
withestable
neving
dowerent60
trofted
beestre
beary1971
dend1963
compled
```

6.9

Priority[1]

Password can be cracked using low GPU effort

1 occurrences

Many password cracking tools rely on dictionary rulesets, so it is important to avoid common passwords (such as Aa123456 or P@ssw0rd) and regular, unmodified dictionary terms. Inserting intentional, idiosyncratic misspellings or using acronyms is the recommended best practice. You can enhance Candor's cracking abilities by uploading a custom wordlist to Candor's Custom Dictionary and retest to uncover passwords that could be predicted or guessed by attackers who invest in social engineering techniques and are familiar with their targets.

```
administrator
```

7.7

Priority[1]

Domain user has remote code execution privileges on several hosts (more than 2)

1 occurrences

By gaining access to hosts, an attack might use the compromised credentials to move laterally across the network.

```
CLIENT.CORP
```

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements

8.8

Priority[1]

Print Nightmare (CVE-2021-34527)

1 occurrences

A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)

7.0

Priority[1]

User accounts are defined with password not required attribute

1 occurrences

Password Not required attribute allows a user to perform a successful authentication without using a password, regardless of the fact that a password is set. A user with this attribute does not require any password cracking, and could be used without any password at all.

CLIENT.CORP

5.5

Priority[1]

User accounts are defined with password never expires attribute

1 occurrences

Password Never Expire attribute is usually used for user accounts that are utilized as service accounts. This attribute should not be set on other users because most security policies require users to change their password within a certain time frame. For most organizations, the password policy requires users to change their password at least every 90 days.

CLIENT.CORP

2.3

Priority[1]

Discovered closed ports on the host

31 occurrences

Discovered closed port on the host (reachable without firewalling).

192.168.5.101 (ACCOUNTING-PC.CLIENT.CORP)

192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)

192.168.5.103 (TECH-PC.CLIENT.CORP)

192.168.4.14

192.168.5.50 (CLIENT-SVR-WIN2022.CLIENT.CORP)

192.168.4.29

192.168.4.28 (DESKTOP-KK865F1)

192.168.4.6

192.168.5.100 (STAFF-01.CLIENT.CORP)

192.168.5.49 (CAN-DEMO-HV)

192.168.4.9

192.168.4.1

192.168.4.4

192.168.4.19

192.168.4.53

192.168.4.15

192.168.4.16

192.168.4.3

192.168.4.27 (DESKTOP-QU21GJG)

192.168.4.13

192.168.4.10

192.168.4.5

192.168.4.41

192.168.4.12

192.168.5.104 (DABOSS-PC.CLIENT.CORP)

192.168.4.7

192.168.4.8

192.168.4.11

192.168.4.18

192.168.5.1 (_gateway)

192.168.4.17

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements

Priority[1]

3.3

Host uses NTLMv1 authentication

1 occurrences

An attacker might grab the NTLMv1 hash and crack it easily, NTLMv2 is more complex to crack.

192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)

Priority[1]

1.0

SMB message signing is disabled

8 occurrences

An attacker could abuse the unsigned SMB servers to relay NTLM challenges from other hosts and gain shell access.

192.168.5.100 (STAFF-01.CLIENT.CORP)
192.168.5.49 (CAN-DEMO-HV)
192.168.5.103 (TECH-PC.CLIENT.CORP)
192.168.4.28 (DESKTOP-KK865F1)
192.168.5.104 (DABOSS-PC.CLIENT.CORP)
192.168.4.27 (DESKTOP-QU21GJG)
192.168.5.101 (ACCOUNTING-PC.CLIENT.CORP)
192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)

Priority[1]

0.0

Host supports SMBv1 protocol

5 occurrences

An attacker might abuse many security flaws in the protocol to take over the host. Microsoft has advised to completely stop the use of Server Message Block 1.0.

192.168.5.100 (STAFF-01.CLIENT.CORP)
192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)
192.168.4.28 (DESKTOP-KK865F1)
192.168.5.103 (TECH-PC.CLIENT.CORP)
192.168.5.104 (DABOSS-PC.CLIENT.CORP)

Priority[1]

2.0

Printer Spooler service is available

1 occurrences

An attacker may use valid credentials in order to authenticate to the target machine Printer Spooler service, and attempt to initiate a reverse-authentication from the targeted machine account back to the attacker machine.

192.168.5.102 (CLIENT-SVR-2012.CLIENT.CORP)

[1] Remediation priority recommendations factor in the number of hosts affected by a vulnerability, the number and severity of achievements

233 Achievements

Candor accomplished 233 achievements in total. Every achievement represents a discrete successful action performed by Candor.

(Listing 18 of 18 items).

Severity	Details
9.4	(3) Gathered valuable information from host An attacker might find sensitive information and credentials on the host that might help in further attacks
9.1	(2) Opened a remote access session on the host An attacker can remotely execute arbitrary code on a host in the network, might steal or manipulate sensitive data, cause a denial of service and possibly extend his attack over the network.
9.0	(1) Validated domain credentials An attacker may abuse the domain credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.
8.1	(102) Obtained user's cleartext password An attacker might capture user's cleartext password and use it to login into hosts or services, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services.
7.7	(1) Found domain user with privileged remote code execution capabilities on several hosts By gaining access to hosts, an attack might use the compromised credentials to move laterally across the network.
7.6	(1) Replicated DC's credentials DB using DRSUAPI (DCSync) An attacker with high privileges on the domain controller (DC) can impersonate a DC entity and replicate all the credentials without executing remote code.
7.5	(102) Cracked user hash using GPU An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.
7.1	(1) Found a user with privileged RCE capabilities An attacker might use gathered credentials from breached hosts to move laterally across the network.
7.0	(1) Found users with Password-Not-Required attribute Password Not required attribute allows a user to perform a successful authentication without using a password, regardless of the fact that a password is set. A user with this attribute does not require any password cracking, and could be used without any password at all.
5.5	(1) Found users with Password-Never-Expires attribute Password Never Expire attribute is usually used for user accounts that are utilized as service accounts. This attribute should not be set on other users because most security policies require users to change their password within a certain time frame. For most organizations, the password policy requires users to change their password at least every 90 days.
5.5	(1) Captured credentials over HTTP An attacker may steal credentials by sniffing unencrypted HTTP traffic and use them to access hosts or services in the network, which may lead to sensitive data theft or manipulation, and possibly to a complete take-over of the hosts or services.

Severity	Details
5.5	(6) Captured credentials over SMB An attacker may steal credentials by impersonating hosts and tricking users to authenticate with him over SMB, and use them in order to access hosts or services in the network, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts or services.
5.4	(2) Performed a relay attack over SMB An attacker may abuse the Relay attack vector to authenticate to another host without obtaining the cleartext credentials.
3.5	(2) Validated local credentials An attacker may abuse the local credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.
3.4	(2) Uploaded malware to host An attacker can execute arbitrary malicious code on a host to extract sensitive data, manipulate the system, or use it to further advance the attack.
3.0	(2) Infiltrated .SCF file An attacker may create a malicious file on a remote share or host which will cause other users viewing it to authenticate with him over SMB so he can steal their credentials.
2.0	(2) Accessed shares using domain credentials An attacker with valid domain credentials may access shared folders and steal sensitive information from them.
2.0	(1) Authenticated with machine's printer service using validated credentials An attacker may use valid credentials in order to authenticate to the target machine Printer Spooler service, and attempt to initiate a reverse-authentication from the targeted machine account back to the attacker machine.

MITRE ATT&CK Matrix for Enterprise - Heat Map (1 of 2)

MITRE | ATT&CK®	Total Patterns	Most Common Technique
	725	Credential Access / Brute Force

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning T1595	Valid Accounts T1078	Windows Management Instrumentation T1047		Create or Modify System Process T1543	Indicator Removal on Host T1070
Scanning IP Blocks T1595.001	Domain Accounts T1078.002	System Services T1569 ^		Windows Service T1543.003	File Deletion T1070.004
Vulnerability Scanning T1595.002		Service Execution T1569.002			DCShadow T1207
Gather Victim Network Information T1590 ^					
DNS T1590.002					

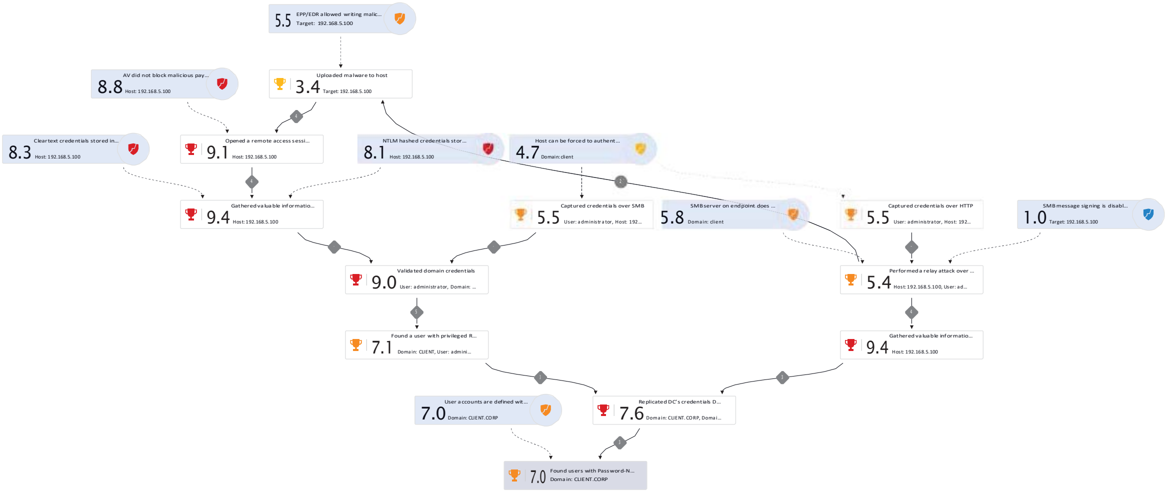
MITRE ATT&CK Matrix for Enterprise - Heat Map (2 of 2)

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Sniffing T1040 🟥	Remote System Discovery T1018 🟦	Taint Shared Content T1080 🟨	Adversary-in-the-Middle T1557 🟦	Remote File Copy T1105 🟧		Network Denial of Service T1498 🟦
Brute Force T1110 ⌃ 🟥	Network Sniffing T1040 🟥	Exploitation of Remote Services T1210 🟨	Data from Network Shared Drive T1039 🟦			
Password Guessing T1110.001 🟥	Network Service Scanning T1046 🟥	Remote Services T1021 ⌃ 🟧				
Adversary-in-the-Middle T1557 ⌃ 🟥	Network Share Discovery T1135 🟥	SMB/Windows Admin Shares T1021.002 🟨				
LLMNR/NBT-NS Poisoning and SM... T1557.001 🟥	System Network Configuration... T1016 🟦	Remote Desktop Protocol T1021.001 🟦				
Credential Dumping T1003 ⌄ 🟥	File and Directory Discovery T1083 🟦	Distributed Component Objec... T1021.003 🟦				
Credentials from Password Stores T1555 ⌃ 🟥	Cloud Service Discovery T1526 🟦	Windows Remote Management T1021.006 🟧				
Credentials from Web Browsers T1555.003 🟥	System Information Discovery T1082 🟦					
Forced Authentication T1187 🟨	System Owner/User Discovery T1033 🟦					
Unsecured Credentials T1552 ⌃ 🟥	Permission Groups Discovery T1069 ⌄ 🟦					
Credentials In Files T1552.001 🟥	Password Policy Discovery T1201 🟨					
Credentials in Registry T1552.002 🟥	Query Registry T1012 🟦					

Appendix

Select Attack Vector(s)

🏆 7.0 Found users with Password-Not-Required attribute


5.5 EPP/EDR allowed writing malic...
Target: 192.168.5.100
8.8 AV did not block malicious pay...
Host: 192.168.5.100
3.4 Uploaded malware to host
Target: 192.168.5.100
8.3 Cleartext credentials stored in...
Host: 192.168.5.100
9.1 Opened a remote access sessi...
Host: 192.168.5.100
8.1 NTLM hashed credentials stor...
Host: 192.168.5.100
4.7 Host can be forced to authent...
Domain: client
9.4 Gathered valuable informatio...
Host: 192.168.5.100
5.5 Captured credentials over SMB
User: administrator, Host: 192...
5.8 SMB server on endpoint does ...
Domain: client
5.5 Captured credentials over HTTP
User: administrator, Host: 192...
1.0 SMB message signing is disabl...
Target: 192.168.5.100
9.0 Validated domain credentials
User: administrator, Domain: ...
5.4 Performed a relay attack over ...
Host: 192.168.5.100, User: ad...
7.1 Found a user with privileged R...
Domain: CLIENT, User: admini...
9.4 Gathered valuable informatio...
Host: 192.168.5.100
7.0 User accounts are defined wit...
Domain: CLIENT.CORP
7.6 Replicated DC's credentials D...
Domain: CLIENT.CORP, Domai...
7.0 Found users with Password-N...
Domain: CLIENT.CORP
4
4
2
5
4
3
3
3

Parameters

Domain: CLIENT.CORP

Details

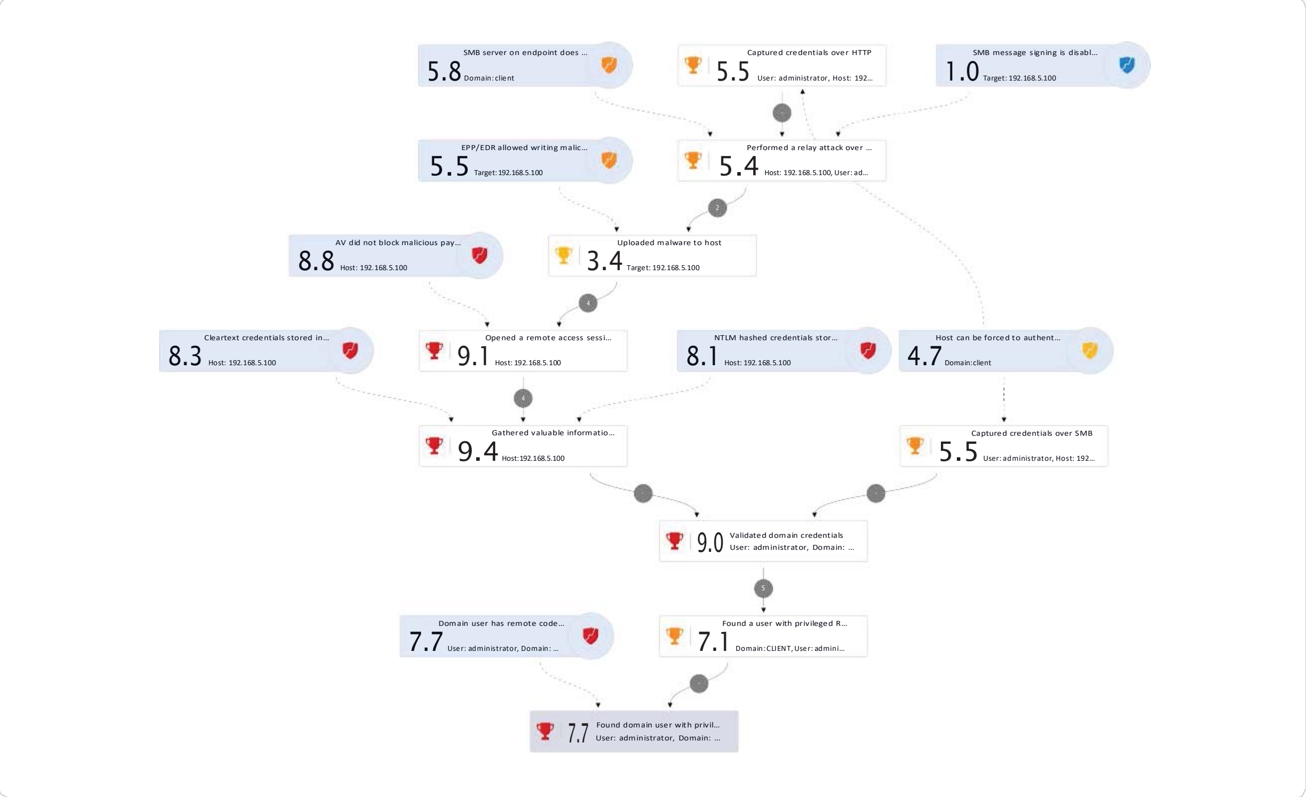
Time: Jun 30, 2022 15:21

MITRE Technique(s): DCShadow (T1207) ,Credential Dumping (T1003) ,DCSync (T1003.006)

Insight

Password Not required attribute allows a user to perform a successful authentication without using a password, regardless of the fact that a password is set. A user with this attribute does not require any password cracking, and could be used without any password at all.

7.7 Found domain user with privileged remote code execution capabilities on several hosts


SMB server on endpoint does ...
5.8 Domain: client
Captured credentials over HTTP
5.5 User: administrator, Host: 192...
SMB message signing is disabl...
1.0 Target: 192.168.5.100
EPP/EDR allowed writing malic...
5.5 Target: 192.168.5.100
Performed a relay attack over ...
5.4 Host: 192.168.5.100, User: ad...
2
AV did not block malicious pay...
8.8 Host: 192.168.5.100
Uploaded malware to host
3.4 Target: 192.168.5.100
4
Cleartext credentials stored in...
8.3 Host: 192.168.5.100
Opened a remote access sessi...
9.1 Host: 192.168.5.100
NTLM hashed credentials stor...
8.1 Host: 192.168.5.100
Host can be forced to authent...
4.7 Domain: client
4
Gathered valuable informatio...
9.4 Host: 192.168.5.100
Captured credentials over SMB
5.5 User: administrator, Host: 192...
9.0 Validated domain credentials
User: administrator, Domain: ...
5
Domain user has remote code...
7.7 User: administrator, Domain: ...
Found a user with privileged R...
7.1 Domain: CLIENT, User: admini...
7.7 Found domain user with privil...
User: administrator, Domain: ...

Summary

User has high privileges on 3 hosts

Parameters

User: administrator **Domain:** CLIENT **NTLM:** a1****************************** **Password:** ll**************

Details

Time: Jun 30, 2022 15:20

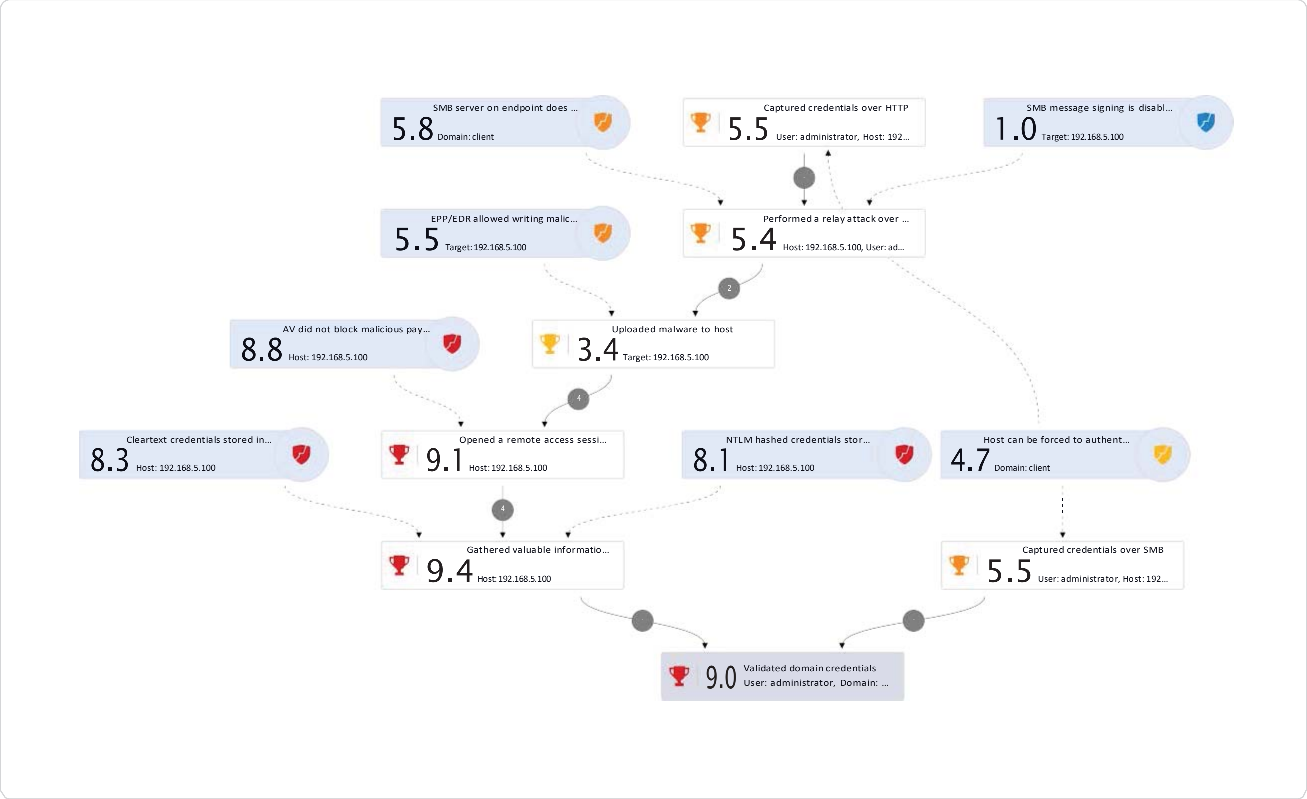
Insight

By gaining access to hosts, an attack might use the compromised credentials to move laterally across the network.

Results

Hosts:
192.168.5.50
192.168.5.102
192.168.5.100

9.1 Validated domain credentials


SMB server on endpoint does ...
5.8 Domain: client
Captured credentials over HTTP
5.5 User: administrator, Host: 192...
SMB message signing is disabl...
1.0 Target: 192.168.5.100
EPP/EDR allowed writing malic...
5.5 Target: 192.168.5.100
Performed a relay attack over ...
5.4 Host: 192.168.5.100, User: ad...
2
AV did not block malicious pay...
8.8 Host: 192.168.5.100
Uploaded malware to host
3.4 Target: 192.168.5.100
4
Cleartext credentials stored in...
8.3 Host: 192.168.5.100
Opened a remote access sessi...
9.1 Host: 192.168.5.100
NTLM hashed credentials stor...
8.1 Host: 192.168.5.100
Host can be forced to authent...
4.7 Domain: client
4
Gathered valuable informatio...
9.4 Host: 192.168.5.100
Captured credentials over SMB
5.5 User: administrator, Host: 192...
9.0 Validated domain credentials
User: administrator, Domain: ...

Parameters

User: administrator **Domain:** CLIENT **Password:** ll***************

Details

Time: Jun 30, 2022 15:19

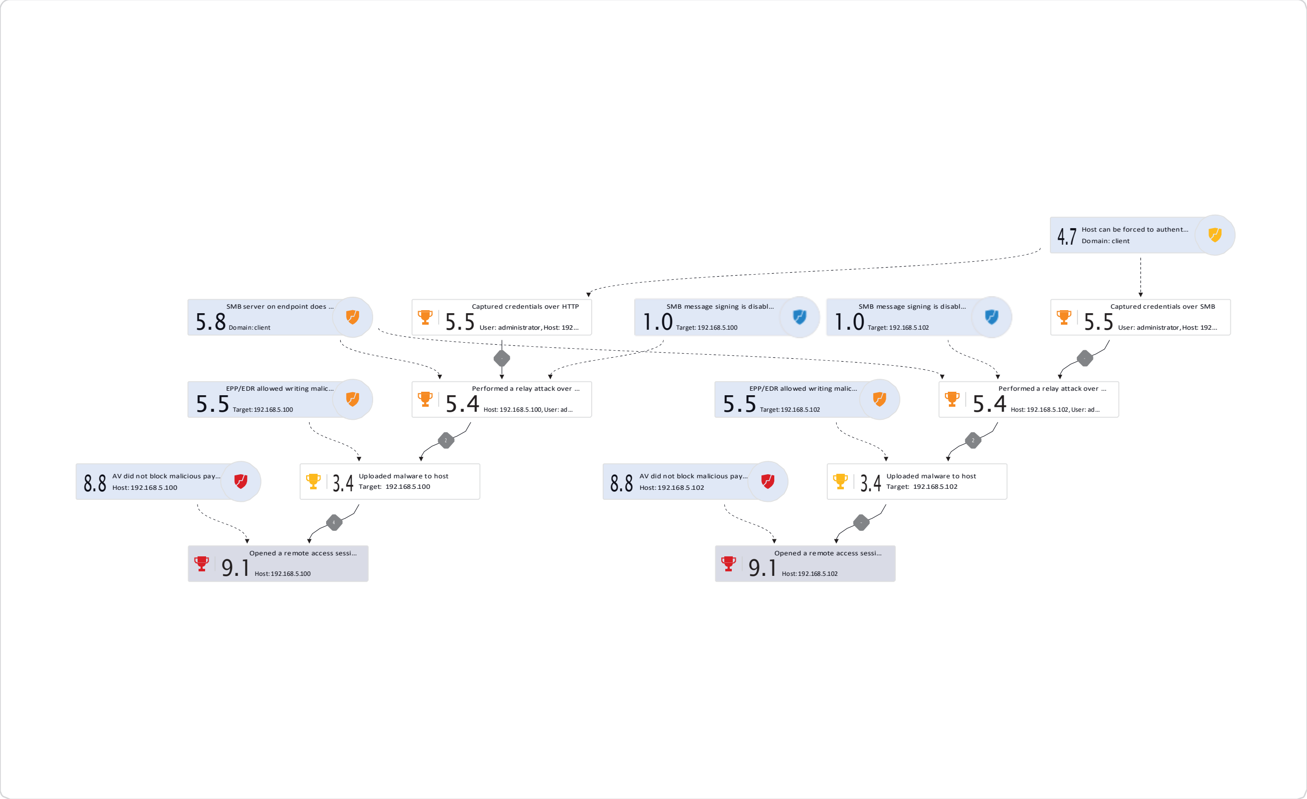
Insight

An attacker may abuse the domain credentials to login to hosts and gather information about the users and possibly take-over the host and escalate his attack.

Results

Host: 192.168.5.50
Protocol: Kerberos
Port: 88

9.2 Opened a remote access session on the host


4.7 Host can be forced to authent...
Domain: client
5.8 SMB server on endpoint does ...
Domain: client
5.5 Captured credentials over HTTP
User: administrator, Host: 192...
1.0 SMB message signing is disabl...
Target: 192.168.5.100
1.0 SMB message signing is disabl...
Target: 192.168.5.102
5.5 Captured credentials over SMB
User: administrator, Host: 192...
5.5 EPP/EDR allowed writing malic...
Target: 192.168.5.100
5.4 Performed a relay attack over ...
Host: 192.168.5.100, User: ad...
5.5 EPP/EDR allowed writing malic...
Target: 192.168.5.102
5.4 Performed a relay attack over ...
Host: 192.168.5.102, User: ad...
8.8 AV did not block malicious pay...
Host: 192.168.5.100
3.4 Uploaded malware to host
Target: 192.168.5.100
8.8 AV did not block malicious pay...
Host: 192.168.5.102
3.4 Uploaded malware to host
Target: 192.168.5.102
9.1 Opened a remote access sessi...
Host: 192.168.5.100
9.1 Opened a remote access sessi...
Host: 192.168.5.102
2
4
2

Parameters

Domain: CLIENT **Host:** 192.168.5.100

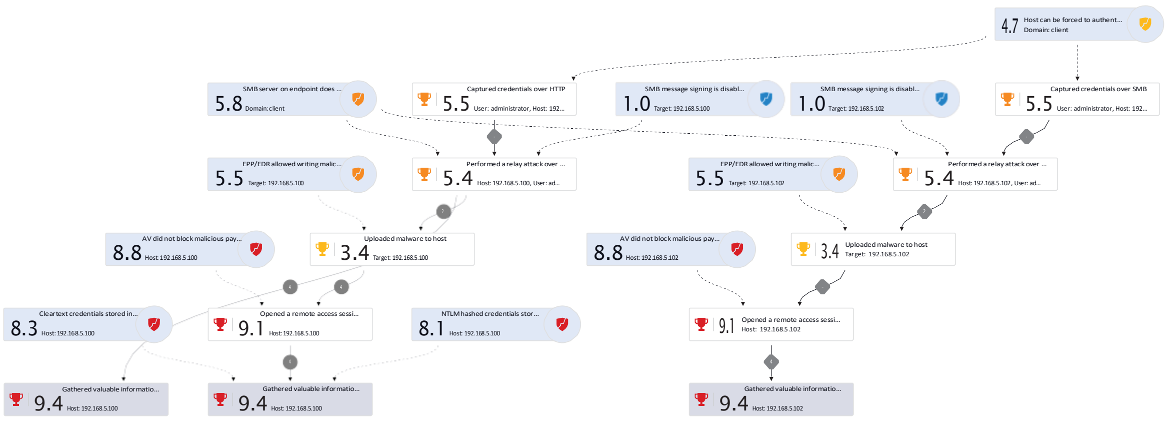
Details

Time: Jun 30, 2022 15:16
Domain: CLIENT.CORP
IPv4: 192.168.5.100
MAC: 00:15:5D:05:0A:0B
OS: Win7 (D)
Vendor: Microsoft
MITRE Technique(s): Credentials from Password Stores (T1555) ,Credentials from Web Browsers (T1555.003) ,Unsecured Credentials (T1552) ,Credentials In Files (T1552.001) ,Credentials in Registry (T1552.002)

Insight

An attacker can remotely execute arbitrary code on a host in the network, might steal or manipulate sensitive data, cause a denial of service and possibly extend his attack over the network.

9.4 Gathered valuable information from host


4.7 Host can be forced to authent... Domain: client
5.8 SMB server on endpoint does ... Domain: client
5.5 Captured credentials over HTTP User: administrator, Host: 192...
1.0 SMB message signing is disabl... Target: 192.168.5.100
1.0 SMB message signing is disabl... Target: 192.168.5.102
5.5 Captured credentials over SMB User: administrator, Host: 192...
5.5 EPP/EDR allowed writing malic... Target: 192.168.5.100
5.4 Performed a relay attack over ... Host: 192.168.5.100, User: ad...
5.5 EPP/EDR allowed writing malic... Target: 192.168.5.102
5.4 Performed a relay attack over ... Host: 192.168.5.102, User: ad...
2
8.8 AV did not block malicious pay... Host: 192.168.5.100
3.4 Uploaded malware to host Target: 192.168.5.100
8.8 AV did not block malicious pay... Host: 192.168.5.102
3.4 Uploaded malware to host Target: 192.168.5.102
4
8.3 Cleartext credentials stored in... Host: 192.168.5.100
9.1 Opened a remote access sessi... Host: 192.168.5.100
8.1 NTLM hashed credentials stor... Host: 192.168.5.100
9.1 Opened a remote access sessi... Host: 192.168.5.102
9.4 Gathered valuable informatio... Host: 192.168.5.100
9.4 Gathered valuable informatio... Host: 192.168.5.100
9.4 Gathered valuable informatio... Host: 192.168.5.102

Summary

Extracted 2 local NTLM hash(es)

Parameters

Domain: CLIENT **User:** administrator **Host:** 192.168.5.100

Details

Time: Jun 30, 2022 14:44
Domain: CLIENT.CORP
IPv4: 192.168.5.100
MAC: 00:15:5D:05:0A:0B
OS: Win7 (D)
Vendor: Microsoft

Insight

An attacker might find sensitive information and credentials on the host that might help in further attack

Testing Scenario Details

Group	Type	Details
Info	Name	Candor Protect: Client Demo
	Description	Simulated Black Box Senario
	Type	Penetration Testing (Black Box)
	Scheduling	No Schedule
	Created By	admin
Summary	Completion Status	✓ Completed successfully
	Time & Duration	Jun 30 2022 14:23 – Jun 30 2022 16:24, 02:00
	Action Approval Score	64 / 69 , 93%
Ranges	Include IP Range(s)	192.168.4.1 - 192.168.4.254 192.168.5.1 - 192.168.5.254
Intensity	Maximum Duration	00d:01h:00m
	Spoofing Duration	00d:01h:00m
	Perform Automatic Rescan	Not Defined
	Stealthiness Level	(1) Full enumeration with noisy discovery
Exploitation Settings	Basic	Allow Exploits – Require Approval for Exploits
		Allow DHCP Man In the Middle Attacks (Always requires approval)
		Allow Worst of Both Worlds Exploit / Attack
		Allow Out of IP Range Spoofing
		Allow Services Bruteforce – Require Approval
		Allow Web Application Bruteforce (always requires approval) – Use 'Password Cracking Custom Dictionary' in Web Application Bruteforce (might extend cracking time significantly)
		Allow Automatic Active Directory Account Creation, Relay Attacks