

# Indice

<b>1</b>	<b>Introduzione</b>	<b>11</b>
1.1	Che cos'è il Brute Force . . . . .	11
1.2	Hash . . . . .	11
1.2.1	Type . . . . .	11
1.2.2	Common Hash example . . . . .	11
1.3	Strumenti . . . . .	11
1.4	Password analysis . . . . .	11
<b>2</b>	<b>Tecniche di Brute Force</b>	<b>13</b>
2.1	Brute Force Attack . . . . .	13
2.2	Dictionary Attack . . . . .	13
2.3	Rainbow Table Attack . . . . .	13
2.4	Social engineering . . . . .	13
2.5	Offline Attack . . . . .	13
2.6	Mask Attack . . . . .	13
2.7	Rule Attack . . . . .	13
<b>3</b>	<b>Extract Hashes</b>	<b>15</b>
3.1	Windows . . . . .	15
3.2	Linux . . . . .	15
3.3	MacOS . . . . .	15
3.4	Network Hashes . . . . .	15
3.5	Database hash extraction . . . . .	15
3.6	Virtual Machines . . . . .	15
3.6.1	VMware . . . . .	15
3.6.2	Docker . . . . .	15
3.6.3	Kubernetes . . . . .	15
3.7	Cloud Services . . . . .	15
3.7.1	AWS . . . . .	15
3.7.2	GCP <i>GoogleCloudPlatform</i> . . . . .	15
<b>4</b>	<b>Brute Force Dispositivi mobile</b>	<b>17</b>
4.1	Brute Force con Dispositivi mobile . . . . .	17
4.1.1	NetHunter . . . . .	17

4.1.2	Rubber Ducky & Android_HID . . . . .	17
4.2	Brute force con Kali . . . . .	17
4.3	Android-PIN-Bruteforce . . . . .	17
4.4	WBRUTE . . . . .	18
4.5	CiLocks . . . . .	18
4.6	Arkhotia . . . . .	18
<b>5</b>	<b>Wi-Fi Brute Force</b>	<b>19</b>
5.1	Tecniche . . . . .	19
5.2	Strumenti . . . . .	19
5.3	Esempio . . . . .	19
<b>6</b>	<b>Parallelismo</b>	<b>21</b>
6.1	Tecniche . . . . .	21
6.2	Strumenti . . . . .	21
6.3	Esempio . . . . .	21
<b>7</b>	<b>CUDA</b>	<b>23</b>
7.1	CPU vs GPU . . . . .	23
7.2	Strumenti . . . . .	23
7.3	Esempio . . . . .	23
<b>8</b>	<b>Tecniche di difesa</b>	<b>25</b>