بسمه تعالی

حملات جستجوی فراگیر SSH[1]

[1] Brute-Force SSH Attacks

فهرست مطالب

۱ مقدمه

در رمزنگاری، «حمله جستجوی فراگیر[2]»، حمله‌ای است که در آن تمام حالات ممکن تا رسیدن به جواب بررسی می‌گردد. برای هر الگوی رمزنگاری می‌توان زمان لازم برای آزمودن کلیه حالات ممکن برای کلید را محاسبه نمود و معمولاً الگوهای رمزنگاری طوری طراحی می‌شوند که آزمودن تمامی حالات ممکن در یک زمان قابل قبول، غیرممکن یا غیرموثر باشد. همچنین حمله جستجوی فراگیر یک معیار برای شناخت روش‌های شکستن رمز است، به این معنی که هر روشی که سریع‌تر از روش حمله جستجوی فراگیر بتواند رمز را بازگشایی نماید، یک روش شکستن رمز تلقی می‌شود. آزمودن کلیه حالات ممکن روشی برای یافتن رمز عبور نیز به شمار می‌رود. به طور معمول نرم‌افزارها پس از چند بار وارد کردن رمز عبور نادرست، حساب کاربر را مسدود نموده و یا در فرایند اعتبارسنجی تأخیر زمانی ایجاد می‌کنند تا از آزمودن دیگر حالات جلوگیری شود.

مطالعات اخیر درباره روش‌های آسیب‌پذیری به دو روش اصلی حمله اشاره می‌کند:

۱. حملات جستجوی فراگیر علیه سرویس‌های راه‌دور مانند SSH[3]، FTP[4] و Telnet[5].
۲. آسیب‌پذیری‌های برنامه‌های تحت وب.

در ۲۰ گزارش برتر خطرات امنیتی سال ۲۰۰۷، موسسه SANS حملات حدس رمز عبور جستجوی فراگیر علیه سرورهای SSH، FTP و Telnet را این‌گونه نام‌گذاری کرد: «رایج‌ترین نوع حمله جهت به خطر انداختن سرورهای دارای دسترسی به اینترنت». این گزارش بیان می‌کند که رخنه‌های اصلاح‌نشده مانند آسیب‌پذیری سرریز بافر در فعالیت‌های اعتبارسنجی این سرویس‌ها می‌تواند باعث اجرای اختیاری کد شود؛ هرچند، این گزارش به تهدید جهانی اشاره دارد. رمزهای عبور ضعیف به عنوان نقاط ضعف احتمالی در این سیستم‌ها شناخته شده‌اند، به دلیل اینکه «رمزهای عبور جستجوی فراگیر قابل به‌کارگیری به عنوان یک تکنیک جهت به خطر انداختن کلیه سیستم‌ها و حتی سیستم‌های کاملاً اصلاح‌شده است».

1- Brute-Force Attack
2- Secure Shell: is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unsecured network.
3- FTP: The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.
4- Telnet: Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers.

در این گزارش، بر حملات جستجوی فراگیر SSH تمرکز می‌شود. همچنین داده‌های حاصل از تعداد بسیاری از حملات جستجوی فراگیر SSH علیه سیستم‌های لینوکس متصل به انواع مختلف شبکه‌ها آنالیز می‌شوند. الگوهای موجود در رمزهای عبور بکار رفته در این حملات و همچنین روش‌های بکار گرفته شده بحث می‌شوند.

۲ الگوهای حمله

در این بخش به بررسی عمیق‌تر الگوهای حمله پرداخته می‌شود. ابتدا انواع مختلف رمزهای عبور استفاده شده در این حملات روی هانی‌پات‌ها[۶] و سپس مبحثی درباره برخی سناریوهای حمله ذکر می‌شوند.

۲-۱ رمزهای عبور و لغت‌نامه‌های حمله

برای سرورهای SSH که اجازه اعتبارسنجی رمز عبور را می‌دهند، رمزهای عبور یکی از عوامل آسیب‌پذیری به حساب می‌آیند. بنابراین این تحلیل، با یک بررسی از انواع مختلف رمزهای عبور و لغت‌نامه‌های استفاده‌شده در حملات روی هانی‌پات‌ها شروع می‌گردد.

۲-۱-۱ رمزهای عبور

یکی از اولین سؤال‌های به وجود آمده در این تحلیل به میزان اشتراکی وابسته است که می‌تواند در رمزهای عبور استفاده‌شده در حملات روی هانی‌پات‌ها وجود داشته باشد. جدول ۱، ۲۰ رمز عبور با بیشترین تکرار در هر هانی‌پات را نشان می‌دهد. رمزهای عبور دارای فونت برجسته، رمزهایی هستند که میان ۲۰ رمز برتر در هر سه هانی‌پات یافت شده‌اند. در زمان ارزیابی این لیست‌ها، مشاهده شد که این رمزهای عبور در حملات حاصل از ۲۷۹ آدرس IP تولید شده‌اند. تنها ۸ آدرس IP در این حملات روی بیش از یک هانی‌پات بوده‌اند.

در کل، ۱۲ رمز عبور در لیست ۲۰ رمز عبور برتر در هر سه هانی‌پات و ۵ رمز عبور نیز در دو هانی‌پات یافت شدند. این نتایج، نتایج قابل‌توجهی هستند به دلیل اینکه این مسئله به سبب وجود سه رمز عبور طولانی در لیست هانی‌پات «تجاری» نبوده است.

1- Honeypots: consists of low-end PCs with minimal Linux server installations.

۱. asutcmhack123@
۲. 40232046bad
۳. #@!asutcmhack!@#

این رمزهای عبور، هر کدام صدها مرتبه در ترکیب با نام‌های کاربری مختلف در یک حمله روی هانی‌پات تجاری استفاده شده‌اند. همچنین این رمزهای عبور جزئی از قوی‌ترین نوع رمزهای عبور نیز به حساب می‌آیند. در واقع، رمز عبور asutcmhack123@ «بهترین رتبه» را در زمان آزمایش با ابزار بررسی آنلاین رمز عبور مایکروسافت دریافت کرد، درحالی‌که ۲ رمز عبور دیگر به عنوان رمز عبور «متوسط» رتبه‌بندی شدند.

جدول ۱. ۲۰ رمز عبور برتر حاصل از هر هانی‌پات

محدوده دانشگاهی	محدوده تجاری	محدوده مسکونی
123456	**123456**	**123456**
password	**password**	**password**
12345	**test**	**test**
test	**admin**	**12345**
admin	**test123**	**123**
1234	asutcmhack123@	**1234**
123	*passwd*	**test123**
root	40232046bad	*passwd*
qwetry	!@#asutcmhack!@#	1
abc123	**root**	12
administrator	**12345**	**root**
12345678	**qwetry**	**admin**
user	**1234**	changeme
linux	*mysql*	abc123
test123	**123**	**qwetry**
guest	*apache*	**guest**
mysql	master	lq2w3e
1234567	**user**	**user**
apache	*linux*	Newpass
master	**guest**	asdfgh

۲-۱-۲ لغت‌نامه‌های حمله

تشابه جالب‌توجه مشاهده‌شده میان رمزهای عبور پرمصرف در حملات روی هر سه هانی‌پات، باعث تشکیک در این موضوع شد که ممکن است مهاجمان از لغت‌نامه‌های مشترک نام کاربری و رمزهای عبور استفاده کرده باشند. در واقع، با بررسی تعداد تلاش‌های ورود به سیستم در حملات روی هر سه هانی‌پات و مقایسه دستی نام‌های کاربری و رمزهای عبور منحصربه‌فرد استفاده شده در هر حمله، شواهدی مبنی بر وجود حداقل ۵ نوع از چنین لغت‌نامه‌هایی حاصل شد.

معیارهای استفاده‌شده برای تشخیص این لغت‌نامه‌های حمله بسیار سخت‌گیرانه بودند. به‌ویژه، این‌گونه تصور می‌شود که در دو مورد از حملات از یک لغت‌نامه استفاده شده اگر و فقط اگر از جفت‌های نام کاربری / رمز عبور دقیقاً مشابه و به همان ترتیب استفاده شده باشد. همچنین بسیاری از کاربردهای جزئی از لیست‌های نام کاربری / رمز عبور مشابه مشاهده گردیده که به دلیل جزئی‌بودنشان به حساب نمی‌آیند.

جدول ۲ برخی آمار درباره تناوب لغت‌نامه‌های تشخیص داده شده و استفاده‌شده در حمله را نشان می‌دهد. لغت‌نامه‌ها براساس تعداد جفت‌های نام کاربری / رمز عبور موجود در هر لغت‌نامه نام‌گذاری شده‌اند. مجموع ۵۱ حمله‌ای که از این لغت‌نامه‌ها استفاده می‌کنند، ۱۷ درصد حملات جستجوی فراگیر SSH روی

هانی‌پات‌ها را دربرمی‌گیرند. با توجه به معیارهای سخت‌گیرانه‌ی استفاده‌شده برای تعریف هر لغت‌نامه، نتایج به‌دست آمده بسیار جالب‌توجه هستند. اطلاعات بیشتر درباره هر لغت‌نامه در ادامه ارائه شده است.

جدول۲. لغت‌نامه‌های نام‌کاربری/ رمز عبور استفاده‌شده در حملات SSH

	دانشگاهی	تجاری	مسکونی	مجموع
لغت‌نامه ـ ۹	۷	۴	۶	۱۷
لغت‌نامه ـ ۶۶	۱	۲	صفر	۳
لغت‌نامه ـ ۱۶۸	۸	۶	۱۰	۲۴
لغت‌نامه ـ ۳۶۳	۱	۱	۲	۴
لغت‌نامه ـ ۳۷۳	۲	صفر	۱	۳
مجموع	۱۹	۱۳	۱۹	۵۱

۲-۱-۲-۱ لغت‌نامه ـ ۹

کوچک‌ترین لغت‌نامه در بین ۵ لغت‌نامه که شامل ۹ جفت نام‌کاربری/ رمز عبور است، مجموعاً در ۱۷ حمله روی هر ۳ هانی‌پات استفاده شده است. همان‌طور که جدول ۳ نشان داده شده، نام‌های کاربری و رمزهای عبور استفاده‌شده کاملاً ساده هستند. واضح است که این لغت‌نامه به‌گونه‌ای طراحی‌شده تا به کاوش تعداد زیادی از سرورهای آسیب‌پذیر احتمالی در مدت‌زمان بسیار کوتاه اجازه دهد. مدت زمان میانگین مورد نیاز برای تکمیل ۱۷ حمله با استفاده از این لغت‌نامه کمتر از ۲۲ ثانیه محاسبه گردید.

جدول ۳. نام‌های کاربری / رمزهای عبور موجود در لغت‌نامه ـ ۹

نام‌های کاربری	رمزهای عبور
test	test
guest	guest
admin	admins
user	User
root	password
root	root
root	123456
test	123456

۲-۱-۲-۲ لغت‌نامه ـ ۶۶

تمامی جفت‌های نام‌کاربری/ رمز عبور موجود در این لغت‌نامه مخصوصاً به سمت حساب کاربری ریشه[۷] حرکت می‌کنند. رمزهای عبور استفاده‌شده، تعداد اندکی از لیست ۲۰ رمز برتر و همچنین بعضی عبارت‌های ساده مانند changeme و trustno1 را دربرمی‌گیرد. با این‌حال، اکثریت رمزهای عبور یافت شده در این لغت‌نامه براساس الگوهای ساده صفحه کلید می‌باشند:

- qazwsxedc
- qpwoeiruty
- 1q2w3e4r
- !@#$%^

۲-۱-۲-۳ لغت‌نامه ـ ۱۶۸

این لغت‌نامه ثابت کرده که رایج‌ترین انتخاب برای حمله روی هانی‌پات‌ها است. این لغت‌نامه شامل تنوع وسیعی از نام‌های کاربری است، از جمله: حساب کاربری ریشه؛ حساب‌های گوناگون سیستمی؛ نام‌های حساب عمومی یا موقتی مانند کارکنان، فروشندگان و استخدامی؛ همچنین نام‌های مناسب. رمزهای عبور موجود در کل کاملاً ساده هستند که اکثریت آن‌ها به یک نام کاربری یا یک تغییر محدود شده‌اند. به عبارت دیگر هر نسخه در حملات روی چندین هانی‌پات استفاده شده و از جفت‌های نام‌کاربری/ رمزعبور دقیقاً مشابه و دقیقاً به همان ترتیب استفاده می‌کند. هر نسخه تعداد کمی از تغییرات (۱۰ یا کمتر) را به نام‌های کاربری، رمزهای عبور یا هر دو از نسخه‌های دیگر را ترکیب می‌کند. با وجود این تفاوت‌های جزئی، هر نسخه لغت‌نامه ـ ۱۶۸، تعداد مشابهی از جفت‌های نام‌کاربری/ رمز عبور را دربردارد.

۲-۱-۲-۴ لغت‌نامه ـ ۳۶۳ و لغت‌نامه ـ ۳۷۳

این لغت‌نامه‌ها مجموعه گوناگونی از نام‌های کاربری و رمزهای عبور را دربرمی‌گیرند و به سادگی می‌توانند مجموعه‌ای از لغت‌نامه‌های کوچک‌تر را ارائه کنند. حساب کاربری ریشه و حساب‌های گوناگون سیستمی به همراه رمزهای عبور از انواع مختلف مانند کلمات رایج انگلیسی، نام‌های مناسب، الگوهای صفحه‌کلید و

1- Root

«لیت‌ها[8]» که اعداد و نمادها را جایگزین حروفی می‌کند به‌طوری‌که شبیه حرف جایگزین شده است، به خوبی نشان داده شده‌اند. برای مثال، این لغت‌نامه‌های این تغییرات را روی کلمه رمز عبور دربرمی‌گیرند:

- p@ssw0rd
- p@ssword
- passw0rd
- pa$$word
- pa55word
- pa55w0rd

هردوی این لغت‌نامه‌ها بیش از صد جفت نام‌کاربری / رمز عبور یکسان براساس نام‌های مناسب دارند.

۲-۲ روش‌های حمله

همان‌طور که در بخش قبل بیان شد، تعداد تلاش‌های ورود به سیستم که در زمان حملات منحصربه‌فرد مشاهده شدند، بسیار متفاوت هستند. بیش از یک‌سوم حملات، شامل ۱۰ تلاش ورود به سیستم یا کمتر را می‌شود، درحالی‌که دیگر مهاجمان صدها یا حتی هزاران ورود به سیستم را در یک حمله آزمودند. در واقع، در حدود ۱۰ درصد حملات، بیش از هزار تلاش ورود به سیستم ثبت شده است.

درحالی‌که اکثر حملات نسبتاً ساده به نظر می‌رسند، اخیراً تعداد کمی از حملات به گونه‌ای طراحی شده‌اند تا از تشخیص توسط سیستم‌های جلوگیری از نفوذ بگریزند. جزئیات این حملات را در ادامه مشاهده می‌کنید.

۲-۲-۱ حمله آهسته جستجوی فراگیر SSH

در بازه زمانی ۸ روزه در ژانویه سال ۲۰۰۸، ۲۱ حمله مجزا روی یک هانی‌پات که از یک آدرس IP استفاده می‌کرد مشاهده گردید. تعداد ورود به سیستم‌های آزمایش شده در زمان هر جلسه تا حدی تفاوت داشت اما تعداد ورود به سیستم‌های آزمایش شده در زمان یک جلسه هرگز از ۹ روز تجاوز نکرد. مجموع تلاش‌های ورود به سیستم در ۸ روز، ۱۳۰ مرتبه بوده که تمامی آن‌ها حساب کاربری ریشه را هدف گرفته بودند.

1- Leet: (or "1337"), also known as eleet or leetspeak, is an alternative alphabet for the English language that is used primarily on the Internet.

رمزهای عبور استفاده‌شده در ۵۰ تلاش اولیه در ۳ روز اول کامل ساده بودند. این رمزها تقریباً از کلمات رایج انگلیسی، نام‌های خاص و عبارات ساده مانند newuser، stuffedturkey و youareok تشکیل می‌شدند. رمزهای عبور استفاده‌شده در جلسه بعد شامل ۹ تلاش ورود به سیستم که تقریباً از «لیت‌ها» مانند c4bl3m0d3m (cablemodem)، c4l3nd4r (calender) و c4lif0rni4 (california) تشکیل می‌شدند.

با شروع جلسه ۱۱ و ادامه آن در سرتاسر جلسات حملات باقیمانده، رمزهای عبور قوی‌تر شدند. در واقع، از رمزهای عبور استفاده‌شده در ۷۳ تلاش ورود به سیستم آخر، ۵۳ درصد توسط ابزار بررسی رمز عبور شرکت مایکروسافت به عنوان «قوی» رتبه‌بندی شدند. مثالی از این رمزهای عبور در جدول ۴ نشان داده شده‌اند.

جدول ۴. رمزهای عبور «قوی» استفاده‌شده در زمان حمله آهسته جستجوی فراگیر SSH روی یک هانی‌پات

U50s8AdF
OxZBA4xOMd
35t3K6OZ
Zh59Epu5mQxq
8Nv9YupQu0v
K48v87GR8RF
QcxC3OuZUH
848TmMf57
bC28S9R7Weg
nezBh57yi1jm
Kqr17tJ89Tan

۲-۲-۲ حمله توزیع‌شده جستجوی فراگیر SSH

حمله دیگری که ظاهراً به‌گونه‌ای طراحی شده تا از تشخیص توسط سیستم جلوگیری از نفوذ بگریزد مشاهده گردید. این حمله دارای یک سری هماهنگ از تلاش‌های ورود به سیستم بوده که از ۱۰ آدرس IP متوالی در شبکه کلاس C مشابه شروع می‌شوند. در مجموع ۳۳ ورود به سیستم در طول ۳ دقیقه آزمایش شد که تعداد ورودها با استفاده از یک آدرس IP مشابه، بیش از ۵ مرتبه نبوده است. نتیجه تلاش‌های ورود به سیستم در جدول ۵ نشان داده شده است. جفت‌های نام‌کاربری / رمز عبور استفاده‌شده در این حمله با ۳۲ جفت یافت‌شده در یک نسخه از لغت‌نامه حمله به نام «لغت‌نامه ـ ۱۶۸» در بخش قبل مشابه است. با وجود این‌که جفت‌های نام‌کاربری / رمز عبور در ۱۰ منبع آدرس IP توزیع شده‌اند، جفت‌های استفاده‌شده در این حمله، از نظر ترتیب با دیگر حملات ناشی از یک IP واحد، مشابه هستند.

جدول ۵. حمله توزیع‌شده جستجوی فراگیر SSH

آدرس IP	رمز عبور	نام‌کاربری	زمان
aaa.bbb.ccc.131	staff	staff	10:42:34
aaa.bbb.ccc.136	sales	sales	10:42:39
aaa.bbb.ccc.131	recruit	recruit	10:42:44
aaa.bbb.ccc.137	alias	alias	10:42:51
aaa.bbb.ccc.137	office	office	10:42:58
aaa.bbb.ccc.137	samba	samba	10:43:03
aaa.bbb.ccc.131	tomcat	tomcat	10:43:08
aaa.bbb.ccc.136	webadmin	webadmin	10:43:13
aaa.bbb.ccc.138	spam	spam	10:43:21
aaa.bbb.ccc.134	virus	virus	10:43:29
aaa.bbb.ccc.139	cyrus	cyrus	10:43:36
aaa.bbb.ccc.136	oracle	oracle	10:43:41
aaa.bbb.ccc.134	michael	michael	10:43:46
aaa.bbb.ccc.137	ftp	ftp	10:43:51
aaa.bbb.ccc.135	test	test	10:43:57
aaa.bbb.ccc.138	webmaster	webmaster	10:44:05
aaa.bbb.ccc.134	postmaster	postmaster	10:44:10
aaa.bbb.ccc.139	postfix	postfix	10:44:15
aaa.bbb.ccc.139	postgres	postgres	10:44:21
aaa.bbb.ccc.131	paul	paul	10:44:26
aaa.bbb.ccc.131	root	root	10:44:32
aaa.bbb.ccc.133	guest	guest	10:44:38
aaa.bbb.ccc.139	admin	admin	10:44:43
aaa.bbb.ccc.138	linux	linux	10:44:49
aaa.bbb.ccc.140	user	user	10:44:54
aaa.bbb.ccc.139	david	david	10:45:00
aaa.bbb.ccc.136	web	web	10:45:06
aaa.bbb.ccc.137	apache	apache	10:45:11
aaa.bbb.ccc.132	pgsql	pgsql	10:45:17

aaa.bbb.ccc.134	mysql	mysql	10:45:22
aaa.bbb.ccc.138	Info	info	10:45:30
aaa.bbb.ccc.135	tony	tony	10:45:35
aaa.bbb.ccc.138	core	core	10:45:45

این حملات تلاش‌های جدیدی را برای کاهش حجم حملات جستجوی فراگیر SSH ارائه کرده و بنابراین از تشخیص اجتناب می‌کند. به نظر می‌رسد حملات توزیع‌شده SSH برای باتنت‌های بزرگ و توزیع‌شده کاربردی‌تر باشد.

۲-۲-۳ حمله ماسک

حمله ماسک، حمله‌ای غیرقابل‌جایگزین است و زمانی به کار می‌رود که قسمتی از رمز عبور یا تعداد کاراکترهای آن مشخص باشد. برای مثال زمانی که مشخص است رمز عبور ۱۲ کاراکتر بوده و با qwerty خاتمه می‌یابد، واضح است که جستجو برای محدود رمزهای عبور ۱۲ کاراکتری غیرمنطقی است. در این مورد تنها نیاز است ۶ کاراکتر اول از رمز عبور بازیابی شود. استفاده از حمله ماسک، مدت زمان جستجوی فراگیر را کاهش می‌دهد. این روش در ذیل با یک مثال توضیح داده می‌شود:

رمز عبور Julia1984 را در نظر بگیرید. در حمله قدیمی جستجوی فراگیر، به یک مجموعه کاراکتر شامل تمامی حروف‌های بزرگ، کوچک و اعداد نیاز است. این رمز عبور ۹ کاراکتری و تعداد ترکیبات موجود برای پیدا کردن آن ۶۲۹ است. اگر با نرخ 100 ۹M/s حمله ماسک انجام شود، به زمانی بیش از ۴ سال برای پیدا کردن رمز عبور نیاز است.

در حمله ماسک مهاجمان از انسان‌ها و شیوه انتخاب رمز عبور توسط آن‌ها آگاه هستند. رمز عبور بالا با الگویی ساده و رایج تطابق دارد. این حمله به‌گونه‌ای قابل پیکربندی است که تنها حرف ابتدایی رمز را به صورت بزرگ جستجو کند. وجود حرف بزرگ در کاراکتر دوم یا سوم رایج نیست. با استفاده از حمله ماسک، پیدا کردن رمز عبور را می‌توان به ۲۳۷,۶۲۷,۵۲۰,۰۰۰ ترکیب کاهش داد که با نرخ 100 M/s حدود ۴۰ دقیقه زمان نیاز دارد.

1- Mask per second

۲-۲-۴ روش ادغام دو لغت‌نامه

در این روش هر کلمه از لغت‌نامه اول با تمامی کلمات لغت‌نامه دوم ترکیب می‌شود. به طور پیش‌فرض، لغات با یکدیگر ترکیب شده‌اند اما می‌توان تعداد ترکیبات احتمالی را با اضافه کردن Space، Underline و دیگر نشانه‌ها، بررسی ترکیبات حروف بزرگ یا کوچک و استفاده از تغییرات اضافی افزایش داد.

۲-۲-۵ روش هیبرید[10]

این روش یکی از جالب‌ترین روش‌های حمله است. این حمله مانند حمله ترکیب‌کننده است که یک طرف ترکیب لغت‌نامه و طرف دیگر آن نتایج حمله جستجوی فراگیر می‌باشد. به عبارت دیگر فضای‌کلید جستجوی فراگیر، یا به ابتدا یا به صورت مکمل به هر کدام از کلمات لغت‌نامه اضافه می‌شوند. به همین دلیل است که این روش، هیبرید نام دارد.

1- Hybrid

۳ جلوگیری از حملات جستجوی فراگیر

مهاجمان، حملات جستجوی فراگیر را با ابزارهایی شروع می‌کنند که از لیست کلمات و مجموعه قوانین هوشمند برای حدس خودکار رمز عبور کاربر استفاده می‌کنند. اگرچه چنین حملاتی به راحتی قابل تشخیص هستند، اما جلوگیری از آن‌ها کار آسانی نیست. برای مثال بسیاری از ابزارهای جستجوی فراگیر HTTP، می‌توانند درخواست‌ها را از طریق لیست سرورهای باز پراکسی، بازپخش کنند. به دلیل این‌که هر درخواست از IP متفاوتی حاصل می‌شود، مسدودسازی این حملات از طریق مسدودسازی آدرس IP امکان‌پذیر نیست.

۳-۱ مسدودسازی حساب‌های کاربری

واضح‌ترین راه برای مسدود کردن حملات جستجوی فراگیر، مسدودسازی حساب‌های کاربری بعد از تعداد تلاش‌های نادرست تعریف‌شده رمز عبور است. مسدودسازی حساب‌ها مدت زمان خاصی دارد (مانند یک ساعت یا تا زمان فعال‌سازی دوباره حساب توسط مدیر). بااین‌حال، مسدودسازی حساب همیشه بهترین راهکار نیست، به دلیل این‌که شخص می‌تواند به راحتی معیارهای امنیتی را دستکاری کرده و صدها حساب را مسدود کند. در واقع، برخی وب‌سایت‌ها حملات بسیاری را تجربه می‌کنند به‌گونه‌ای که قادر به اجرای سیاست مسدودسازی نیستند زیرا به طور مداوم مشغول فعال‌سازی حساب‌های کاربری هستند. مشکلات مسدودسازی حساب‌ها در زیر بیان شده‌اند:

- یک مهاجم می‌تواند از طریق مسدودسازی تعدادی زیادی از حساب‌ها، باعث بروز رد سرویس (DoS) شود.
- به دلیل اینکه نمی‌توان حساب کاربری که وجود ندارد را مسدود کرد، تنها نام‌های حساب‌های معتبر مسدود خواهند شد. یک مهاجم می‌تواند از این مسئله استفاده کرده و نام‌های کاربری را با توجه به واکنش‌های خطا، از سایت دریافت کند.
- یک مهاجم می‌تواند با مسدودسازی بسیاری از حساب‌ها و حمله به بخش پشتیبانی باعث جعل و نفوذ شود.
- یک مهاجم می‌تواند به طور مداوم یک حساب مشابه را حتی چند ثانیه بعد از فعال‌سازی مجدد توسط مدیر، غیرفعال کند که این کار حساب را عملاً از کار می‌اندازد.
- مسدودسازی حساب در مقابل حملات آهسته‌ای که در هر ساعت فقط چند رمز عبور را امتحان می‌کنند، غیرمؤثر است.

- مسدودسازی حساب در مقابل حملاتی که یک رمز عبور را برای تعداد بیشماری از نام‌های کاربری امتحان می‌کنند، غیرمؤثر است.
- اگر مهاجم از ترکیب نام‌کاربری / رمز عبور استفاده کند و در چند تلاش ابتدایی به نتیجه برسد، مسدودسازی حساب غیرمؤثر است.
- حساب‌های قدرتمند مانند حساب‌های مدیران غالباً سیاست مسدودسازی را دور می‌زنند، اما این حساب‌ها مطلوب‌ترین حساب‌ها برای حمله هستند. برخی سیستم‌ها، حساب‌های مدیران را براساس ورود به سیستم‌های مبتنی بر شبکه مسدود می‌کنند.
- حتی زمانی‌که حسابی را مسدود شود، حمله می‌تواند ادامه داشته باشد و منابع باارزش انسانی و کامپیوتری را مصرف کند.

گاهی اوقات مسدودسازی حساب مؤثر است، اما فقط در محیط‌های کنترل‌شده یا مواردی که خطر به اندازه‌ای بزرگ است که حتی حملات ادامه‌دار DoS نیز حساب را به خطر می‌اندازند. در اکثر موارد، مسدودسازی حساب برای جلوگیری از حملات جستجوی فراگیر کافی نیست. برای مثال، یک سایت مزایده را در نظر بگیرید که چندین پیشنهادکننده برای یک شئ مشابه بحث می‌کنند. اگر وب‌سایت مزایده سیاست مسدودسازی حساب‌ها را اجرا کند، یک پیشنهادکننده می‌تواند به راحتی حساب‌های دیگر پیشنهادکنندگان را در دقیقه آخر مزایده مسدود کرده و از موفقیت آن‌ها برای پیروزی در مزایده جلوگیری کند. یک مهاجم می‌تواند از تکنیکی مشابه برای مسدودسازی تراکنش‌های حیاتی مالی یا ارتباطات ایمیلی استفاده کند.

۳-۲ یافتن دیگر اقدامات متقابل

۳-۲-۱ تزریق تأخیر

همان‌گونه که مطرح شد، مسدودسازی حساب‌ها معمولاً راهکاری عملی نیست، اما روش‌های دیگری برای مقابله با حملات جستجوی فراگیر نیز وجود دارد. اولاً، به دلیل اینکه موفقیت این حمله به زمان وابسته است، تزریق توقف‌های تصادفی در زمان بررسی یک رمز عبور ساده‌ترین راهکار است. اضافه کردن توقف چند ثانیه‌ای می‌تواند تا حد زیادی حمله جستجوی فراگیر را آهسته کند.

این نکته شایان ذکر است که با وجود این‌که اضافه کردن تأخیر می‌تواند حمله تک‌رشته‌ای را آهسته کند، اما در صورتی‌که مهاجم به طور همزمان چندین درخواست اعتبارسنجی ارسال کند، اثرپذیری آن کاهش می‌یابد.

۳-۲-۲ مسدودسازی آدرس IP

راهکار دیگر مسدودسازی آدرس IP است که از طریق آن چندین تلاش ناموفق صورت گرفته است. اشکال این راهکار این است که ممکن است به صورت سهوی تعداد زیادی از کاربران از طریق مسدودسازی سرور پراکسی استفاده‌شده توسط یک ISP یا شرکت بزرگ، مسدود شوند. اشکال دیگر آن این است که ابزارهای بسیاری از لیست پراکسی‌ها استفاده می‌کنند و قبل از تغییر آدرس IP، فقط چند درخواست را از آدرس IP کنونی ارسال می‌کنند. با استفاده گسترده از لیست پراکسی‌های باز در دسترس، مهاجم می‌تواند به راحتی هر مکانیزم مسدودسازی IP را دور بزند. به دلیل این‌که اکثر سایت‌ها بعد از یک تلاش ناموفق رمز عبور، آدرس IP را مسدود نمی‌کند، مهاجم می‌تواند به ازای هر پراکسی دو یا سه تلاش انجام دهد. مهاجمی که لیست ۱۰۰۰ تایی پراکسی در اختیار دارد، می‌تواند ۲۰۰۰ یا ۳۰۰۰ رمز عبور را بدون این‌که مسدود شود امتحان کند. با وجود ضعف این روش، وب‌سایت‌هایی که حملات بیشماری را تجربه می‌کنند، حتماً مسدودسازی آدرس‌های IP پراکسی را انتخاب کنند.

۳-۳ تکنیک‌های دیگر

برای کاربران حرفه‌ای که می‌خواهند از حساب‌های خود در مقابل حمله محافظت کنند، گزینه‌ای در نظر گرفته شود تا به آنها اجازه دهد فقط از یک سری آدرس IP خاص وارد شوند.

مهاجمان غالبا می‌توانند بسیاری از این تکنیک‌ها را دور بزنند، با ترکیب چندین تکنیک، می توان حملات جستجوی فراگیر را محدود کرد. متوقف‌سازی یک مهاجم که برای به دست آوردن رمز عبور مصمم است، آسان نیست، اما این تکنیک‌ها می‌توانند در مقابل بسیاری از حملات از جمله مهاجمان تازه‌کار مؤثر باشند. همچنین این تکنیک‌ها نیازمند فعالیت بیشتر از سمت مهاجم است که به مدیر سایت فرصت بیشتری برای تشخیص حمله و احتمالا تشخیص مهاجم می‌دهد.

باوجود این‌که متوقف‌سازی کامل حملات جستجوی فراگیر مشکل است، تشخیص آن‌ها کار آسانی است به دلیل این‌که هر تلاش ورود ناموفق، یک کد حالت HTTP 401 در گزارش‌های وب سرور ثبت می‌کند. بررسی فایل‌های گزارش برای جلوگیری از حملات جستجوی فراگیر اهمیت بسیاری دارد.

۳-۴ شرایط احتمالی بیان‌کننده حمله جستجوی فراگیر

- تعداد زیاد ورود ناموفق به سیستم از طریق آدرس IP مشابه
- ورود به سیستم با چندین نام کاربری از طریق آدرس IP مشابه
- ورود به یک حساب از طریق چندین آدرس IP مختلف
- استفاده بیش از حد و مصرف پهنای باند در یک ورود به سیستم
- تلاش‌های ناموفق ورود به سیستم از طریق نام‌های کاربری و رمزهای عبور به ترتیب حروف الفبا
- ورود به سیستم از طریق URL ارجاع ایمیل یک شخص یا مشتری IRC
- ورود به سیستم‌هایی که دارای رمزهای عبور مشکوک هستند مانند ownsyou (ownzyou)

۳-۵ استفاده از عبارت امنیتی[11]

عبارت امنیتی برنامه‌ای است که به مدیران وب‌سایت‌ها اجازه می‌دهد فرق بین انسان و کامپیوتر را تشخیص دهند. در ابتدا به طور گسترده توسط موتور جستجوی AltaVista استفاده شد تا از ارسال‌های خودکار جستجو جلوگیری کند، عبارات امنیتی به شکل خاصی در جلوگیری از هرگونه سوءاستفاده خودکار از جمله حملات جستجوی فراگیر مؤثر هستند. این عبارات به‌گونه‌ای عمل می‌کنند که تعدادی آزمایش تصادفی را که برای انسان آسان ولی برای کامپیوتر مشکل است را فراهم می‌کنند؛ بنابراین می‌توانند به طور قطع نتیجه بگیرند که یک شخص در حال انجام آزمایش است.

برای این‌که یک عبارت امنیتی مؤثر باشد، اشخاص باید بتوانند تقریباً در ۱۰۰ درصد مواقع به آزمایش درست پاسخ دهند. کامپیوترها نیز نباید تقریبا در ۱۰۰ مواقع موفق شوند. رایج‌ترین نوع عبارت امنیتی استفاده‌شده، به کاربر کلمه مبهمی را نشان می‌دهد که کاربر باید آن را تایپ کند. یک عبارت امنیتی ساده می‌تواند در مقابل حملات جستجوی فراگیر مؤثر باشد.

1- CHAPTCHA: A Completely Automated Public Turing test to Tell Computers and Humans Apart.

۴ معرفی ابزارهای مناسب برای منع نفوذ از طریق درگاه SSH

۴-۱ تکنیک DenyHosts

DenyHosts یک ابزار امنیتی منع نفوذ مبتنی بر گزارش[۱۲] است. این ابزار به منظور جلوگیری از حملات جستجوی فراگیر روی سرورهای SSH از طریق بررسی تلاش‌های نامعتبر ورود به سیستم در گزارش اعتبارسنجی و مسدودسازی آدرس‌های IP مبدأ طراحی شده است.

۴-۲ نرم‌افزار Brute Force-Blocker

این نرم‌افزار یک اسکریپت به زبان پرل[۱۳] است که به همراه فیلترینگ بسته[۱۴] (PF) عمل می‌کند. هدف کلی این نرم‌افزار مسدودسازی حملات جستجوی فراگیر SSH از طریق دیوار آتش است. زمانی که اسکریپت در حال اجرا است، گزارش‌های ssh را از گزارش سیستمی (syslog) بررسی کرده و به دنبال تلاش‌های ناموفق ورود به سیستم می‌گردد. زمانی‌که IP ارائه‌شده به حد عدم موفقیت خود برسد، این اسکریپت IP را در جدول PF قرار داده و هرگونه ترافیک ارسالی به آن را مسدود می‌سازد.

۴-۳ نرم‌افزار Fail2ban

این نرم‌افزار فایل‌های گزارش را بررسی کرده و IPهایی که از خود رفتارهای مخرب مانند عدم موفقیت بسیار در وارد کردن رمز عبور و جستجو برای ابزارهای مخرب نشان می‌دهند را مسدود می‌سازد. در کل این نرم‌افزار برای به‌روزرسانی قواعد دیوار آتش بکار می‌رود تا بتواند آدرس‌های IP را برای مدت زمان مشخص مسدود کند.

Fail2ban قادر است تعداد تلاش‌های اعتبارسنجی‌های نادرست را کاهش دهد، هرچند نمی‌تواند خطر را به دلیل اعتبارسنجی ضعیف، برطرف سازد.

1- Log
2- Perl
3- Packet Filter

۴-۴ نرم‌افزار SSHGuard

SSHGurad میزبان‌ها را در مقابل حمله‌های جستجوی فراگیر علیه SSH و دیگر سرویس‌ها محافظت می‌کند. این نرم‌افزار گزارش‌های سیستمی را جمع‌آوری کرده و مهاجمان تکراری را که از یکی از عقبه‌های

دیوار آتش[15] پنل مدیریت از جمله iptables[16]، ipfw[17] و pf[18] استفاده می‌کنند را مسدود می‌سازد.

SSHGurad می‌تواند پیام‌های گزارش حاصل از ورودی استاندارد را بخواند یا یک یا چند فایل گزارش را بررسی کند. پیام‌های گزارش به صورت خط به خط برای الگوهای قابل تشخیص تجزیه و تحلیل می‌شوند. اگر یک حمله مانند چندین تلاش ناموفق ورود به سیستم در چند ثانیه تشخیص داده شود، IP مهاجم مسدود می‌شود. مهاجمان را می‌توان پس از دوره زمانی خاصی از بلاک خارج کرد اما می‌توان با استفاده از گزینه لیست سیاه آن‌ها را برای مدت نامعلوم مسدود کرد.

۵ منابع

1. A Study of Passwords and Methods Used in Brute-Force SSH Attacks Clarkson University
2. https://en.wikipedia.org/wiki/Brute-force_attack#Theoretical_limits
3. http://www.sshguard.net /
4. https://cs.virginia.edu/~csadmin/gen_support/brute_force.php
5. https://www.owasp.org/index.php/Blocking_brute_Force_Attacks
6. https://en.wikipedia.org/wiki/DenyHosts
7. http://www.fail2ban.org/wiki/index.php/Main_Page

1- Firewall Back ends
2- iptables: One of the base system firewalls
3- ipfw: One of the base system firewalls
4- pf: One of the base system firewalls