# صفحه: 1

HALIBOYS.COM  
  
NAMP cla ‏اسکربپت‎  
  
WWW.KALIBOYS.COM

# صفحه: 2

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
WWW.KALIBOYS.COM  
  
afp-path-vuln  
  
broadcast-avahi-dos  
  
clamav-exec  
distcc-cve2004-2687  
  
dns-update  
firewall-bypass  
  
ftp-libopie  
  
ftp-proftpd-backdoor  
  
ftp-vsftpd-backdoor  
  
ftp-vuln-cve2010-4221  
  
-CVE-2010-0533 «Mac OS X AFP (65555 pls ‏شناسایی آسیب‌پذیری پیمایش‎  
  
جستجو ‎Gly‏ پیدا کردن میزبان ها در شبکه ی محلی با استفاده از پروتکل ‎BES‏ سرویس ‎DNS‏ و  
ارسال یک بسته ی ‎NULL UDP‏ به هر میزبان برای آزمایش در صورتی که بسته ی انکار سرویس  
‎Avahi NULL UDP‏ آسیب پذیرباشد(07۳-2011-1002)).  
  
استفاده از سرورهای آسیب پذیر ‎cl» ClamAV‏ اجرای دستور ‎Clamav‏ نامعتبر است.  
  
شناسایی و استفاده از یک آسیب پذیری ‎oF‏ از ‎oly‏ دور در ‎daemon compiled distcc‏ این آسیب  
پذیری در سال ۲۰۰۲ منتشر ‎ad‏ اما هنوز هم در اجرای کنونی به ‎elo‏ پیکربندی نادرست سرویس  
وجود دارد.  
  
تلاش برای به روز رسانی ‎DNS‏ پویا بدون احراز هوبت.  
  
شناسایی آسیب پذیری در ‎netfilter‏ و ‎So‏ فایروال ها که از برنامه های کمکی برای پورت های باز  
پویا برای پروتکل ‎ole‏ مانند ‎Sip ftp‏ استفاده می‌کنند.  
  
بررسی اینکه ‎FTPd‏ متمایل ‎a,‏ ۷۳-2010-1938)(سرریز پشته جدا از یک 0۳|۴)» آسیب پذیری  
‎cul‏ که توسط ‎Maksymilian Arciemowicz‏ و ‎Adam "pi3" Zabrocki‏ شناسایی شده  
است. برای راهنمایی ‎https://nmap.org/t/fbsd-sa-opie‏ رامشاهده کنید. توصیه می‌شود که اگر  
  
بر ضد میزبان آسیب‌پذیر ‎og Lol‏ این ‎FTP cay Sal‏ را تخریب خواهد کرد.  
  
معیارهایی برای وجوددرب پشتی 1.3.360 ‎ProOFTPD‏ به عنوان 69562 ‎OSVDB-ID‏ گزارش شده  
است. این اسکریپت به‌طور پیش فرض اقداماتی را برای به کارگیری درب‌پشتی از فرمان 0[ بی-  
خطراستفاده می کند. اما می تواند با آرگومان‌های اسکریپت ‎pwsiftp-proftpd-backdoor.cmd‏  
‏کند.  
  
معیارهایی برای وجود درب‌پشتی 2.3.4 ‎vSFTPd‏ در 2011-07-04 گزارش شده است-07۳))  
(2011-2523. این اسکریپت به‌طور پیش فرض اقداماتی را برای به کارگیری مخفیانه از فرمان 10  
بی‌خطراستفاده می ‎eS‏ اما می تواند با آرگومان‌های اسکریپت ‎exploit.cmd‏ یا ‎ftp-vsftpd-‏  
‏40 تقتغییر کند.  
  
بررسی ‎Gly‏ سرریز بافر ‎ee‏ » پشته در سرور ‎PrOFTPD‏ « اسخهی ‎cys‏ 1.32703 و 1.3:30: پا  
ارسال تعداد زیادی از رشته‌ی ‎alee TELNET\_IAC ECS‏ اشتباه فرآیند ‎Jsbproftpd‏ بافر و  
یک مهاجم از راه دور می‌تواند پشته را ‎pas‏ دهد و کد دلخواه را درمحدوده‌ی فرآیند ‎proftpd‏ اجرا  
کند(2010-4221-:0۹7۳)) . احراز هویت برای به‌کارگیری از این آسیب پذیری لازم نیست.

# صفحه: 3

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
http-adobe-coldfusion-  
apsal301  
  
http-aspnet-debug  
  
http-avaya-ipoffice-users  
  
http-awstatstotals-exec  
  
http-axis2-dir-traversal  
  
http-cookie-flags  
  
http-cross-domain-policy  
  
http-csrf  
http-dlink-backdoor  
  
http-dombased-xss  
  
http-enum  
http-fileupload-exploiter  
  
http-frontpage-login  
  
WWW.KALIBOYS.COM  
  
اقداماتی برای به‌ کارگیری از آسیب پذیری ‎olf AF‏ احراز ‎Cage‏ در سرورهای ‎Adobe Coldfusion‏  
‎Gly‏ بازیابی مدیریت معتبر کوکی نشست است.  
  
تعیین ‎LT aS!‏ برنامه‌ی ‎ASP.NET‏ دارای اشکال زدایی با استفاده از یک درخواست ‎DEBUG‏  
‏۳ آاست.  
  
Avaya IP Office systems 7.x 0 ‏اقداماتی برای شمارش کاربران‎  
  
به‌کارگیری آسیب‌پذیری اجرایی کد از ‎oly‏ دور در 1.0 ‎Awstats Totals‏ تا 1.14 و احتمالا ‎ple‏  
‏محصولات مبتنی بر آن(2008-3922 ‎(CVE:‏ .  
  
به‌کارگیری آسیب پذیری ‎Glen‏ دایرکتوری در ‎Apache Axis2‏ نسخه‌ی 1.4.1 با ارسال یک  
درخواست خاص به پارامتر84< ‎(OSVDB-59001)‏ به طور پیش‌فرض, برای بازیایی فایل  
پیکربندی سرویس ‎Yconf/axis2.xml'‏ با استفاده از مسیر ‎ly /axis2/services/'‏ بازگشت نام  
کاربری و گذرواژه حساب کاربری تلاش خواهد کرد.  
  
برزسی ‎lai SoS‏ توسط سرویس‌های ‎HTTP‏ تتطیم سی‌شنوند. گزارشاتی خر مورق هر ‎lS‏ ]5 کوکی‌های  
نشست بدون پرچم ‎httponly‏ وجود دارد. گزارشاتی در مورد هر کدام از کوکی‌های نشست. در  
سرتاسر ‎SSL‏ بدون پرچم امن به کار برده می‌شود. اگر ‎http-enum.nse‏ نیز ‎Lol‏ شودء هر مسیر  
جالبی که توسط آن پیدا می شود علاوه بر ‎Hy‏ بررسی می شود.  
  
‎pla‏ سیاستی دامنه‌ی مقابل ‎(/crossdomain.xml)‏ و فایل سیاست دسترسی مشتری  
‎(clientaccesspolicy.xml/)‏ را در برنامه ‎cle‏ وب بررسی کرده و دامنه های قابل اعتماد را لیست  
می کند. تنظیمات مجاز بیش‌|زحد» می‌تواند سیب حملات جعل درخواست از سایت دیگر شود و ممکن  
‎Cul‏ به مهاجمان اجازه دسترسی به داده‌های حساس را بدهد. این اسکریپت برای شناسایی تنظیمات  
مجاز و قابل استفاده اسامی‌دامنه محتمل برای خرید به ‎glare‏ به‌کارگیری برنامه‌هاء قابل‌استفاده است.  
شناسایی درب‌پشتی میان‌افزار برروی برخی روترهای ‎D-Link‏ با تغییرعامل کاربر به یک مقدار  
"سری". به‌کاربردن "سری" ‎ole‏ کاربری احرازهویت را کنارگذاشته و اجازه دسترسی مدیر به روتر را  
به دنبال مکان‌هایی است که اطلاعات تحت کنترل مهاجم در ‎DOM‏ ممکن ‎Gly Cul‏ تاثیر بر اجرای  
جاوا اسکریپت به روش‌های خاصی مورد استفاده قرار گیرد .این حمله در اینجا توضیح داده شده‌است:  
‎http://www.webappsec.org/projects/articles/071105.shtml‏  
  
‏شمارش دایرکتوری‌های به کار رفته توسط برنامه‌های رایج وب و سرورها.  
  
‏فرم‌های آپلود فایل بی‌اعتبار در برنامه های وب با استفاده از تکنیک های مختلف مانند تغییر سرآیند  
نوع‌محتوا يا ایجاد فایل ‎Ge‏ تصویری معتبر بسته‌های اطلاعاتی در ‎aly‏ را به کارمی گیرد.  
  
‏بررسی اینکه ‎LI‏ ماشین‌های هدف برای ورود فرانت‌پیج ناشناس» آسیب‌پذیر هستند یا خیر.

# صفحه: 4

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
http-git  
  
http-huawei-hg5xx-vuln  
  
http-iis-webdav-vuln  
  
http-internal-ip-disclosure  
  
http-jsonp-detection  
  
http-litespeed-sourcecode-  
download  
  
http-majordomo2-dir-  
traversal  
  
http-method-tamper  
  
http-passwd  
  
http-phpmyadmin-dir-  
traversal  
  
http-phpself-xss  
  
http-shellshock  
  
http-slowloris-check  
http-sql-injection  
  
WWW.KALIBOYS.COM  
  
بررسی برای یافتن منبع ‎Git‏ سند وبسایت ‎root /.git/<something>)‏ و بازیابی اطلاعات پس-  
گرفته‌شده تاحدامکان, از جمله زبان / چارچوب. راه‌های‌دورء آخرین ‎pls‏ فرستاده‌شده و شرح منبع.  
شناسایی مودم‌های ‎Huawei‏ مدل‌های ‎HG520x HG530x‏ 105107 آ(و احتمالاً  
  
‎college pele‏ اسیب ,بیرق ‎jbael‏ رآقور واقهای ‎at desl Gleb!‏ همخنین اقتبار  
5و دیگر مقادیر پیکربندی موردنظر را برمی‌گزیند.  
  
‏بررسی ‎lp‏ آسیب‌پذیری 5.1/6.0 ‎TIS‏ که ‎a‏ کاربران دل‌خواه اجازه دسترسی به فایل‌های  
۷ ایمن را با جستجو ‎a‏ دنبال پوشه‌ی محافظت شده با ‎joy‏ عبور و تلاش ‎sly‏ دسترسی به  
آن را می‌دهد. این ‎uel‏ پذیری در بیانیه‌ی امنیتی مایکروسافت ‎‘MS09-020‏  
‎https://nmap.org/t/ms09-020‏ قرار گرفته است.  
  
‏تعیین می کند که ‎LT‏ سرور وب هنگام ارسال درخواست 1.0 / ‎HTTP‏ بدون سرآیند میزبان» آدرس  
‎IP‏ داخلی خود را از افشا می کند.  
  
‏تلاش برای یافتن نقاط انتهایی ‎ISONP‏ در سرورهای وب. نقاط انتهایی ‎ISONP‏ می تواند ‎Gly‏  
‏عبور از محدودیت ‎gle‏ سیاستی خاستگاه مشترک در مرورگرهای وب استفاده شود.  
  
‏به کارگیری آسیب‌پذیری مسموم ‎Cob‏ صفر در ‎Litespeed Web Servers 4.0.x‏ قبل از 4.0.15  
برای بازیابی کد منبع اسکریپت هدف با ارسال یک درخواست ‎HTTP‏ با یک بایت صفر به دنبال یک  
پسوند فایل ‎(CVE-2010-2333) .txt‏  
  
‏به‌کارگیری اسیب پذیری پیمایش موجود در ‎Majordomo?2‏ برای بازیابی فایل‌های راه‌دور. ‎(CVE-‏  
‏(2011-0049.  
  
‏تلاش برای عبور از منابع حفاظت شده ی گذرواژه(وضعیت 401 ‎CATTP‏ با دستکاری کلمه‌ی  
0 انجام می‌شود. اگر آرایه ای از مسیر ها برای بررسی تعیین نشده ‎Sb‏ سرور وب را جابه‌جا  
خواهد کرد وبررسی در برابر هر منبع حفاظت شده گذرواژه که آن را پیدا می ‎UT‏ انجام می دهد.  
بررسی می‌کند که آیا سرور وب در برابر پیمایش دایرکتوری» با تلاش برای بازیابی ‎/ete/passwd‏ يا  
‎\boot.ini‏ آسیب‌پذیر است یا خیر.  
  
‏به‌کارگیری آسیب پذیری پیمایش دایرکتوری در 2.6.4-011 ‎syphpMyAdmin‏ احتمالا سایر نسخه  
ها) برای بازیابی فایل ‎GE‏ راه‌دور در سرور وب.  
  
‏جابه‌جایی سرور وب و تلاش برای یافتن آسیب‌پذیری فایل‌های ۳11۳برای عبور معکوس اسکریپت  
نویسی در ‎cole‏ از طریق متغیر ‎$\_SERVER["PHP\_SELF"]‏  
  
‏تلاش برای به‌کارگیری از آسیب پذیری ‎CVE-2014-6271) "shellshock"‏ و ‎CVE-2014-‏  
‏7169( در برنامه های وب.  
  
‏معبارهای سرور وب برای ‎uel‏ پذیری به حمله ‎Slowloris DoS‏ بدون انجام حمله ‎DOS‏  
‎cle Spider‏ یک سرور ‎HTTP‏ به دنبال ‎URL‏ هایی است که حاوی ‎Cel‏ پذیری درخواست ها  
برای حمله تزریق ‎SQL‏ است.

# صفحه: 5

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
http-stored-xss  
http-tplink-dir-traversal  
  
http-trace  
  
http-vmware-path-vuln  
  
http-vuln-cve2006-3392  
http-vuln-cve2009-3960  
  
http-vuln-cve2010-0738  
  
http-vuln-cve2010-2861  
  
http-vuln-cve2011-3192  
  
http-vuln-cve2011-3368  
  
http-vuln-cve2012-1823  
  
http-vuln-cve2013-0156  
  
WWW.KALIBOYS.COM  
  
رفع فیلتر "<(علامت بزرگتر. نشانه‌ای از آسیب‌پذیری 698 (پنهانی.  
به‌کارگیری آسیب‌پذیری پیمایش دایرکتوری موجود در چندین روتر بی‌سیم ‎TP-LInk‏ مهاجمان  
ممکن است از این آسیب‌پذیری برای خواندن هر کدام از فایل‌های پیکربندی و رمز عبور از راه دور و  
بدون احراز هویت استفاده کنند.  
درخواست ‎JLo)! TRACE HTTP‏ نموده و نشان می‌دهد که آیا متد ‎JLITRACE‏ شده‌است یا  
خیر. اگر اشکال‌زدایی فعال ‎wb‏ فیلدهای سرآیندی را که درپاسخ تغییر کرده اند را باز می‌گرداند.  
بررسی برای آسیب‌پذیری ‎Golan‏ مسیر در ‎ESXi VMWare ESX‏ و 0 55 ‎(CVE-2009-‏  
‏)3733  
‏به‌کارگیری افشای فایل در ‎(CVE-2006-3392) Webmin‏  
به‌کارگیری ‎cve-2009-3960‏ ونیز با عنوان ‎Adobe XML External Entity Injection‏  
بررسی اینکه آیا هدف ‎JBoss‏ برای عبور از احراز هویت کنسول ‎JMX‏ آسیب پذیر ‎(CVE-cxel‏  
‏(2010-0738.  
‏اجرای حمله ‎Glew‏ دایرکتوری دربرابر سرور 0014۳8101 و تلاش برای درهم کردن گذرواژه را  
برای کاربر مدیر. سپس استفاده از مقدار بیشتری(مخفی در صفحه وب) برای درهم کردن ‎SHALL‏  
‎HMAC‏ ایجاد می‌کند که سرور وب برای احراز هویت به عنوان ‎pre‏ نیاز دارد. ‎Lad‏ می توانید این  
مقدار را به سرور ‎ColdFusion‏ به عنوان ‎de‏ بدون شکستن درهم‌ریختگی رمز عبور منتقل کنید.  
شناسایی آسیب‌پذیری ‎ISI‏ سرویس در روشی که سرور وب ‎Apache‏ درخواست برای چند دامنه  
ساده/ مشترک یک ‎amie‏ )| کنترل می‌کند.  
معیارهایی برای آسیب‌پذیری 11-2011-3368/-)(گذرگاه پروکسی معکوس) در حالت پروکسی  
معکوس سرور ‎cy Sul Apache HTTP‏ ۳ معیار را اجرا خواهد کرد:  
\* معیار ‎Lloopback‏ ۳ بسته‌اطلاعاتی برای کنترل قوانین بازنویسی شده متفاوت  
\* معیار میزبان‌های ‎bb‏ با توجه به ‎Contextis‏ ما انتظار یک تاخیر قبل‌از ‎Glas‏ سرور را  
داریم.  
‎sae ©‏ وب سایته‌هارجی ان با این ‎Coad baw‏ که قمامی توائیةباد یک 18 شتیکه محلی  
‎yo baled Lay, mega’‏ هر ‎I‏ این یک مساله مرقط است:  
شناسایی نصب ‎PHP-CGT‏ که برای ‎CVE-2012-1823‏ آسیب پذیر ‎cool‏ این آسیب پذیری  
  
بحرانی به مهاجمان اجازه می دهد تا کد منبع را بازیابی و کد را از راه دور اجرا کنند.  
شناسایی آسینبه پذیری سرورهای ‎sly Ruby on Rails‏ تزریق ‎eet‏ اجرای دستورات از ‎Aly‏ دور و  
حملات انکار ‎(CVE-2013-0156) yrs poo‏ ۰

# صفحه: 6

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
http-vuln-cve2013-6786  
  
http-vuln-cve2013-7091  
http-vuln-cve2014-2126  
  
http-vuln-cve2014-2127  
  
http-vuln-cve2014-2128  
  
http-vuln-cve2014-2129  
  
http-vuln-cve2014-3704  
  
http-vuln-cve2014-8877  
  
http-vuln-cve2015-1427  
  
http-vuln-cve2015-1635  
  
http-vuln-cve2017-  
1001000  
  
http-vuln-cve2017-5638  
  
http-vuln-cve2017-5689  
  
http-vuln-cve2017-8917  
  
http-vuln-misfortune-  
cookie  
  
WWW.KALIBOYS.COM  
  
شناسایی تغییر مسیر ‎g URL‏ آسیب پذیری ‎XSS‏ در سرور وب 0 ‎Allegro RomPager ys‏ . این  
آسیب‌پذیری در ‎CVE-2013-6786‏ اختصاص یافته‌است.  
  
\*روز در تاریخ ۶ دسامبر ۲۰۱۳ توسط 1130112119 منتشر شد و در 7.2.6 ‎Zimbra‏ اصلاح شد.  
شا ‎LT acy‏ تجهیزات ‎Cisco ASA‏ برای افزایش ویژه‌ی آسیب‌پذیری ۸5۸ ‎Cisco‏  
  
.(CVE-2014-2126) 5 & cul ‏آسیب‌پذیر‎ 1  
  
Cisco ASA SSL ‏افزایش ویژه‌ی آسیب‌پذیری‎ Gl» Cisco ASA ‏تجهیزات‎ LI ‏ینکه‎  
‎. (CVE-2014-2127) > ‏آسیب‌پذیر است یا‎ VPN  
  
شناسایی ینکه آیا تجهیزات ۸5۸ ‎Cisco‏ برای عبور از احراز هویت آسیب‌پذیری ‎Cisco ASA‏  
‎SSL VPN‏ آسیب‌پذیر ‎col‏ یا 15 ‎.(CVE-2014-2128)‏  
‏شناسایی اینکه ‎LT‏ تجهیزات ‎Cisco ASA‏ برای انکارسرویس آسیب‌پذیری ‎Cisco ASA SSL‏  
  
. (CVE-2014-2129) 5 & ‏آسیب‌پذیر است‎ VPN  
‏شنلخته می‌شود.‎ Drupal ‏در‎ 'Drupageddon' ‏و نیز با عنوان‎ CVE-2014-3704 ‏به‌کارگیری‎  
  
نسخه‌های 7.32 > از هسته [102(آنیز تحت‌تاثیر قرار خواهند گرفت.  
  
CM ‏در پلاگین مدیریت‎ (CVE-20 14-8877) ‏آسیب‌پذیری تزریق کد از راه دور‎ CHF Wa  
‏که شناخته شده اند تحت تاثیر قرار می گیرند.‎ <= 2.0.0 cle ‏وردپرس. نسخه‎  
  
این اسکریپت تلاش می کند تا یک آسیب پذیری را شناسایی ‎CVE-2015-1427 es‏ که به  
مهاجمان اجازه می دهد تا ویژگی های وسیله‌ی نفوذ این ‎APT‏ را برای به دست آوردن اجرای کد از راه  
دور غیرمجازاستفاده کنند(۴ع6) =  
  
بررسی ‎cle‏ آسیب‌پذیری اجرای کد از راه دور(8/1515-034) در سیستم های ویندوز مایکروسافت  
‎(CVE2015-2015-1635)‏  
  
تلاش برای شناسایی آسیب‌پذیری افزایش ویژه در وردپرس 4.7.0 و 4.7.1 که & کاربران غیرمجاز,  
اجازه تزریق محتوا در پست‌ها را می‌دهد.  
  
شناسایی ‎Gare URL Ul ase!‏ شده برای آسیب‌پذیری اجرای کد از ‎ol,‏ دور ‎Apache Struts‏  
آسیب‌پذیر است با > ‎.(CVE-2017-5638)‏  
  
شناسایی اینکه آیا سیستم باتکنولوژی مدیریت فعال داخلی ‎Gly‏ افزایش ویژه‌ی آسیب‌پذیری  
‎INTEL-SA-00075‏ آسیب‌پذیر است یا >. ‎.(CVE2017-5689)‏  
  
آسیب‌پذیری تزریق ‎ASSQL‏ بر جوملا ‎I‏ می‌گذارد! .3.7 قبل از 3.7.1 اجازه می‌دهد تا کاربران  
غیرمجاز دستورها ‎SQL‏ دل‌خواه را اجرا کنند. این آسیب‌پذیری ناشی از یک جز جدید. که در نسخه  
۰ معرفی شد.ء در دسترس عموم قرار گرفت. که به این معنی است که می توان آن را توسط هر فرد  
مخربی که از ‎Cole‏ بازدید ‎MT ge‏ مورد بهره‌برداری قرار داد.  
  
شناسایی آسیب‌پذیری کوکی ‎RomPager 4.07 Misfortune‏ توسط به‌کا رگیری ایمن ‎Ol‏

# صفحه: 7

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
http-vuln-wnr1000-creds  
  
http-wordpress-users  
  
ipmi-cipher-zero  
irc-botnet-channels  
irc-unrealircd-backdoor  
  
mysql-vuln-cve2012-2122  
netbus-auth-bypass  
  
uppet-naivesignin:  
  
qconn-exec  
  
rdp-vuln-ms12-020  
realvnc-auth-bypass  
  
rmi-vuln-classloader  
  
rsa-vuln-roca  
samba-vuln-cve-2012-  
1182  
  
smb-double-pulsar-  
backdoor  
  
WWW.KALIBOYS.COM  
  
یک آسیب پذیری در سری 1000 ‎WNR‏ کشف شده است که به مهاجم اجازه می دهد تا مجوزهای  
مدیریت را با ‎Lil‏ روتر بازیابی کند. تست شده برروی نسخه‌ی نرم‌افزار(ها)ی دائمی:  
  
6 \_۷1.0.2.60(آخرین) و ‎V1.0.2.54\_60.0.82NA‏  
  
شمارش کاربران در نصب وردپرس ‎blog/CMS‏ با به‌کارگیری آسیب‌پذیری افشاء اطلاعات موجود در  
نسخه‌های 2.6 3.1 3.1.1 3.1.3 و ‎3.2-beta2‏ و احتمالات دیگر.  
  
‎cle‏ آسیب‌پذیری عبور از احرازهویت توسط استفاده از به‌رمز درآوردن صفر.  
  
‏بررسی سرور ‎IRC‏ برای کانال‌هایی که معمولا برای بات‌نت‌های مخرب استفاده می‌شوند.  
  
‏بررسی ‎IRC go 5 Sal‏ با اچرای قربان برسهای ‎(PING) Gly‏ وبررسی ‎Job pie Sal‏  
می‌کشد تا واکنش نشان ‎ABO‏ درب‌پشتی می‌شود.  
  
‏بررسی ‎a!‏ آیا سرور ‎NetBus‏ برای آسیب‌پذیری عبور احرازهویت که اجازه دسترسی کامل بدون  
دانستن گذرواژه را می دهد: آسیب‌پذیراست:  
شناسایی ‎LI ase!‏ امضای‌خام برروی سرور ‎puppet‏ فعال است. این ‎yal‏ مهاجمان را قادر می‌سازد تا هر  
گونه درخواست امضای گواهی را ایجاد کرده و آن را امضا کرده و به آن‌ها اجازه جعل بعنوان ‎ole‏  
  
‏1 داده شود. این می تواند پیکربندی عوامل و همچنین هر گونه اطلاعات حساس دیگر موجود  
تلاش برای شناسایی این که آیاروح ‎QNX QCONN‏ استماع به کاربران غیرمجازاجازه می‌دهد تا  
دستورها سیستم غملکردی دل‌خواه را اجرا کنند.  
  
‏بررسی ‎LI aXe!‏ دستگاه دربرابر ‎MS12-020 RDP‏ آسیب‌پذیر است.  
  
‎(CVE-2006-c.0! pds Quel RealVNC ‏برای دور زدن احراز هویت‎ WNC ‏یک سرور‎ LI  
.2369(  
  
‏معیارهایی مبنی بر این که ‎Java rmiregistry‏ اجازه دانلود ‎GUS‏ را می‌دهد. پیکربندی پیش فرض  
‎ojleIrmiregistri‏ می دهد تا کلاس ها را از ‎cle URL‏ از ‎ol,‏ دور دانلود ‎AUS‏ که می تواند به  
اجرای کد از راه دور منجر شود. فروشنده ‎(Oracle/Sun)‏ این را به عنوان یک ویژگی طراحی طبقه  
بندی می کند.  
  
‏شناسایی آسیب‌پذیری کلید ‎RSA‏ دربرابر حمله‌ی فاکتورگیری برای بازیابی کلیدهای خصوصی  
‎(ROCA)‏  
  
‏بررسی اینکه ‎LT‏ ماشین‌های هدف ‎ply jo‏ آسیب‌پذیری سرریز پشته ی سامبا ‎CVE-2012-1182‏  
  
‏بررسی اینکه آیا ماشین‌هدف در ‎Double Pulsar SMB‏ اجرا می‌شود.

# صفحه: 8

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
smb-vuln-conficker  
  
smb-vuln-cve-2017-7494  
  
smb-vuln-cve2009-3 103  
  
smb-vuln-ms06-025  
  
smb-vuln-ms07-029  
  
smb-vuln-ms08-067  
  
smb-vuln-ms10-054  
  
smb-vuln-ms 10-061  
  
smb-vuln-ms17-010  
  
smb-vuln-regsvc-dos  
  
smb-vuln-webexec  
  
smb2-vuln-uptime  
  
smtp-vuln-cve2010-4344  
  
smtp-vuln-cve2011-1720  
  
WWW.KALIBOYS.COM  
  
شناسایی سیستم‌های ویندوز مایکروسافت که توسط ‎Conficker Worm‏ آلوده می‌شوند. ‎cpl‏ بررسی  
‎SU‏ است وهعکن است سیستم ها رواب کند.  
  
‎yy‏ اینکه ‎LT‏ دستگاه‌های ‎Gow‏ در ‎ply‏ آسیب‌پایری:پارگذاری کتابخانه اشنتراکنی دل‌خواه:-078)  
2017-7494 آسیب‌پذیر هستند.  
  
‏شناسایی آسیب‌پذیری سیستم‌های ویندوز مایکروسافت برای انکار ‎(CVE-2009-3103) nrg po‏  
  
‏این اسکریپت. اگر آآسیب‌پذیر باشد» این سرویس را خراب خواهد کرد.  
شناسایی سیستم‌های ویندوز مایکروسافت با سرویس ‎Ras RPC‏ دربرابر ‎pec) MS06-025‏  
شناسایی سیستم‌های ویندوز مایکروسافت با ‎Dns Server RPC‏ دربرابر ۸/507-029 آسیب‌پذیر  
  
‏شناسایی آسیب‌پذیری سیستم‌های ویندوز مایکروسافت دربرابر آسیب‌پذیری اجرای کد از راه‌دور  
شناخته شده به ‎siete‏ ۸808-067 این برزسی خطرناک است و ممکن است سیستم ها ‎Uy‏ خزاب  
کند.  
  
‏معیارهایی که ‎LT‏ دستگاه‌های هدف دربرابر آسیب‌پذیری تخریب حافظه از راه‌دور ‎ams10-054 SMB‏  
  
‏معیارهایی که ‎LT‏ دسگاه‌های هدف دربرایر آسیب‌پذیری جعل هماهنگ‌کننده‌ی ‎Sle‏ 2810-061  
تلاش برای شناسایی این که ‎LT‏ سرور 58/18۷1 مایکروسافت در برابر یک آسیب‌پذیری اجرای کد از  
‎ol,‏ دور آسیب‌پذیر است(۳:۳011۵1[۳116 ‎a.k.a.‏ ,7-010 1281) . این آسیب‌پذیری به طورفعال توسط  
‎WannaCry‏ و ‎Petya ransomware‏ و سایر بدافزارها مورد استفاده قرارمی گیرد.  
  
‏مسیاأرقایی که ‎bl‏ وینذوژ + ‎e+‏ مایکروسافت:ذربرایز تغریب فر ‎fole‏ 1688۷08 توسط, ‎Ele ,| pac‏ آشاره-  
آسیب‌پذیری اجرای ‎oF‏ از ‎ol,‏ دور بحرانی در ‎(WebExec) WebExService‏ وجود دارد.  
  
‏تلاش برای شناسایی ‎POLLS‏ دست رفته در سیستم های ویندوز توسط بررسی بازگشت زمان‌فعالیت  
آپدیت در طول مذاکره پروتکل 52/2 .  
  
‏بررسی و/ یا به‌کارگیری سرریز پشته در نسخه‌هایی از ‎Exim‏ قبلی تا نسخه‌ی 4.69 ‎(CVE-2010-‏  
‏)4344 و افزایش آسیب‌پذیری ویژه در 4.72 ‎Exim‏ و قبل از 51 ‎(CVE-2010-4345)‏  
  
‎oy yp‏ خرایی ‎abs‏ در سرور ‎Postfix SMTP‏ هنگام استفاده از مکانیزم‌های احراز هویت کتابخانه  
‎(CVE-2011-1720) Cyrus SASL‏ این آسیب پذیری می تواند امکان ‎ISI‏ سرویس و احتمالا  
  
‏اجرای کد از راه دور را بدهد.

# صفحه: 9

معرفی تمامی اسکریپت ‎(cle‏ ابزار ‎NMAP‏  
  
smtp-vuln-cve2011-1764  
  
ssl-ccs-injection  
  
ssl-cert-intaddr  
  
ssl-dh-params |  
  
ssl-heartbleed  
  
ssl-known-key  
  
ssl-poodle  
sslv2-drown  
  
supermicro-ipmi-conf  
  
tls-ticketbleed  
  
wdb-version  
  
WWW.KALIBOYS.COM  
  
‎Se‏ کردن آسیب پذیری رشته فرمت در سرور ‎Exim SMTP‏ (نسخه‌ی 4.70 تا 4.75 با پشتیبانی  
‎(CVE-2011-1764) DomainKeys Identified Mail (DKIM)‏ مکانیزم ثبت ‎DKIM‏  
‏هنگام مشخص‌کننده‌های قالب ‎ay‏ ثبت برخی از قسمت‌های فیلد سرآیند ‎DKIM-Signature‏ را  
‎Oy cod Fas‏ مهاجم ازراه دور که قادر به ارسال ‎ros!‏ است. می‌تواند از این آسیب‌پذیری بهره‌برداری  
کرده ‎uF‏ دلخواه را با امتیازات ‎Daemon Exim‏ اجرا کند.  
  
‏شناسایی ‎LI aXe!‏ سرور دربرابر آسیب‌پذیری "تزریق ‎SSL/TLS "CSS‏ آسیب‌پذیری  
  
‏است ‎(CVE-2014-0224)‏ اولین‌بارتوسط ‎Masashi Kikuchi‏ کشف شد. این اسکریپت برپایه‌ی  
‎ccsinjection.c os‏ توسط ‎Ramon de C Valle‏ نوشته‌شده-  
‎(https://gist.github.com/revalle/71£4b027d61a78c42607) cu!‏  
  
‏گزارش هر 1۳۷4 خصوصی ‎(RFC1918)‏ که در زمینه ‎cle‏ مختلف یک گواهی سرویس ‎SSL‏ یافت  
می شود. این موارد تنها در صورتی گزارش می‌شوند که خود آدرس هدف خصوصی نباشد. ‎Nmap‏  
‏0 یا بالاتر مورد نیاز است.  
  
‏شناسایی پارامتر ‎Diffie-Hellman‏ ناپایدار ‎oly‏ خدمات ‎SSL/TLS‏  
  
‏شناسایی ‎Sel‏ آیا سرور دربرابر خطای ‎OpenSSL Heartbleed‏ آسیب ‎(CVE-2014- cus! pi:‏  
(0160. این ‎oF‏ براساس اسکریپت پایتون ‎ssltest.py‏ توسط ‎by Jared Stafford‏ نوشته‌شده -  
است ‎(jspenguin@jspenguin.org)‏  
  
‏بررسی می‌کند که آیا گواهی ‎SSL‏ که توسط یک میزبان استفاده می‌شود دارای انگشت‌نگاری است  
‎ols a5‏ پایگاه‌دادای, ستشکل از کلین‌های مشکن‌داز اس  
  
‏بررسی می‌کند که ‎LI‏ رمزنگاری ‎SSLV3 CBC‏ مجاز است(آ۳001).  
  
‏تعیین اینکه ‎LI‏ سرور از ‎SSLV2‏ پشتیبانی می‌کند. از چه نوع رمزنگاری پشتیبانی ‎gS ce‏  
معیارهایی برای ‎CVE-2016-0703 CVE-2015-3197‏ و ‎CVE-2016-0800‏  
‎(DROWN)‏  
  
‏تلاش برای بارگیری فایل پیکربندی محافظت نشده حاوی اعتبارنامه کاربرمتن ساده برحسب کنترل-  
کنندگان ‎Cow! Supermicro Onboard IPMI‏ پذیراست.  
  
‏شناسایی اینکه آیا سرور در برابر ‎Ticketbleed cles‏ ۳5 آسیب پذیر است.  
  
‏شناسایی آسیب‌پذیری و جمع‌آوری اطلاعات(مانند شماره‌های نسخه و پشتیبانی سخت‌افزار) از عوامل  
‎.VxWorks Wind DeBug‏  
  
‎https://nmap.org/nsedoc/categories/vuln.html  
‎https://kaliboys.com/nmap-scripts/