



macOS Hacking Tricks

\$Whoami



Ricardo L0gan

Security Specialist with over 15 years of experience, malware research enthusiastic, pentest and reverse engineering. I've a solid knowledge on topics like network security, hardening and tuning across multiple platforms such as Windows, Linux, OS X and Cisco. Beginner in programming languages as Python, C and Assembly.

In Brazil, I contribute with some security conferences organizations such as SlackShow Community, bSides SP and Hackers to Hackers Conference (H2HC).



Long live Open Source - Use Linux (Slackware)



macOS Hacking Tricks



Agenda

0x00 Motivation of Research

0x01 macOS Security Characteristics

0x02 Hacking macOS target

0x03 Hacking macOS target + Demo

0x04 macOS Tools

0x05 Reference

0x06 Conclusion

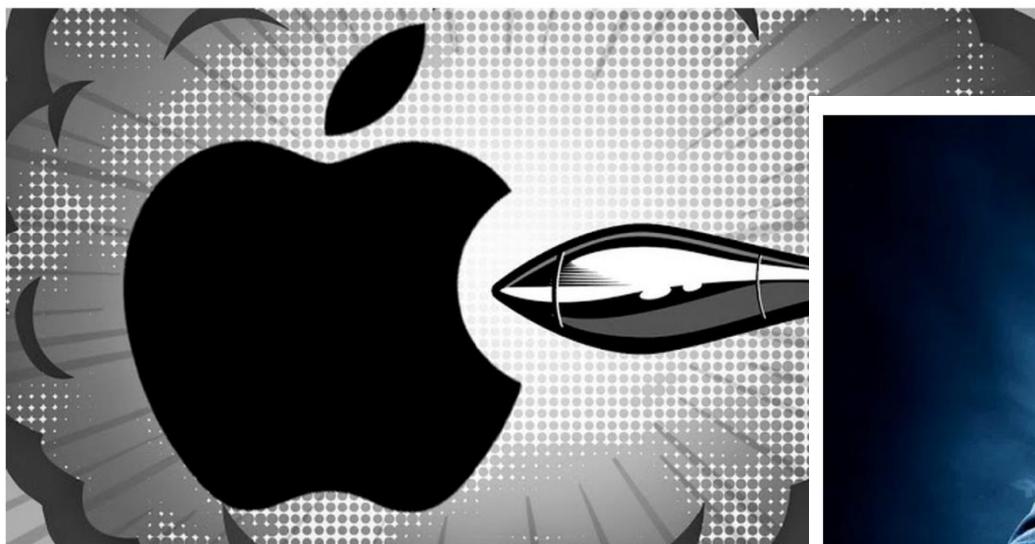


0x00 Motivation of Research

Windows? NO, Linux and Mac OS X Most Vulnerable

Operating System In 2014

Tuesday, February 24, 2015 by Swati Khandelwal



Source: <http://thehackernews.com/2015/02/vulnerable-operating-system.html>



Revoltado com a Apple, hacker do mundo jailbreak publica detalhes de uma falha de segurança do OS X

Rafael Fischmann 23/07/2015 às 09:31

Shutterstock.com



macOS Hacking Tricks



0x00 Motivation of Research

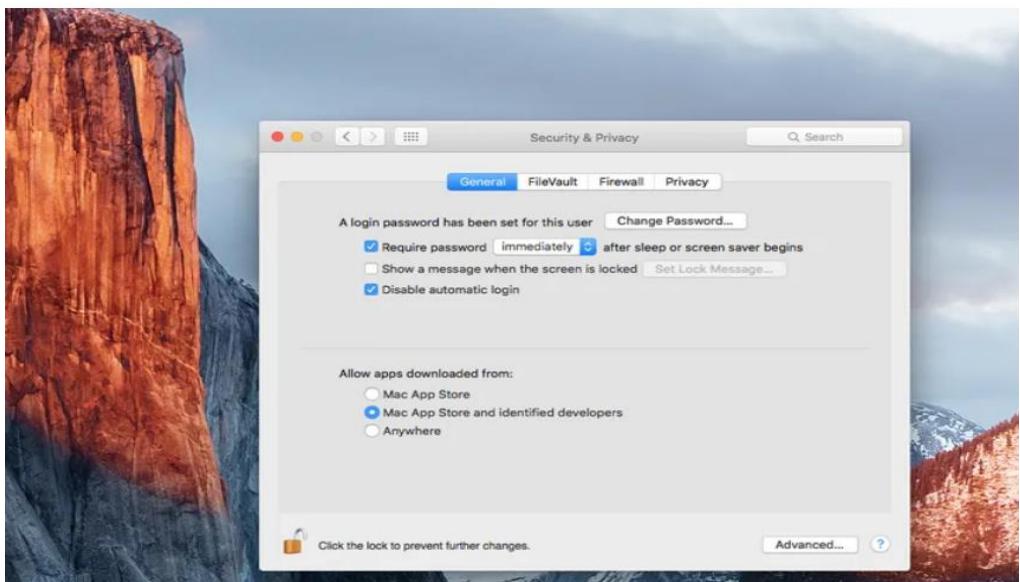


A Google assumiu responsabilidade sobre uma falha catastrófica que "matou" muitos computadores com macOS desde esse começo de semana. O problema, que impede os computadores de reiniciarem após um desligamento ou reboot, está associado a uma atualização do navegador Chrome, que acabou corrompendo o sistema de arquivos do sistema operacional da Apple.

A falha em massa começou a ser reportada na manhã de segunda-feira (23) e atingiu com mais força os editores de vídeo e as produtoras de cinema. Inicialmente, se acreditou ser um problema com o Media Composer, um software da Avid usado justamente por esse nicho e elo comum entre todos aqueles que indicaram estarem sofrendo com a falha nos fóruns oficiais da Maçã.

Researcher exposes vulnerability in macOS Gatekeeper security mechanism

Chance Miller - May, 25th 2019 9:52 am PT [@ChanceHMILLER](#)





0x00 Motivation of Research

The screenshot shows the official website for Transmission, a BitTorrent client. The header features a large 'TRANSMISSION' logo with a subtitle 'A Fast, Easy, and Free BitTorrent Client'. A prominent download button with a downward arrow icon is centered. Below the header, a navigation bar includes links for MAIN, ABOUT, DOWNLOAD, DEVELOPMENT, ADD-ONS, CONTENT, and SUPPORT. A 'Feature Spotlight' section highlights 'Transmission 2.90' with links to 'Download Now', 'Release Notes', and 'Previous Releases'. To the right, a bulleted list details its features: fewer resources, native Mac, GTK+, and Qt GUI clients; Daemon support; remote control via Web and Terminal; Local Peer Discovery; and full encryption, DHT, µTP, PEX, and Magnet Link support. A 'Learn More...' link is also present. At the bottom, there's a 'PayPal' donate button, copyright information (2009-2016), and bandwidth provider details.

OSX/CrescentCore
2019

OSX/Linker
2019

LoundMiner
2019

OSX/MaMi
2018

Crossrider
(OSX/Shalyer)
2018

Mac Auto Fixer
2018

Mshelper
2018





0x01 Security Characteristics

- ❑ A modern Operating system (**macOS fanBoy LOL**) Unix based
- ❑ Kernel XNU is based on micro-kernel of NeXTSTEP (Mach) and kernel of BSD (FreeBSD)
- ❑ Lots of userland applications
- ❑ Mac OS X has grown significantly in market share.

```
bash
↳ $:> clear
l0gan@Zion-Inf3ct3d:[~][21:30:58]
↳ $:> uname -a
Darwin Zion-Inf3ct3d.local 18.7.0 Darwin Kernel Version 18.7.0: Tue Aug 20 16:57:14 PDT 2019;
root:xnu-4903.271.2~2/RELEASE_X86_64 x86_64
l0gan@Zion-Inf3ct3d:[~][21:31:03]
↳ $:>
```

macOS Mojave
Version 10.14.6

MacBook Pro (13-inch, 2019, Four Thunderbolt 3 ports)
Processor 2,8 GHz Intel Core i7
Memory 16 GB 2133 MHz LPDDR3
Startup Disk Chacal
Graphics Intel Iris Plus Graphics 655 1536 MB
Serial Number [REDACTED]

System Report... Software Update...

TM and © 1983-2019 Apple Inc. All Rights Reserved. License Agreement





0x01 Security Characteristics

SIP (System Integrity Protection)

Xprotect

FileVault

Gatekeeper

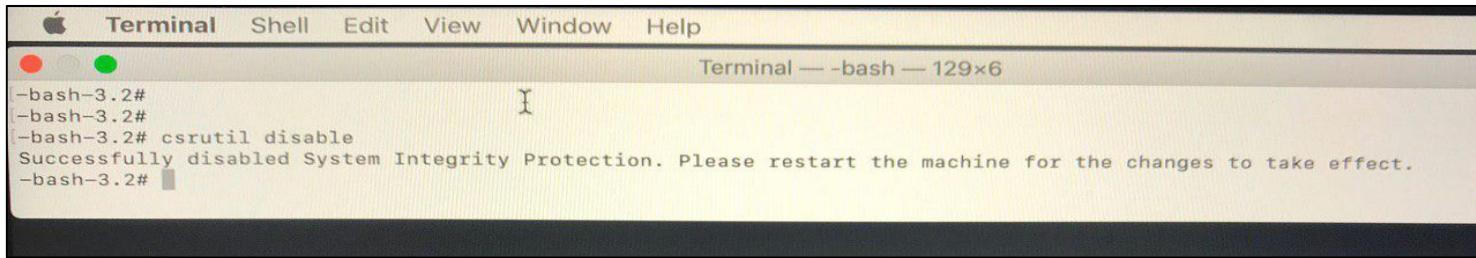
Secure Boot



0x01 Security Characteristics

SIP

Originally introduced with OS X El Capitan, System Integrity Protection, usually referred to as **SIP**, is a security feature built into the Mac operating system that's designed to protect most system locations, system processes, and Kernel extensions from being written to, modified, or replaced.



```
Terminal — -bash — 129x6
-bash-3.2#
-bash-3.2#
-bash-3.2# csrutil disable
Successfully disabled System Integrity Protection. Please restart the machine for the changes to take effect.
-bash-3.2#
```



0x01 Security Characteristics

XProtect

```
10gan@Zion-Inf3ct3d:[/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources][19:12:15]
└──> $:> pwd
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources
10gan@Zion-Inf3ct3d:[/System/Library/C
└──> $:> ls XProtect.*  
XProtect.meta.plist XProtect.plist
10gan@Zion-Inf3ct3d:[/System/Library/C
└──> $:> _
```

```
<dict>
    <key>Description</key>
    <string>OSX.KeRanger.A</string>
    <key>LaunchServices</key>
    <dict>
        <key>LSItemContentType</key>
        <string>com.apple.application-bundle</string>
    </dict>
    <key>Matches</key>
    <array>
        <dict>
            <key>MatchFile</key>
            <dict>
                <key>NSURLTypeIdentifierKey</key>
                <string>public.unix-executable</string>
            </dict>
            <key>MatchType</key>
            <string>Match</string>
            <key>Pattern</key>
            <string>488DBDD0EFFFFFB00000000BA0004000031C049
        </string>
        </dict>
    </array>
</dict>
```

Anti-virus product is internally referred to as XProtect.
Implemented within the CoreServicesUIAgent.



0x01 Security Characteristics

Filevault



Apple implementation of encrypting your data on macOS and Mac hardware. It will encrypt all of your data on your startup disk (although you can also encrypt your Time Machine backups as well) and once enabled, it will encrypt your data on the fly and will work seamlessly in the background.



0x01 Security Characteristics

Gatekeeper

The screenshot shows the 'Security & Privacy' system preference window on macOS. The 'General' tab is selected. A message at the top states 'A login password has been set for this user' with a 'Change Password...' button. Below are two checked options: 'Require password' set to '5 minutes' and 'Show a message when the screen is locked' with a 'Set Lock Message...' button. A yellow box highlights the 'Allow apps downloaded from:' section, which contains three radio button options: 'App Store' (unselected), 'App Store and identified developers' (unselected), and 'Anywhere' (selected). At the bottom left is a lock icon with the text 'Click the lock to prevent further changes.' and an 'Advanced...' button at the bottom right.

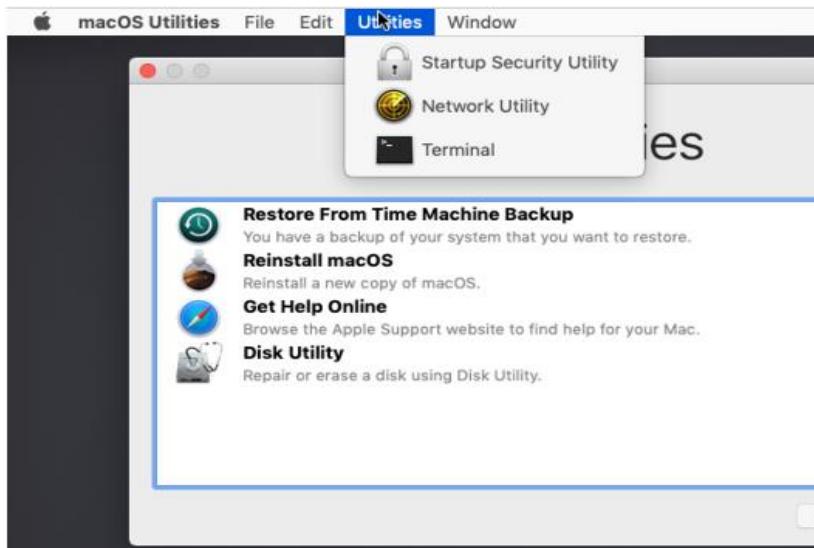
Security feature of the macOS operating system by Apple. It enforces code signing and verifies downloaded applications before allowing them to run, thereby reducing the likelihood of inadvertently executing malware.

```
$ sudo spctl --master-disable
```



0x01 Security Characteristics

SecureBoot



Firmware password protection is off.

Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.

[Turn On Firmware Password...](#)

Secure Boot

Full Security
Ensures that only your current OS, or signed operating system software currently trusted by Apple, can run. This mode requires a network connection at software installation time.

Medium Security
Allows any version of signed operating system software ever trusted by Apple to run.

No Security
Does not enforce any requirements on the bootable OS.

External Boot

Disallow booting from external media
Restricts the ability to boot from any devices such as USB and Thunderbolt drives.

Allow booting from external media
Does not restrict the ability to boot from any devices.

Process where the firmware validates the bootloader prior to loading. It is at the start of the chain of trust that ensures that code that gets run (drivers, kernel, applications) is known and validated



0x01 Security Characteristics

XNU

The screenshot shows the Apple Open Source website at opensource.apple.com. The page title is "Apple Open Source". The "Releases" section is displayed, featuring four categories: macOS, Developer Tools, iOS, and OS X Server. Each category has a corresponding icon: a globe for macOS, a wrench and hammer for Developer Tools, a smartphone for iOS, and a globe for OS X Server. Below each icon is a list of release versions. The "macOS" section lists versions from 10.0 to 10.14. The "Developer Tools" section lists versions from 10.0 to 11.0. The "iOS" section lists versions from 1.0 to 11.0. The "OS X Server" section lists versions from 1.0 to 3.x.

Category	Version
macOS	10.0
	10.1
	10.2
	10.3
	10.4
	10.5
	10.6
	10.7
	10.8
	10.9
	10.10
	10.11
	10.12
	10.13
	10.14
	10.14.1
	10.14.2
	10.14.3
	10.14.4
	10.14.5
10.14.6	
10.14.7	
10.14.8	
10.14.9	
10.14.10	
10.14.11	
10.14.12	
10.14.13	
10.14.14	
10.14.15	
10.14.16	
10.14.17	
10.14.18	
10.14.19	
10.14.20	
10.14.21	
10.14.22	
10.14.23	
10.14.24	
10.14.25	
10.14.26	
10.14.27	
10.14.28	
10.14.29	
10.14.30	
10.14.31	
10.14.32	
10.14.33	
10.14.34	
10.14.35	
10.14.36	
10.14.37	
10.14.38	
10.14.39	
10.14.40	
10.14.41	
10.14.42	
10.14.43	
10.14.44	
10.14.45	
10.14.46	
10.14.47	
10.14.48	
10.14.49	
10.14.50	
10.14.51	
10.14.52	
10.14.53	
10.14.54	
10.14.55	
10.14.56	
10.14.57	
10.14.58	
10.14.59	
10.14.60	
10.14.61	
10.14.62	
10.14.63	
10.14.64	
10.14.65	
10.14.66	
10.14.67	
10.14.68	
10.14.69	
10.14.70	
10.14.71	
10.14.72	
10.14.73	
10.14.74	
10.14.75	
10.14.76	
10.14.77	
10.14.78	
10.14.79	
10.14.80	
10.14.81	
10.14.82	
10.14.83	
10.14.84	
10.14.85	
10.14.86	
10.14.87	
10.14.88	
10.14.89	
10.14.90	
10.14.91	
10.14.92	
10.14.93	
10.14.94	
10.14.95	
10.14.96	
10.14.97	
10.14.98	
10.14.99	
10.14.100	
10.14.101	
10.14.102	
10.14.103	
10.14.104	
10.14.105	
10.14.106	
10.14.107	
10.14.108	
10.14.109	
10.14.110	
10.14.111	
10.14.112	
10.14.113	
10.14.114	
10.14.115	
10.14.116	
10.14.117	
10.14.118	
10.14.119	
10.14.120	
10.14.121	
10.14.122	
10.14.123	
10.14.124	
10.14.125	
10.14.126	
10.14.127	
10.14.128	
10.14.129	
10.14.130	
10.14.131	
10.14.132	
10.14.133	
10.14.134	
10.14.135	
10.14.136	
10.14.137	
10.14.138	
10.14.139	
10.14.140	
10.14.141	
10.14.142	
10.14.143	
10.14.144	
10.14.145	
10.14.146	
10.14.147	
10.14.148	
10.14.149	
10.14.150	
10.14.151	
10.14.152	
10.14.153	
10.14.154	
10.14.155	
10.14.156	
10.14.157	
10.14.158	
10.14.159	
10.14.160	
10.14.161	
10.14.162	
10.14.163	
10.14.164	
10.14.165	
10.14.166	
10.14.167	
10.14.168	
10.14.169	
10.14.170	
10.14.171	
10.14.172	
10.14.173	
10.14.174	
10.14.175	
10.14.176	
10.14.177	
10.14.178	
10.14.179	
10.14.180	
10.14.181	
10.14.182	
10.14.183	
10.14.184	
10.14.185	
10.14.186	
10.14.187	
10.14.188	
10.14.189	
10.14.190	
10.14.191	
10.14.192	
10.14.193	
10.14.194	
10.14.195	
10.14.196	
10.14.197	
10.14.198	
10.14.199	
10.14.200	
10.14.201	
10.14.202	
10.14.203	
10.14.204	
10.14.205	
10.14.206	
10.14.207	
10.14.208	
10.14.209	
10.14.210	
10.14.211	
10.14.212	
10.14.213	
10.14.214	
10.14.215	
10.14.216	
10.14.217	
10.14.218	
10.14.219	
10.14.220	
10.14.221	
10.14.222	
10.14.223	
10.14.224	
10.14.225	
10.14.226	
10.14.227	
10.14.228	
10.14.229	
10.14.230	
10.14.231	
10.14.232	
10.14.233	
10.14.234	
10.14.235	
10.14.236	
10.14.237	
10.14.238	
10.14.239	
10.14.240	
10.14.241	
10.14.242	
10.14.243	
10.14.244	
10.14.245	
10.14.246	
10.14.247	
10.14.248	
10.14.249	
10.14.250	
10.14.251	
10.14.252	
10.14.253	
10.14.254	
10.14.255	
10.14.256	
10.14.257	
10.14.258	
10.14.259	
10.14.260	
10.14.261	
10.14.262	
10.14.263	
10.14.264	
10.14.265	
10.14.266	
10.14.267	
10.14.268	
10.14.269	
10.14.270	
10.14.271	
10.14.272	
10.14.273	
10.14.274	
10.14.275	
10.14.276	
10.14.277	
10.14.278	
10.14.279	
10.14.280	
10.14.281	
10.14.282	
10.14.283	
10.14.284	
10.14.285	
10.14.286	
10.14.287	
10.14.288	
10.14.289	
10.14.290	
10.14.291	
10.14.292	
10.14.293	
10.14.294	
10.14.295	
10.14.296	
10.14.297	
10.14.298	
10.14.299	
10.14.300	
10.14.301	
10.14.302	
10.14.303	
10.14.304	
10.14.305	
10.14.306	
10.14.307	
10.14.308	
10.14.309	
10.14.310	
10.14.311	
10.14.312	
10.14.313	
10.14.314	
10.14.315	
10.14.316	
10.14.317	
10.14.318	
10.14.319	
10.14.320	
10.14.321	
10.14.322	
10.14.323	
10.14.324	
10.14.325	
10.14.326	
10.14.327	
10.14.328	
10.14.329	
10.14.330	
10.14.331	
10.14.332	
10.14.333	
10.14.334	
10.14.335	
10.14.336	
10.14.337	
10.14.338	
10.14.339	
10.14.340	
10.14.341	
10.14.342	
10.14.343	
10.14.344	
10.14.345	
10.14.346	
10.14.347	
10.14.348	
10.14.349	
10.14.350	
10.14.351	
10.14.352	
10.14.353	
10.14.354	
10.14.355	
10.14.356	
10.14.357	
10.14.358	
10.14.359	
10.14.360	
10.14.361	
10.14.362	
10.14.363	
10.14.364	
10.14.365	
10.14.366	
10.14.367	
10.14.368	
10.14.369	
10.14.370	
10.14.371	
10.14.372	
10.14.373	
10.14.374	
10.14.375	
10.14.376	
10.14.377	
10.14.378	
10.14.379	
10.14.380	
10.14.381	
10.14.382	
10.14.383	
10.14.384	
10.14.385	
10.14.386	
10.14.387	
10.14.388	
10.14.389	
10.14.390	
10.14.391	
10.14.392	
10.14.393	
10.14.394	
10.14.395	
10.14.396	
10.14.397	
10.14.398	
10.14.399	
10.14.400	
10.14.401	
10.14.402	
10.14.403	
10.14.404	
10.14.405	
10.14.406	
10.14.407	
10.14.408	
10.14.409	
10.14.410	
10.14.411	
10.14.412	
10.14.413	
10.14.414	
10.14.415	
10.14.416	
10.14.417	
10.14.418	
10.14.419	
10.14.420	
10.14.421	
10.14.422	
10.14.423	
10.14.424	
10.14.425	
10.14.426	
10.14.427	
10.14.428	
10.14.429	
10.14.430	
10.14.431	
10.14.432	
10.14.433	
10.14.434	
10.14.435	
10.14.436	
10.14.437	
10.14.438	
10.14.439	
10.14.440	
10.14.441	
10.14.442	
10.14.443	
10.14.444	
10.14.445	
10.14.446	
10.14.447	
10.14.448	
10.14.449	
10.14.450	
10.14.451	
10.14.452	
10.14.453	
10.14.454	
10.14.455	
10.14.456	
10.14.457	
10.14.458	
10.14.459	
10.14.460	
10.14.461	
10.14.462	
10.14.463	
10.14.464	
10.14.465	
10.14.466	
10.14.467	
10.14.468	
10.14.469	
10.14.470	
10.14.471	
10.14.472	
10.14.473	
10.14.474	
10.14.475	
10.14.476	
10.14.477	
10.14.478	
10.14.479	
10.14.480	
10.14.481	
10.14.482	
10.14.483	
10.14.484	
10.14.485	
10.14.486	
10.14.487	
10.14.488	
10.14.489	
10.14.490	
10.14.491	
10.14.492	
10.14.493	
10.14.494	
10.14.495	
10.14.496	
10.14.497	
10.14.498	
10.14.499	
10.14.500	
10.14.501	
10.14.502	
10.14.503	
10.14.504	
10.14.505	
10.14.506	
10.14.507	
10.14.508	
10.14.509	
10.14.510	
10.14.511	
10.14.512	
10.14.513	
10.14.514	
10.14.515	
10.14.516	
10.14.517	
10.14.518	
10.14.519	
10.14.520	
10.14.521	
10.14.522	
10.14.523	
10.14.524	
10.14.525	
10.14.526	
10.14.527	
10.14.528	
10.14.529	
10.14.530	
10.14.531	
10.14.532	
10.14.533	
10.14.534	
10.14.535	
10.14.536	
10.14.537	
10.14.538	
10.14.539	
10.14.540	
10.14.541	
10.14.542	
10.14.543	
10.14.544	
10.14.545	
10.14.546	
10.14.547	
10.14.548	
10.14.549	
10.14.550	
10.14.551	
10.14.552	
10.14.553	
10.14.554	
10.14.555	
10.14.556	
10.14.557	
10.14.558	
10.14.559	
10.14.560	
10.14.561	
10.14.562	
10.14.563	
10.14.564	
10.14.565	
10.14.566	
10.14.567	
10.14.568	
10.14.569	
10.14.570	
10.14.571	
10.14.572	
10.14.573	
10.14.574	
10.14.575	
10.14.576	
10.14.577	
10.14.578	
10.14.579	
10.14.580	
10.14.581	
10.14.582	
10.14.583	
10.14.584	
10.14.585	
10.14.586	
10.14.587	
10.14.588	
10.14.589	
10.14.590	
10.14.591	
10.14.592	
10.14.593	
10.14.594	
10.14.595	
10.14.596	
10.14.597	
10.14.598	
10.14.599	
10.14.600	
10.14.601	
10.14.602	
10.14.603	
10.14.604	
10.14.605	
10.14.606	
10.14.607	
10.14.608	
10.14.609	
10.14.610	
10.14.611	
10.14.612	
10.14.613	
10.14.614	
10.14.615	
10.14.616	
10.14.617	
10.14.618	
10.14.619	
10.14.620	
10.14.621	
10.14.622	
10.14.623	
10.14.624	
10.14.625	
10.14.626	
10.14.627	
10.14.628	
10.14.629	
10.14.630	
10.14.631	
10.14.632	
10.14.633	
10.14.634	
10.14.635	
10.14.636	
10.14.637	
10.14.638	
10.14.639	
10.14.640	
10.14.641	
10.14.642	
10.14.643	
10.14.644	
10.14.645	
10.14.646	
10.14.647	
10.14.648	
10.14.649	
10.14.650	
10.14.651	
10.14.652	
10.	



0x01 Security Characteristics

```
10gan@Zion-Inf3ct3d:[~][20:58:07]
└──→ $:> sudo sqlite3 /var/db/SystemPolicyConfiguration/KextPolicy
SQLite version 3.24.0 2018-06-04 14:10:15
Enter ".help" for usage hints.
sqlite> SELECT * from kext_policy;
EG7KH642X6|com.vmware.kext.vmcil|1|VMware, Inc.|1
EG7KH642X6|com.vmware.kext.vmnet|1|VMware, Inc.|1
EG7KH642X6|com.vmware.kext.vmx86|1|VMware, Inc.|1
EG7KH642X6|com.vmware.kext.vmioplug.18.1.2|1|VMware, Inc.|1
2Y8XE5CQ94|com.kaspersky.kext.klif|1|Kaspersky Lab UK Limited|1
2Y8XE5CQ94|com.kaspersky.nkel|1|Kaspersky Lab UK Limited|1
sqlite> _
```

Kext files are essentially drivers for macOS. "Kext" stands for Kernel Extension; kext files "extend" Mac OS X's kernel, the core part of the operating system, by providing additional code to be loaded when your computer boots.



0x01 Security Characteristics

```
10gan@Zion-Inf3ct3d: [/System/Library/Extensions][22:59:00]
└──> $:> pwd
/System/Library/Extensions
10gan@Zion-Inf3ct3d: [/System/Library/Extensions][22:59:05]
└──> $:> ls -l
total 0
drwxr-xr-x@ 3 root  wheel  96 Jun 20 22:51 ALF.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMD1000Controller.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMD7000Controller.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMD8000Controller.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMD9000Controller.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMD9500Controller.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDFramebuffer.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDMTLBronzeDriver.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonVADriver.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonVADriver2.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX4000.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX4000GLDriver.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX4000HWServices.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX5000.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX5000GLDriver.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX5000HWServices.kext
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX5000MTLDriver.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDRadeonX5000Shared.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDShared.bundle
drwxr-xr-x@ 3 root  wheel  96 Jul  3 01:51 AMDSupport.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 20 22:57 Apple16X50Serial.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 24 01:33 AppleACPIPlatform.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 24 01:30 AppleAHCIPort.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 20 22:57 AppleAPIC.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 20 23:02 AppleAVEBridge.kext
drwxr-xr-x@ 3 root  wheel  96 Jul 25 23:07 AppleActuatorDriver.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 24 01:37 AppleBCMWLanBusInterfacePCIe.kext
drwxr-xr-x@ 3 root  wheel  96 Jun 24 01:37 AppleBCMWLanCore.kext
```



0x01 Security Characteristics



Keychain Access

The screenshot shows the Keychain Access application window. The sidebar on the left has a 'Category' section with options: All Items (selected), Passwords, Secure Notes, My Certificates, Keys, and Certificates. The main pane displays a table of items under the heading 'com.apple.facetime: registrationV1'. The table columns are Name, Kind, Date Modified, Expires, and Keychain. The 'Kind' column shows mostly 'application password' entries, with one entry for 'com.apple.facetime: registrationV1' also listed. The 'Date Modified' column includes dates like 'Yesterday, 09:40' and '15 Aug 2019 01:48:08'. The 'Keychain' column shows 'login' for most entries.

Name	Kind	Date Modified	Expires	Keychain
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:08	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:08	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:08	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:08	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:09	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:09	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:19	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:21	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:35	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:48:41	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 01:50:21	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 02:02:19	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 07:20:41	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 07:21:35	--	login
com.apple.cloud.deviceidentifier.Production	application password	15 Aug 2019 23:03:18	--	login
com.apple.cloud.deviceidentifier.Production	application password	16 Aug 2019 19:18:17	--	login
com.apple.cloud.deviceidentifier.Production	application password	19 Sep 2019 17:23:30	--	login
com.apple.cloud.deviceidentifier.Production	application password	23 Sep 2019 09:47:59	--	login
com.apple.cloud.deviceidentifier.Production	application password	30 Sep 2019 22:31:12	--	login
com.apple.cloud.deviceidentifier.Production	application password	7 Oct 2019 22:24:00	--	login
com.apple.facetime: registrationV1	application password	Yesterday, 09:40	--	login
com.apple.gs.appleid.auth.com...ccount.AppleIDAuthentication.token	application password	14 Oct 2019 21:54:17	--	login
com.apple.gs.authagent.auth.c...ccount.AppleIDAuthentication.token	application password	14 Oct 2019 21:54:17	--	login

Keychain file stores secrets data like:
Safari passwords, WIFI keys, Skype
username/password, Google username/password
(contact, Picasa), Exchange username/password



0x01 Security Characteristics

```
l0gan@Zion-Inf3ct3d:[~/Library/Keychains][22:04:29]
└──> $:> pwd
/Users/l0gan/Library/Keychains
l0gan@Zion-Inf3ct3d:[~/Library/Keychains][22:04:31]
└──> $:> ls -l
total 976
drwx----- 10 l0gan staff 320 Oct 17 16:10 8DEA70A8-20E3-5FB9-BBC4-132BC9525660
-rw-r--r--@ 1 l0gan staff 474568 Oct 19 19:49 login.keychain-db
-rw----- 1 l0gan staff 23804 Oct 8 09:52 metadata.keychain-db
l0gan@Zion-Inf3ct3d:[~/Library/Keychains][22:04:34]
└──> $:> _
```

```
l0gan@Zion-Inf3ct3d:[~][16:15:17]
└──> $:> security list-keychains
"/Users/l0gan/Library/Keychains/login.keychain-db"
"/Library/Keychains/System.keychain"
l0gan@Zion-Inf3ct3d:[~][16:15:26]
```

```
l0gan@Zion-Inf3ct3d:[~/Library/Keychains][16:18:14]
└──> $:> file login.keychain-db
login.keychain-db: Mac OS X Keychain File
```



0x01 Security Characteristics

```
l0gan@Zion-Inf3ct3d: [~/Library/LaunchAgents] [23:01:10]
└──> $:> pwd
/Users/l0gan/Library/LaunchAgents
l0gan@Zion-Inf3ct3d: [~/Library/LaunchAgents] [23:01:47]
└──> $:> ls -l
total 24
-rw-r--r-- 1 l0gan
-rw-r--r--@ 1 l0gan
-rw-r--r--@ 1 l0gan
l0gan@Zion-Inf3ct3d: [~/Library/LaunchAgents] [23:01:47]
└──> $:> _

l0gan@Zion-Inf3ct3d: [/Library/LaunchAgents] [23:01:47]
└──> $:> pwd
/Library/LaunchAgents
l0gan@Zion-Inf3ct3d: [/Library/LaunchAgents] [23:01:47]
└──> $:> ls -l
total 24
-rw-r--r-- 1 root
-rw-r--r-- 1 root
-r-xr-xr-x 1 root
l0gan@Zion-Inf3ct3d: [/Library/LaunchDaemons] [23:02:23]
└──> $:> pwd
/Library/LaunchDaemons
l0gan@Zion-Inf3ct3d: [/Library/LaunchDaemons] [23:02:24]
└──> $:> ls -l
total 48
-rw-r--r-- 1 root wheel 632 Sep 19 14:55 com.apple.installer.osmessagetracing.plist
-rw-r--r-- 1 root wheel 584 Oct 7 22:25 com.bjango.istatmenus.daemon.plist
-rw-r--r-- 1 root wheel 557 Oct 7 22:25 com.bjango.istatmenus.fans.plist
-rw-r--r-- 1 root wheel 608 Aug 15 21:58 com.bjango.istatmenus.installerhelper.plist
-r-xr-xr-x 1 root wheel 1080 Jun 25 14:24 com.kaspersky.kav.plist
-rw-r--r-- 1 root wheel 382 Aug 15 07:31 org.wireshark.ChmodBPF.plist
l0gan@Zion-Inf3ct3d: [/Library/LaunchDaemons] [23:02:26]
└──> $:> _

$ launchctl load arquivo.plist
```

PLIST file is a settings file, also known as a "properties file," used by macOS applications.

It contains properties and configuration settings for various programs. PLIST files are formatted in XML and based on Apple's Core Foundation DTD.



0x02 Hacking macOS target

Obtain system user access

From remote access:

- By common “server side” vulnerabilities like SMB, SSH, WEB, ...
- By “client side” vulnerabilities of Safari, iTunes, iChat, Quicktime, Skype, ..



0x02 Hacking macOS target

```
Terminal — -bash — 129x6
-bash-3.2#
-bash-3.2#
-bash-3.2# csrutil disable
Successfully disabled System Integrity Protection. Please restart the machine for the changes to take effect.
-bash-3.2#
```

```
sh-3.2# pwd
/var/db/dslocal/nodes/Default/users
sh-3.2# ls
_amavisd.plist          _devicemgr.plist        _krbtgt.plist      _softwareupdate.plist
_analyticsd.plist        _displaypolicyd.plist    _launchservicesd.plist _spotlight.plist
_appleevents.plist       _distnote.plist        _ldagent.plist     _ssh.plist
_applepay.plist          _dovecot.plist        _locationd.plist   _svn.plist
_appowner.plist          _dovenuull.plist      _lp.plist         _taskgated.plist
_appserver.plist         _dpaudio.plist       _mailman.plist    _teamsserver.plist
_appstore.plist          _eppc.plist          _mbsetupuser.plist _timed.plist
_ard.plist               _findmydevice.plist    _mcxalr.plist     _timezone.plist
_assetcache.plist        _fpsd.plist          _mdnsresponder.plist _tokend.plist
_astris.plist            _ftp.plist           _mobileasset.plist _trustevaluationagent.plist
_atsserver.plist         _gamecontrollerd.plist _mysql.plist      _unknown.plist
_avbdevidced.plist      _geod.plist          _netbios.plist    _update_sharing.plist
_calendar.plist          _hidd.plist          _netstatistics.plist _usbmuxd.plist
_captiveagent.plist      _iconservices.plist    _networkd.plist   _uucp.plist
_ces.plist               _installassistant.plist _nsurlsessiond.plist _warmd.plist
_clamav.plist            _installer.plist      _nsurlstoraged.plist _webauthserver.plist
_cmiodalassistants.plist _jabber.plist        _ondemand.plist   _windowserver.plist
_coreaudiod.plist         _kadmin_admin.plist    _postfix.plist    _www.plist
_coremediaiod.plist       _kadmin_changepw.plist _postgres.plist   _wwwproxy.plist
_ctkd.plist              _krb_anonymous.plist  _qtss.plist      _xserverdocs.plist
_cvmsroot.plist          _krb_changepw.plist   _reportmemoryexception.plist _daemon.plist
_cvs.plist               _krb_kadmin.plist     _sandbox.plist    _logan.plist
_cyrus.plist              _krb_kerberos.plist   _screensaver.plist _nobody.plist
_datadetectors.plist     _krb_krbtgt.plist    _scsd.plist      _root.plist
_devdocs.plist            _krb_krbtgt.plist    _securityagent.plist
```

Hashdump Python Script + Crack the Hash (Hashcat)





0x02 Hacking macOS target

Exploit-db

Exploit Title	Path
Apple macOS 10.13.1 (High Sierra) - Insecure Cron System Local Privilege Escalation	exploits/macos/local/43247.md
Apple Intel GPU Driver	exploits/macos/dos/44561.txt
Apple Safari 10.0.3 - .	exploits/macos/dos/45391.py
Apple Safari 10.1 - Spr	exploits/macos/local/40956.c
Apple WebKit 10.0.2 - .	exploits/macos/local/40957.c
Apple iOS/macOS - Kerne	exploits/macos/local/43926.sh
Apple iOS/macOS - Sandb	exploits/macos/local/43218.sh
Apple iOS/macOS - Sandb	exploits/macos/local/43216.rb
Apple iOS/macOS - '32-bit s	exploits/macos/local/45107.txt
Apple macOS - 'getrusag	exploits/macos/dos/45823.py
Apple macOS - 'necp_get	exploits/macos/dos/45788.txt
Apple macOS - 'stacksho	exploits/macos/dos/45787.txt
Apple macOS - Disk Arbi	exploits/macos/local/44307.m
Apple macOS - IOHIDSyst	exploits/macos/local/43224.sh
Apple macOS - Kernel Co	exploits/macos/local/43223.sh
Apple macOS - Lack of B	exploits/macos/local/43222.sh
Apple macOS 10.12 - 'ta	exploits/macos/local/43220.sh
Apple macOS 10.12 - Dou	exploits/macos/local/43219.sh
Apple macOS 10.12 16A32	exploits/macos/local/42334.txt
Apple macOS/iOS 10	exploits/macos/local/41952.txt
Apple macOS 10.12.1 / i	exploits/macos/local/45782.c
Apple macOS 10.12.1 / i	exploits/macos/local/45916.rb
Apple macOS 10.12.1 / i	exploits/osx/local/24609.txt
Apple macOS 10.12.1 Ker	exploits/osx/local/24608.txt
Apple macOS 10.12.3 / i	exploits/macos/dos/46236.py
Apple macOS 10.13 - 'wo	exploits/macos/local/43217.sh
Apple macOS 10.13.1 (Hi	exploits/osx/local/19439.txt
Apple macOS 10.13.1 (Hi	exploits/macos/local/41854.txt
Apple macOS/iOS - Proxi	exploits/macos/local/41853.txt
Apple macOS/iOS Ker	exploits/macos/local/43225.sh
Apple macOS/iOS Ker	exploits/macos/remote/45998.rb
Apple macOS/iOS Ker	exploits/macos/local/43221.sh
Apple macOS/iOS Ker	exploits/macos/local/45854.txt
Apple macOS/iOS Ker	exploits/macos/local/42454.txt
Apple macOS/iOS Ker	exploits/macos/webapps/44803.txt
Apple macOS/iOS Ker	exploits/multiple/dos/46248.c
Apple macOS/iOS Ker	exploits/macos/dos/43521.c
Apple macOS - 'process_policy'	exploits/macos/dos/43923.c
macOS - 'sysctl_vfs_gen	exploits/macos/dos/43780.c
macOS 10.13 (17A365) - K	exploits/macos/dos/44007.c
macOS Kernel - Use-After-Free Due to Lack of Locking in 'AppleEmbeddedOSSupportHostClient::registerNotificationPort'	exploits/macos/dos/45032.txt
macOS/iOS - JavaScript In	

MULLBYTE



0x03 Hacking macOS target Demo

Demos 01

Service: RAE (Remote Apple Events)

Detail: AppleScript and Objects
Port TCP/UDP 3031 = eppc



0x03 Hacking macOS target Demo

Demo 02

XNU: copy-on-write behavior bypass via
mount of user-owned filesystem

Autor: Jann Horn (Google Project Zero)

<https://bugs.chromium.org/p/project-zero/issues/detail?id=1726&q=>

CVE-2019-6208

Corrigido = macOS Mojave 10.14.3

<https://support.apple.com/pt-br/HT209446>

- ❖ buggycow.c
- ❖ mod.c
- ❖ pressure.c



0x03 Hacking macOS target Demo

Demo 03

“local phishing”

Detail: OSASCIPT (OSA Open Scripting Architecture Language Script)

Reference: <https://ss64.com/osx/osascript.html>

Bônus:

How to Create a Fake PDF Trojan with AppleScript, Part 1 (Creating the Stager)

<https://null-byte.wonderhowto.com/how-to/hacking-macos-create-fake-pdf-trojan-with-applescript-part-1-creating-stager-0184692/>

How to Create a Fake PDF Trojan with AppleScript, Part 2 (Disguising the Script)

<https://null-byte.wonderhowto.com/how-to/hacking-macos-create-fake-pdf-trojan-with-applescript-part-2-disguising-script-0184706/>



0x04 macOS Tools

Lipo -> create or operate on universal files
otool -> object file displaying tool like a objdump and ldd
nm -> display name list (symbol table)
codesign -> create and manipulate code signatures
machOView -> visual Mach-O file browser
class-dump -> utility for examining the Objective-C runtime information stored in Mach-O files.
dtrace -> generic front-end to the DTrace facility
fs_usage -> report system calls and page faults related to filesystem activity in real-time
xattr -> display and manipulate extended attributes
Xcode -> xcode is an (IDE) containing a suite of software development.
hopper -> tool used for disassemble, and decompile your 32/64bits mach-o file.
lldb -> debugger
fseventer -> disk activity tool with a good graphical representation and solid filter tool.



0x04 macOS Tools

`launchctl` -> Manage and Inspect daemons, agents and XPC Services (PLIST)
`sysctl` -> get or set kernel state
`nettop` -> Display updated information about the network
`lsmmp` -> list port used by process
`ndisasm` -> The Netwide Disassembler, an 80x86 binary file disassembler
`spctl` -> SecAssessment system policy security (Gatekeeper)
`dscl` -> Directory Service command line utility
`csrutil` -> Configure system security policies (SIP)
`open snoop` -> snoop file opens as they occur. Uses DTrace.
`activity Monitor` -> tool to help you keep your system in good shape.
`procxp` -> It's a simple tool like a top get information accessible by `proc_info`
`lsock` -> based on PF_SYSTEM provider, you can get real time notifications of socket activity like TCPView from SysInternals.
`little Snitch` -> network traffic monitoring and control.



0x05 Reference

Hacking is a way of life

Reference:

Kernel Architecture Overview

https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html#/apple_ref/doc/uid/TP30000905-CH1g-TPXREF101

Apple Developer

<https://developer.apple.com/>

macOS Kernel Debugging

<https://blog.quarkslab.com/an-overview-of-macos-kernel-debugging.html>

Building XNU for macOS

<https://kernelshaman.blogspot.com/2018/01/building-xnu-for-macos-high-sierra-1013.html>



0x06 Conclusion

Thanks a Lot

Any Questions ?

ricardologanbr@gmail.com @10ganbr

<https://www.slideshare.net/10ganbr/nullbyte-6ed-2019>



macOS Hacking Tricks