Phrack ProPhile on Gera

AUTHOR: Phrack Staff

[... the full length prophile is available in the eZine only ...]

Specs

Name: gera
Handle: gera
Handle origin: it's just my name ¯_(ツ)_/¯
AKA: casper (around 1993?),
Richie++ (¿ 4:900/208.3 ? @FidoNet)
Country: Argentina
Website: http://127.1:631
GitHub: gerasdf

Background

2400 bauds version:

I always wanted to do robots. My mother sent me (at 11 yo?) to learn Logo, and I did. Got my first computer (TI99/4A). Got a Commodore 64 and then a 128. Learned assembly on the Commodore, at around 12 years old. PC enters life. Got hold of Turbo Assembler, Turbo Pascal, Turbo Debugger, etc at school. Found friends to learn together. After struggling, I found Ralf Brown's interrupt list, then Sourcer disassembler. The Stoned virus found me, got totally hooked, and started collecting virii. Wrote my first "virus" to bypass security at school.

Collected PC viruses, and wrote a few myself. Found more friends to learn with, and we moved on to accessing openly available remote computers.

We thought we could even make (legal) money from what we loved. (Co) Founded Core SDI/Core Security, wrote and released ABOs (Advanced Buffer overflows), (co) created Core IMPACT, (this is no longer 2400 bps version and I'm not liking it), I taught assembly and exploit writing, put together the exploits writing team at Core... got fed up of the security industry, started Disarmista (2008?), exclusively offering reverse engineering services for "good reasons".

Got a call from a friend, along the lines of "hey, want to come and do satellites?" – I said "no", but there was really no reason to say no. 15 years later I'm still doing satellites, and their security too.

Inspiration

Wanting to do games was the reason I first learned assembly (why would somebody learn assembly today?). Then viruses and their reproductive capability really hooked me. Reproduction is one of the main characteristics of living organisms, I felt then (though virii don't have opposite thumbs like Koalas, which have two).

Reversing stealth viruses I learned there were many tricks only a few knew, that gave you invisibility. With friends I learned hacking, and the thirst for knowledge and solving puzzles was just too strong and addictive, it still is. As for people, I started so disconnected that it was hard to get a model, though I always say my great teacher was Petro, "just" a teacher, who was so good at explaining, that you always left thinking you understood it all and just had the greatest idea of humanity, just by yourself.

Favorites:

In Argentina, as in many forgotten countries, cracking was a necessity. Many times, even when you wanted to buy the software and had the money (not very likely), you couldn't. So, we were only left to our own devices, likely by design (as they say, the first is free...) I mean, we had to do some cracking. During my C64/128 era I just didn't understand enough, but entering the PC I realized that I just couldn't copy a program and install it at home. So, here comes the cracking and the debugger.

So I cracked a few apps, for myself or to amuse friends, like getting infinite money in Sim City. But one day I was the first to get the new version of Remote Access (a BBS hosting software) in Argentina, and it needed cracking.

So I set out to crack it. It was a quick job initially, but then I discovered there was a whole set of functionality that wasn't regularly available. This gave me the idea of adding even more functionality (some may call it a backdoor) that enabled a sort of god mode. It took me a couple of days. The whole time I was telling people 'yes yes, I'm almost there, cracking isn't easy you know.' When I finally finished, I slightly changed the banner to identify it easily, and set it free.

Memorable Experiences:

For this issue, just one, or it'll get too long: It was the last evening before shipping our third satellite (Tita, for Tita Merelo). It was unfinished, of course, and we were doing software changes all the time, even on the satellite systems themselves (no CI/CD, sorry). The satellite had (has?) 6 Linux systems, and the main linux guy was doing the final touches, everybody around doing stuff, and then "MIERDA!", he shouted, and silence fell on the floor. All cameras to his face, he was buried in his hands, frozen in place, not even breathing... so, somebody approaches to see the screen, and there were 6 sshs, all doing the same with those multi-ssh things, all reading:

```
# rm -rf /
# ^C
# _
```

[...continues in the eZine only]

What is the achievement you're most proud of?

There's something that makes me proud, not exactly my personal achievement, more like a group achievement:

The size and quality of the security scene in Argentina

Many things happened at the same time, and maybe the Ekoparty was a bigger contributor through the years, but so many amazing people passed through Core, for many their first true job (because nobody else dared to employ them, heh), untamed creativity, infinite thirst for breaking the limits and doing impossible things.

Core grew and grew, attracting talent, until it exploded. First I was mad at us and the people leaving, but with some time I felt how the spores got rooted in other places, new companies got infected with the culture, and suddenly the family got back together, and it was larger than before and amazing again.

Of course, I should have made a lot of money when we "sold" it, but no, we just didn't. I think we got around $5k total (each!). Don't sign anything with the big monsters, they'll just eat you.

On a different life, I'm also happy (not sure if proud) I could write an OS purely in Smalltalk (see SqueakNOS), with network drivers, and all.

How did Phrack influence you and helped shape who you are?

A lot. Along with other zines, Phrack always stood out for its technical content. I remember studying all articles on heap exploitation (w00w00's, MaXX', the anonymous one) nergal's article on ret2libc and klog's on frame pointer overwrite, grugq's ELF article, and his and scut's on ELF encryption, and many more that I now recognize browsing the online issues.

I used to print those articles and read them over and over. I even carried a few of the original printouts with me through many moves over the years. A few months ago, I found the stack and finally gave them a new life.

Reading all the tricks, understanding all the different points of view, finally helped me develop the instinct that a bit is just a bit, and all the meaning is in the observer.

And I figured I'm not a lonely weirdo who ENJOYS squeezing the constrained options a vulnerability offers to conquer the execution flow. We are legion.

What is your favourite bug/exploit?

- CVE-2004-0368 - dtlogin double free.
- CVE-2001-0550 - wu-ftpd gobbing heap overflow (arbitrary free)
- CVE-1999-1085 - SSH CRC32 compensation attack
- CVE-2001-0114 - SSH CRC32 compensation attack integer overflow

Would you recommend newcomers to contribute to open source projects?

Totally! Why not? I wish I had time and energy to do more of that. I'm all for full disclosure, even of exploits. And all for contributing.

Contributing back to OS is sort of the easiest way to get your code maintained :-p (not quite). Commercially you may think that "giving up" your code for free is not a good idea, but it comes back, and sometimes surprisingly soon. It'll get you a job, that's for sure, but it could also become an income by itself.

But then, also, and more seriously (if anybody needed to get serious), it's fine to do things just because you can. We used to answer exactly that

Why do you do that?!
Because I can

Technology has a significant impact. At some point, I began thinking about how my work could help people and make their lives better, even just a little bit. You never know what people will find useful, and the feedback you receive when you release something is a great feeling: the realization that someone is actually using what you created.

Your opinion in the infosec scene now vs then

All mercenaries. Don't get me started. Not really, not everybody. But that catches my feelings. When the big money entered the scene, we all lost friends and stopped sharing as much as before. The flow of information slowed down, though we still have Phrack, Ekoparty, H2HC, Defcon and the others, it doesn't feel the same. Maybe the great techniques were always kept secret and surfaced only 20 years later, but it seems worse than before.

It's not fair, there's still a lot of people believing in full disclosure for a better World, and they do a great job at it. My special admiration and respect to "The Qualys Security Team", who keeps showing art and dedication in every single advisory.

My respect too to Google's Project Zero. There should be an invite only conference on 0-day hunting, where these heroes share their experience and fishing techniques. Kill the class, not the single bug, or better fix both.

And Kill the 0-day!

Recommendations

Technical Books:

- Phrack. 40 years of fun and profit. Hard cover.
- Computational Geometry - Algos and Apps (<3 sweeping line <3)

Thirty Years Later: Lessons from the Multics Security Evaluation Reflections

Hacker Spirit:

Understanding how things work, finding a way around limits, and sharing it with others, to make understanding easier, Loop. The three things together. On the attackers side, there's too much money for a healthy competition and open sharing, MAYBE it's easier on the defender's side. Kill the 0-day!

Exploit Industry:

The monetization of the vulns and exploit has clearly made the power imbalance even worse and broke the flow of information. The way out IMHO, is to double up and openly share even more. It may get worse at first, but it'll be positive at the end.

Career Burnout:

I left security to go do satellites, to then come back. It was also great to move to the defenders side, and see things from a different PoV. Don't be afraid of going out of your comfort zone. If you love learning and doing new stuff, then, do new stuff and learn. ¯_(ツ)_/¯

Insights

Hacking Milestones:

Learn assembly and solve all CTFs you find online, before 20. Write ASCII self decoding shellcode, extract data from a blind SQL injection, write a remote shell client-server over a non-standard protocol (icmp, dns, etc), use gdb to install a backdoor in a running nginx and OllyDbg to do the same in Windows, without touching the filesystem, implement a known Cryptographic primitive, understand rainbow tables, implement a TCP/IP stack, solve some of the advanced cracking challenges by ricnar and most ABOs, write a remote heap overflow that always works, reverse engineer an unknown server with crypto back to C, implement its client in python... all before you are 25.

IT's not my story, but a HACKER needs to be the best in every discipline, or keep trying. And remember, with great power comes great fun, and also some responsibility.

Nontraditional Hacking:

Lying when they ask me for personal information they don't really need. It's stupid, but it takes practice to lie when they ask your name or your birth date, and you may need to remember what you said: practice it, pollute DBs. I also love hacking toys for my kids (adding a RC, etc) and fixing things that broke.

The "Art" of Hacking:

Understanding things better than their creators to find the hidden menu options they didn't know they put there.

Personal

Other Interests:

Electronics! Woodworking. Making things. Creating Tech.

Philosophy:

If it has a solution, it's not a problem. And if it doesn't, why worry at all? Carpe Diem, totally, during the night when I'm statistically more productive.

Zines:

Conferences are ephemeral. Zines are forever, and the articles are usually well thought. A blog is fine, but without an editor pushing you to get it done, the quality degrades over time.

Quotes

Yes: Backticks, please, best quotes ever.

And maybe:

"I want room service!" - standing on a pile of trash.

Though the written story is better than the movie.

Closing Thoughts

```
CALL $+4
RET
POP EBX
```