INSIDE DOD ARMED WITH SCIENCE

Who Wants to Work With a Hacker?

FEB. 12, 2020 |
BY KRISTOPHER JOHNSON - DIRECTOR, DOD CYBER CRIME CENTER VULNERABILITY DISCLOSURE PROGRAM

Do you want to work with a hacker? While the answer is usually a resounding “no” for many organizations, the Defense Department’s Cyber Crime Center Vulnerability Disclosure Program welcomes hackers and has been partnering with them for nearly four years. Of course, I’m talking about ethical hackers, also referred to as “white hat” hackers.

We have hackers from all walks of life, including professional security researchers, academics, soldiers, airmen, DOD contractors and others. I’m also happy to say that hacking is no longer just a male activity. We’ve been fortunate to work with some tremendous women, as well.

Kristopher Johnson, director of the Vulnerability Disclosure Program in the Defense Department's Cyber Crime Center.

The disclosure program evolved from the "Hack the Pentagon" event, led by our good friends at the Defense Digital Service, which truly kick-started the partnership between the DOD and the white hat community. In addition to finding 138 vulnerabilities, they also uncovered a need for DOD to have an enduring open door for hackers to report the vulnerabilities they find. Enter the Vulnerability Disclosure Program. On Nov. 21, 2016, we started what has become the largest disclosure program in the world.

Working with hackers to improve an organization's cyber hygiene was considered a revolutionary idea in 2016, but it has evolved to become almost commonplace in DOD. "Hack the Pentagon" invited a few select hackers to scan a very limited set of systems for vulnerabilities. The resulting disclosure program opens up the aperture and allows anyone with an internet connection to report on any public-facing DOD website.

A common question we receive is can these ethical hackers be trusted? They are hackers after all. To top it off, VDP doesn't give cash payments to its ethical hackers. So, what's the incentive for ethical hackers who partner with DOD's disclosure program? Credibility! That's right, credibility. They work toward gaining credibility and earning a good reputation, which may lead to work opportunities such as "invitation only" private bug-bounty programs. The Vulnerability Disclosure Program's cybersecurity researchers are ranked on a leaderboard managed by HackerOne, a talent management agency for the world's top hackers that also serves as a vulnerability and bug-bounty reporting platform service for businesses and DOD.

Trust is the foundation of the disclosure program. The white hat hackers trust that VDP will provide them with the legal, safe harbor if they follow the guidelines spelled out in policy that the hackers are required to affirm. They trust that VDP will always deal in good faith with those who discover, test and submit vulnerabilities. They trust that we will always err on the side of openness and transparency with them. We trust that the hackers will follow the policy and do no harm. I am happy to report that trust is at an all-time high, with no incidents reported on either side in the three years that VDP has been in operation.

Working with ethical hackers has been, and continues to be, a win-win. Since VDP was established in 2016, 12,925 vulnerabilities have been reported; 70 percent were confirmed to be valid and required mitigation. Of those, 100 percent were unknown to DOD, and more than $65 million has been saved by averted cyberattacks. There has also been an incalculable increase in the cyberhygiene of major DOD websites -- including myPay, AMRDEC Safe, DTS and all MILDEP sites (army.mil, af.mil, etc.). Another benefit is the knowledge VDP is able to share with our counterparts at the

Department of Homeland Security Cybersecurity and Infrastructure Security Agency. They've spent the past 12 months preparing to execute Binding Operational Directive 20-01, which establishes VDPs for all of their departments and agencies.

As mentioned, this is a win-win scenario. The VDP provides a large, safe training ground where younger and inexperienced white hat hackers can learn. There is no shortage of websites for the 1,460 (and growing) VDP hackers to actively test their various operating systems, software packages, tools and tactics. Those who go above and beyond are recognized with a "Researcher of the Month" award on our Twitter page. In February, VDP will announce the "2019 VDP Researcher of the Year" and mail them a box of swag as a token of our appreciation. The researchers, once given permission by VDP, have also used VDP reports on their personal blogs, video tutorials, presentations and academia. Many of the hackers that made it to our online leaderboard have also become professionals in the field. VDP is a great way to start hacking and build a resume that will get you invited to many of the paid programs.

In looking ahead, VDP has several very interesting initiatives that we are looking to roll out in the next 12 months. We are working on a policy update to expand the VDP scope from DOD websites to all DoD Information Systems. Since the program started in 2016, some hackers have submitted amazing -- but out of scope -- vulnerabilities on systems not covered within the existing policy. I believe we are ready to enter into an era of "see something, say something." This will allow the researcher community to disclose anything they find outside of DOD's scope, while being afforded the legal, safe reporting mechanism.

VDP is also exploring ways to support the Defense Industrial Base to better protect the DOD's supply chain. We have partnered with the Defense Counterintelligence and Security Agency to conduct a nine-month feasibility study on what a Defense Industrial Base disclosure program would look like. We are trying to determine if there is a need at small- to medium-size companies, the legal framework for the federal government to provide this service, and the estimated cost.

It is a great time to be a white hat hacker, and we encourage those who are interested to look into the various resources available. We are starting to see many high schools, colleges and universities offer ethical hacking curricula. There is also the Certified Ethical Hacker qualification through the International Council of Electronic Commerce Consultants. However, you can also start off the way many of our researchers do -- by

downloading Kali Linux and checking out the tutorials, videos and blogs online. Coding experience is also tremendously helpful, and several languages -- including Python, HTML, Java and C++ -- are good places to start.

Happy hacking from your friends at DC3VDP!
