Practitioner Perspectives

WOLF DEN ASSOCIATES, LLC

August 2017 *(Vol. 6; Issue 8)*

Top Attack Vectors that are Still Relevant in 2017 (like it's 1999)

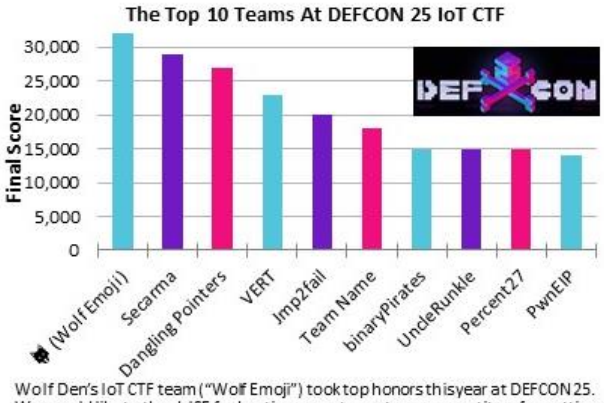
1. ***Default administrator passwords***
2. ***Windows XP on the backend***
3. ***Unpatched software/service/OS (wannaCry)***
4. ***Devices that are running telnet - for no reason (cleartext protocols)***
5. ***Exposure of unnecessary services (FTP, Telnet, and UPnP)***
6. ***Input validation (e.g., SQLi, XSS, and CSRF)***
7. ***Running code/services at root/admin (command injection)***
8. ***Untrained Employees (Spear Phishing and CSRF)***
9. ***Unsecured LAN (Gateway is single point of failure)***
10. ***No virus scanner on email server or desktops/laptops***
11. ***Home office networking equipment in the enterprise***
12. ***No WiFi password or use of old WiFi encryption protocols***
13. ***Unencrypted hard drives on laptops***

The Dog Days of DEFCON

- If you are developing IoT devices, spend the time and money to fully test them – you don't want them to be part of the next botnet
- Compliance checklists do little to improve security posture unless augmented with active and independent white-hat testing
- The IoT Cybersecurity bill is a major step forward and recognizes the scope and scale of the threat posed by IoT vulnerabilities
- Invest in products and companies with hands-on cyber security bona fides and who deploy firmware fixes for compromised devices
- Consider joining us next year – DEFCON is a great place to catch up with former colleagues, potential hires, competitors, and customers
- Steel sharpens steel – consider redirecting training budgets to make room for CTF competitions like the IoT CTF that have higher ROI

Right Now

In 2016, we explained how proliferation of Internet of Things (IoT) has introduced major security vulnerabilities for home and office networks, evolving from a discrete niche to the tail that is wagging the dog in cybersecurity. This threat continues to increase, fueled in part by the widespread use of smart tv and home devices (e.g., Google Chromecast and Amazon Echo). This pervasiveness was reflected at DEFCON 25, with many new Villages exhibiting an IoT focus: Car Hacking, Industrial Control Systems, and even a Voting Machine area. These vulnerabilities are well known within the hacking community, yet they persist through device upgrades and release cycles. The federal government has taken notice with the introduction of the IoT Cybersecurity Improvement Act of 2017 to levy basic security requirements and standards on IoT devices.



Wolf Den's IoT CTF team ("Wolf Emoji") took top honors this year at DEFCON 25. We would like to thank ISE for hosting a great event, our competitors for putting up a good fight, and our employees who are now owners of coveted "black badges."
Source: https://www.sohopelesslybroken.com

Dance The Night Away

Despite the location in fabulous Las Vegas, DEFCON is far from a boondoggle. For 2½ days, 26,000 attendees from around the world comprising 86 teams of hackers competed hunched over cramped rows of laptops in a windowless ballroom that left us longing for the luxury of our usual SCIF accommodations. The goal of the "SOHOplesslybroken" competition is to amass points by compromising the most IoT devices before other competitors. The Wolf Den team toiled ceaselessly to score points in the IoT Village by day and researched additional exploits in our Rainman suite by night. In the end, we were the first team to compromise all 18 devices and did it in just over 14 hours. With the remaining time, we replaced the readout on an LG refrigerator with a picture of our favorite wolf, but we know nothing about the erratic behavior of the Caesars Palace elevators.

Runnin' With The Devil

While the Cybersecurity Improvement Act may seem rote to seasoned hackers, its basic security practices remain critical. As evidenced by our "Top Attack Vectors" list at the left, most vulnerabilities can be combated with basic blocking and tackling. Overall, we see it as far more meaningful and impactful than the old compliance checklists that comprise the majority of system security plans. Vulnerability scans and risk assessments are necessary, but not sufficient, and must be augmented with active penetration testing. We especially like the Act's proposed exemption from liability for cybersecurity practitioners engaging in good-faith research. Too few cyber security teams perform hands-on research anymore. Similarly, too many consumers hire cyber security charlatans on the basis of pernicious PowerPoint promises and common compliance cowardice.

Here We Go Around…

While participating in the various competitions at DEFCON over the past several years, we continue to be surprised that none of the other 85 competing teams were people we regularly run into in federal or even commercial markets. As far as we could tell, we were the only service provider there, which leads us to conclude that the other "usual suspects" either shy away from competition or have already blown their training budgets on big production, low value affairs. We have always abided by the mantra that "steel sharpens steel", so why not compete on the global stage? Competitions like this provide the best possible way to test your mettle in real world scenarios that cannot easily be replicated in antiseptic classrooms or labs. Also, there is nowhere to hide in cyberspace, so if you are competing incognito you are only fooling yourself, not your prospective clients or your adversaries.

1751 Pinnacle Drive
McLean, VA 22102
wolfdenassociates.com

Will K.
(404) 939-7364
Will@wolfdenassociates.com

Rick T.
(703) 638-5924
Rick@wolfdenassociates.com

Ian K.
(571) 253-2522
Ian@wolfdenassociates.com