Tuesday AUGUST 6

This schedule is also available at **bsideslv.org/schedule**

2019 BSides Las Vegas

Time markers: 0800 0900 1000 1100 1200 1300 1400 1500 1600: HAPPY HOUR 1700 1800 1900

Middle Ground
Florentine C&D

PvJ CTF Begins | Opening Remarks | **KEYNOTE:** Bob Lord | Lock Pick: Beginner lesson | PvJ CTF ENDS | Lock Pick: Contest | Raffle Draw | PvJ CTF End of Day Hotwash
Silent Auction Begins | | | | | Hacker Standup Comedy

Hire Ground
Florentine B

Now that you hacked the plane, what you going to do about career? | Addressing non-linear InfoSec career paths | Discovering Your Passion in Cyber Security | Hack (Apart) Your Career-How to Fund Doing What You Love | How to Fail Well (to be Success-ful)-From IT to Infosec | Behind Recruit-ing Curtain: What Recruit-ers Really Say and Do

Networking [all day] | Career Coaching & Résumé Reviewing

Breaking Ground
Florentine A

Keynote Q&A with Bob Lord | BEEMKA / Electron Post-Exploitation When The Land Is Dry | Unpacking pkgs: A look inside macOS Installer packages and common security flaws | Using Machines to exploit Machines-harnessing AI to accelerate exploitation | Meltdown's Aftermath: Leveraging KVA Shadow To Bypass Security Protections | Neurosecurity: where Infosec meets Brain-machine Interface

Proving Ground
Florentine G

Bestsellers in the Under-ground Econo-my-Measuring Malware Popu-larity by Forum | Examining DES-based Cipher Suite Support within the TLS Ecosystem | Satellite Vulnerabilities 101 | Analyzing user decision making on phishing sites - using mouse data, keyboard dynamics | Broken Arrow: apply-ing InfoSec and Forensic practices to escape domes-tic abuse | The Human API: Evolving End Users From Autho-rized Adver-saries Into Our Best Defense. | Burpsuite Team Server-Collaborative Web Pwnage | The Resilient Hacker: Growth Mindset, Health Hacks & Power-ful Help to Navi-gate Personal Challenges | So you think you can CHMOD | Building the badge-How you can make small, cheap and custom hard-ware for func-tion or fashion | Salesforce Data Governance What dark secrets lurk in your instance??

Common Ground
Florentine F

DLP Sucks and Why You Should Use It | Where in the world are Carmen's Sadjective cyber attacks: The game show that wonders why things aren't worse | The Contemplator Approach: Data Enrichment Through Elastic Stack | Mind the Diversity Gap-A Panel Discussion | Meet the CISO

Underground
Florentine E

Duck and (Re)Cover-The missing link in the security evolution | Reverse Engineering Mobile Apps: Never Pay for Transit Again | Giving Credit Where It's Not Due: Visualizing Joker's Stash | China as a New Russia? Analyzing Similarities and Differences of Chinese Threat Actors from their Russian Counterparts | Ask the EFF

Ground Truth
Firenze

Applying Information Security Paradigms to Misinformation Campaigns: A Multidisciplinary Approach | Building an enterprise security knowledge graph to fuel better decisions, faster | Grapl-A Graph Platform for Detection and Response | Profiling User Risk: Borrowing from Business Intelligence to Understand the Security of Your Userbase | Reducing Inactionable Alerts via Policy Layer | Trying (Unsuc-cessfully) to Make Meter-preter Adver-sarial Example | Evaluating Code Embeddings

Ground1234!
Tuscany

SSO Wars: The Token Menace | My quest for (privileged) identity to own your domain | Enterprise Overflow: How Breached Credentials Impact Us All | Give the dog a bone-Exploring OSINT capabilities of pen-testing tools | Why FIDO Security Keys & WebAuthn are Awesome

I Am the Cavalry
Siena

IATC Welcome & Overview | Can the CAN bus fly—Risks of CAN bus networks within avionics systems | Coordinated Disclosure of ICS Products: Who's got time for that? | Als Wide Open-Making Bots Safer Than Completely $#%cking Unsafe | The Case for Software Bill of Materials | Automatic Security Analysis of IoT Firmware | I Just Want to Help Make Flying More Secure. . .not Work with the Government or How I Learned to Love a Govvie

The Quiet Room

Copa Room, Tuscany ground floor, near casino: Relax and step away from the conference hustle. This space is reserved for people who need a quiet environment to recharge, think, or just rest their ears.

The following sessions are at the PLATINUM HOTEL

Training Ground 1
Malware Traffic Analysis Workshop | Malware Traffic Analysis Workshop [cont.]

Training Ground 2
Windows Breakout and Privilege Escalation | Windows Breakout and Privilege Escalation [cont.]

Training Ground 3
Hack Back! Malware Reverse Engineering and Command & Control Server Exploitation | Hands-on: How to Use CALDERA's Chain Mode

Training Ground 4
Knowing the Unknown: Using PCAP to Break Down Application-Layer Protocols | Active Directory security: 8 (very) low hanging fruits and how to smash those attack paths

CISO Summit
Board Communications (NACD) | Zero Trust (Duo Security) | Supply Chain Security (Panorays) | AppSec/SDLC/DevSecOps (Whitehat) | Crisis Communication & Brand Monitoring (ZeroFOX) | CISO Unconference

Public Ground
Professionalization-Possibilities and Potholes | Reverse Engineering the Cyber Policy API | What's Next in Coordinating Vulnerability Disclosures | Als Wide Open—Making Bots Safer Than Completely #$%cking Unsafe

Special Thanks to **The Hewlett Foundation** for sponsoring Public Ground.

Evening time markers: 1900 2000 2100 2200 2300 0100 0200 0300 0400

Evening Events

Volunteers Meetup at The Tuscany Pool | **QueerCon Mixer** at The Tuscany Pool

BSides Organizers Meetup in Siena

The New Hacker Pyramid in Middle Ground

Hacker Karaoke in Pub 365 back room, Tuscany ground floor

Time columns: 0800 · 0900 · 1000 · 1100 · 1200 · 1300 · 1400 · 1500 · 1600: **HAPPY HOUR** · 1700 · 1800 · 1900

Middle Ground — *Florentine C&D*
- PvJ CTF Begins
- Lock Pick: Beginner lesson
- PvJ CTF ENDS
- Lock Pick: Contest
- Raffle Draw
- Hacker Standup Comedy
- PvJ CTF End of Day Hotwash
- Silent Auction ENDS
- BSides Las Vegas 2019 Closing Ceremonies
- Final Raffle Draw

Hire Ground — *Florentine B*
- The Importance of Culture in Security
- Hacking from Above: A Brief Guide for Transitioning to Leadership
- Noobs: Training the Next Generation of Security Engineers
- Startup Security Leadership: Lessons to Level Up from Fortune 100 to Tech Startup
- Career Coaching with Pete Cooper, Brian Markham
- Networking [all day]
- Career Coaching & Résumé Reviewing

Breaking Ground — *Florentine A*
- Loki: Add a little chaos to your USB drive
- From EK to DEK: An Analysis of Modern Document Exploit Kits
- From email address to phone number
- Virtual Breakpoints for x86_64
- ROP with a 2nd Stack, or This Exploit is a Recursive Fibonacci Sequence Generator
- At Your Service-Abusing the Service Workers Web API
- State of DNS Rebinding-Attack & Prevention Techniques and the Singularity of Origin

Proving Ground — *Florentine G*
- Making your website vulnerable for fun and security awareness
- Human honeypots, or: How I learned to stop worrying and love the NFC Implant
- The struggles of teaching automation
- The SOC Counter ATT&CK
- The drunk colonel and the flipped stone: Game Theory for a Defensive Strategic Advantage
- I'm a hunter! But what does that mean?
- Breaking the Bodyguards
- Cover Your A**
- Cyber Deception after Detection: Safe observation environment using Software Defined Networking
- Deepfakes, Deep Trouble: Addressing Potential Market Manipulation Caused by Deepfakes
- Baited Canaries-Monitoring attackers with active beacons
- Securing Fast (and Furious) DevOps pipelines
- Please inject me, a x64 code injection

Common Ground — *Florentine F*
- The Road to Hell is Paved with Bad Passwords
- Prisoner Number Six
- Excuse Me, Your Sword Is In My Eye: Responding to Red Teams and 'IRL' Threats in 2019 and Beyond
- Escape Questionnaire Quagmire: thoughtful approach addressing security inquiries customers & prospects
- Getting CVSS, NVD, and CVEs to Work for You: Standardizing and Scaling Your Vulnerability Risk Analysis
- Have You Distributed Randomness?
- CloudSec Rules Everything Around Me (C.R.E.A.M.)
- Meet the Nation This Week on Sunday: A Special Vulnerability Edition

Ground Floor — *Florentine E*
- CTFs for Fun and Profit: Playing Games to Build your Skills
- Hidden Networks Pivoting: Redefining DNS Rebinding Attack
- Low & Slow-Techniques for DNS Data Exfiltration
- Windows 10 DFIR Challenges
- ATT&CKing Your Adversaries-Operationalizing cyber intelligence in your own environment for better sleep and a safer tomorrow
- Cyber Threat Intel & APTs 101
- Musings of an Accidental CISO

Ground Truth — *Firenze*
- Security data science-Getting the fundamentals right
- Is This Magikarp a Gyarados?: Using Machine Learning for Phishing Detection
- Old things new again: efficient automatic signature generation for malware classification
- Reduce, Reuse and Recycle ML models-and the security powers is yours
- Scheming with Machines: Using ML to Support Offensive Teams
- Birthday Hunting
- All that glitters isn't Chrome: Hunting for suspicious browser extensions
- Scratching the Surface of Risk

Ground1234! — *Tuscany*
- Breaking Smart [Bank] Statement
- An investigation of the security of passwords derived from African languages
- (Im)proper Database Authentication
- Who dis? The Right Way To Authenticate
- Exploiting Windows Group Policy for Reconnaissance and Attack
- Why can't we be friends? (Ask a Fed & the EFF.)
- Ham Exams

I Am the Cavalry — *Siena*
- How to Treat Your Hacker (and Responsible Vulnerability Disclosure)
- Hacking the Pentagon: How a Rebel Alliance Shifts Culture to Protect National Security
- Certification and Labeling in IoT
- Real World Security in a Clinical Healthcare Environment: Hacking a Hospital
- Why journalists and hackers need each other (a panel discussion with infosec reporters)
- We the People: Providing for a 'common defence' with CVD
- No IOUs with IOT
- "Hackers of the world-unite?"

The Quiet Room
Copa Room, Tuscany ground floor, near casino: Relax and step away from the conference hustle. This space is reserved for people who need a quiet environment to recharge, think, or just rest their ears.

The following sessions are at the PLATINUM HOTEL

Training Ground 1
- Using Wireshark for Incident Response and Threat Hunting
- Using Wireshark for Incident Response and Threat Hunting [cont.]

Training Ground 2
- Hacking the STORM
- Hacking the STORM [cont.]

Training Ground 3
- Introduction to Cryptographic Attacks
- Hands on Hacking The OWASP TOP 10 and beyond

Training Ground 4
- Linux Hardening—The Easy Way
- Pentesting ICS 102

Training Ground 5
- Tournament: The Ultimate Secure Coding Throw Down
- Finding Evil with Mitre ATT&CK and the Elastic Stack

Public Ground
- Free and Fair Elections in an Internet Era
- Let's hear from the Hackers: What should DOJ do next?
- Certification and Labeling for IoT
- Why we need a Cyber Peace Institute

Special Thanks to **The Hewlett Foundation** for sponsoring Public Ground.

Evening timeline: 1900 · 2000 · 2100 · 2200 · 2300 · 0100 · 0200 · 0300 · 0400

Evening Event
BSidesLV Pool Party at The Tuscany Pool

Drink, eat, and float around the Tuscany's fantastic pool while listening to **djdead**, **Jackalope**, **An Hobbes**, and **Circuit Static** playing the best music you've never heard before. Bring your swimsuit & badge!