



White Wolf Security/SANS ICE II

October 1 – 3, Caesar's Palace, Las Vegas

Integrated Cyber Exercise (ICE) hosted at SANS Network Security 2008

LIVE HACKING

Real networks, real data, real attacks. Come watch some of the world's best security professionals attack live systems in an all out competition.

LIVE ATTACK DATA FOR YOUR PRODUCT

Katana sponsors can drop their security devices into the infrastructure and show attendees how their product works in a live environment.

SPECTATORS

Come watch the 3D scoring and listen to commentary from PaulDotCom. Or better yet; participate. Spectators are provided phones and computers to interact with the defending and attacking teams in real time.

CONFERENCE ATTENDEES

SANS attendees search out technical solutions to take back to the office and want to see live demos to continue the learning process. Consider the pre-qualifiers: attending a 6 day track at SANS costs an attendee's employer over \$3,000 for tuition alone. Factor in the cost of time away from the office, travel and hotel and you have a sizeable investment in security education.



- Welcome to the most complex cyber exercise competition of its kind hosted at the top information security training event in the world.
- Defenders must protect complex networks including power grid nodes, phones, cameras and servers.
- Attackers are given free rein to attack whatever they want, however they want. Come see how real hackers operate when there are *no consequences* for their actions.
- Choose your Pack; Defend, Attack or Field Op. They all have missions and only some will survive.
- Three evenings of competition. October 1 – 3rd, 5pm to 10pm at Caesar's Palace

The Scenario

Welcome to The Hunt Group; a non-governmental organization which maintains balance in the world by doing things governments cannot. As a recently hired IT administrator for The Hunt Group, you are charged with keeping their critical servers up and operational while providing field operatives access to classified data. Several non friendly nations and non-nation actors are actively attempting to penetrate Hunt Group networks in an effort to steal or destroy classified data, plant back doors and to prevent successful mission completion by field ops.

Attackers – you will be responsible for disrupting Hunt Group field operatives by breaking into classified servers. Find agents' true identities by cracking the HR server; bleed off operating funds by hitting the bank or even take over surveillance cameras and spy on the enemy.

Defenders – the odds are against you. You must keep systems up and feeding data to the agents in the field. You have to keep the attackers out but let the field ops in.



White Wolf Security/SANS ICE II

October 1 – 3, Caesar's Palace, Las Vegas

ABOUT SANS

SANS is the most trusted, and by far the largest, source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security.

SANS also operates the Internet's early warning system - Internet Storm Center.

ABOUT WHITE WOLF SECURITY

White Wolf Security has driven the market in information security training. In 1999 we taught one of the first hands on hacking courses. Exercises are the next logical evolution of training and once again, White Wolf Security is leading the pack by providing the most realistic exercises on the market today.

About SANS Las Vegas

SANS Las Vegas is the premier training event of the fall. Last year over 1400 students attended the SANS Las Vegas event. This year, we are expecting even more. The ICE 2008 event is open to all registered SANS Las Vegas students at no additional charge. The event is open in the evenings to maximize exposure while not interfering with the daily classes.

Sponsorship Levels

Tanto (\$5,000)

- Listing on the SANS ICE 2008 event website
- Listing on the White Wolf Security ICE 2008 event website
- Logo placement on event signage at the conference
- Logo placement in exercise program on sponsor page
- Mentioned in Pauldotcom Podcast for the event
- Placement of company literature on the sponsor table at the event
- Send two company personnel to the event; access to spectator room

Wakizashi (\$10,000)

- Everything in Tanto plus
- Banner placement at the event
- Mentioned in Pauldotcom Podcast prior to the event
- Sponsor prize give away (random prize drawing for the prize of your choice up to \$500)
- Logo placed on scoring engine (on display during course of exercise)
- Place a player on Red and Blue teams and one sales representative with access to the spectator room.
- 3 Event Passports for VIP customers
- Mention in a SANS newsbites email campaign (circulation approx 180,000)
- ½ page ad in exercise program and one white paper (maximum 4 pages 8.5x11)

Katana (\$25,000)

- Everything on Wakizashi plus the ability to place your equipment in the exercise and display the results in the spectator room
- IDS sponsor (1 only)
- Full packet capture sponsor (1 only)
- Web application firewall sponsor (1 only)
- Place a player on Red and Blue teams and one sales representative with access to the spectator room.
- 5 Event Passports for VIP customers
- Full page ad in exercise program and one white paper (maximum 4 pages 8.5x11)
- Table in the spectator room



White Wolf Security/SANS ICE II

October 1 – 3, Caesar's Palace, Las Vegas

MULTIPLE EVENTS

Because White Wolf Security runs cyber exercises year round we are in the unique position of offering an annual sponsorship package. The more you sponsor, the more you save. Sponsor two events and save 5% off the total price. Sponsor three events and save 10% off the total price.

SANS 2007 ATTENDEES

Here are just some of the organizations from last year's SANS training in

Las Vegas:

- US Navy*
- US Air Force*
- US Army
- Mutual of Omaha*
- Boeing
- Charles Schwab
- FBI
- Fidelity Investments
- General Electric
- Janus
- JP Morgan Chase
- Key Bank
- Lawrence Livermore Nat'l Lab
- Los Alamos Nat'l Lab
- Sandia National Lab
- Wells Fargo
- Sprint, Verizon
- SPAWAR
- Tim Warner Cable

* Participated in ICE I at SANS Las Vegas, 2007

Special Sponsorship

- Johnny Long as opening night keynote speaker - \$15,000
- Badge and Lanyard (qty 100)– co branded with WWS and your company logo/name; distributed to all exercise players and spectators - \$5,000
- Back cover of exercise program (8.5 x 11) - \$5,000
- Inside front or back cover of exercise program (8.5 x 11) - \$2,500
- Full co-sponsorship of event - \$75,000, event co-branded with White Wolf Security
- Custom moleskin journal (qty 100) – co branded with WWS and your company name - \$6,000
- Polo shirts price and quantity dependant on venue
- Hackers for Charity sponsor:
 - Tanto sponsors can choose to have \$100 of their sponsorship dollars donated in their name to Hackers for Charity
 - Wakizashi sponsors can choose to have \$250 of their sponsorship dollars donated in their name to Hackers for Charity
 - Katana sponsors can choose to have \$500 of their sponsorship dollars donated in their name to Hackers for Charity
- Hardware and software sponsors – taken on a case by case basis.

Tanto Sponsors



Software Sponsors



Hackers for Charity

Giving back to the global community is part of our culture. We have partnered with Hackers for Charity to help those in need with the tech skills we possess. A portion of the proceeds will be donated to help further the cause.



White Wolf Security/SANS ICE II

October 1 – 3, Caesar's Palace, Las Vegas

REAL INFRASTRUCTURE

Real IP addresses, real servers and lots of real data. Nothing is simulated. The e-commerce database has over 10,000 customers. The central login server has over 11,000 employees. There is real data that needs protecting from real attacks.

LIVE DATA FOR YOUR TOOLS

The entire exercise backbone is designed to support multiple span ports and network taps. This backbone allows you to place your network device (packet capture, IDS, IPS, etc) and quickly give you access to the traffic flow for an entire team.

CALL TODAY FOR MORE INFORMATION

Call 717-295-6201 and speak to Joe DeCree for more information.

Or you can email at joe@whitewolfsecurity.com

Or visit us online at www.whitewolfsecurity.com

What is an ICE?

ICE is the Integrated Cyber Exercise; a scenario that puts a group of Red Cell hackers against multiple teams of Blue Cell defenders. Each defending team is given a small network infrastructure with a router, firewall, servers and desktops. The Blue Cells are responsible for keeping their network alive and functional with real services such as email, e-commerce and DNS. The Red Cell is responsible for attacking the Blue Cell network.

Real data, live networks

The ICE network is a real world replica of sections of the Internet. Real IP addresses, Root DNS servers, public VoIP servers and even SCADA devices are on the network for both attackers and defenders to use. Databases are populated with data and login servers have thousands of users.

Spectators can play, too

Spectators are loaned desktops and VoIP phones and are encouraged to interact with the live environment. They can call into the Blue Cell, send traffic or even form alliances with the Red Cell and forward attacks.

Key features and scoring

The ICE network not only facilitates the exercise, but is designed to collect data and simulate a wide array of network activities. Some of the key features of the exercise:

1. MapQuest driven scoring engine that geo plots IP assets and shows their status across geographic regions.
2. 3D visualization of scoring rounds.
3. Tracking and scoring of Red Cell and Blue Cell performance.
4. Dynamic business injects – emails sent to teams that simulate real world business requests.
5. Full packet capture – all the traffic across the defenders' firewalls is captured using custom built full packet capture devices.
6. Distributed intrusion detection.
7. Spanning and trunk port replication allows you to compare IDS systems against identical traffic.
8. Full SCADA support – custom built IP SCADA devices control power flow to the teams.
9. Full VoIP support – we can implement any call list or phone number scheme necessary.
10. Distributed client side traffic generation. Custom built traffic generator to send/receive traffic from anywhere in the network environment.