GSE Rumors, Myths, and Facts

Jeff Pike
jpike@giac.org
What is the GSE?

- GIAC Security Expert -> GSE
- The most prestigious Information Security certification in the world
- The broad-based IT Security Cert with an intensive hands-on lab
- 29 issued to date (since 2003)
- Approaching a tipping point
  - Demand at all time high
Benefits of GSE to Holder

- World wide recognition
- High demand, low availability
- Renews all of your GIAC certifications as long as you maintain it
  - GSE maintained via one multiple choice test after year four
Benefits of GSE to Community

- Only top-tier hands-on credential in the world for IT Sec pros.
- GSE is designed for the top technical security practitioner in an organization. -- You want to be sure that your top gun can do this stuff.
GSE – Pre-requisites

- Evolved to let more people play:
  - GSEC, GCIA, GCIH with two gold
  - GSEC, GCIA, GCIH with one gold plus one 500 level cert
  - GSEC GCIA, GCIH plus two 500 level cert
  - GCWN and GCUX can be subbed for GSEC
GSE – Pre-requisites (2)

- GIAC Gold is no longer officially required, however:
  - We find that people holding one or more GIAC gold certifications do better in the lab, than those who don’t.
  - GIAC Gold is strongly recommended in one or more pre-requisites
GSE Objectives – Five Domains

- http://www.giac.org/certifications/gse.php
- Expert-level knowledge is not just a subset of GSEC/GCIH/GCIA
- The E in GSE = Expert
- The E means you need to prove you have the hands-on ability to get things done
- No practice tests
Steps to obtaining the GSE

- Fulfill all pre-requisite requirements
- Apply (no-cost to apply)
- Take the proctored multiple choice component ($399)
- Register and take the hands-on lab component ($1,199)
Myth
GSEC shouldn’t be a pre-requisite

- GSEC is required because general security knowledge is very relevant
- Unix, Widows, and Firewall security are still relevant although GCFW, GCWN, and GCUX are no longer pre-reqs
- Bottom line - If you are GSE-ready you can challenge the GSEC and pass
Myth – GPEN should be a good substitute for GCIH

- GSE is a defensive minded credential
- Objectives have been determined by first GSEs and senior SANS instructors
- Soft skills pertaining to incident handling are required to pass the GSE
- If GCIH is so easy, challenge it
- You’re a pen-tester; adapt!
Rumors/Myth
The GSE is way too hard

- It’s not super hard, it is comprehensive
- It’s broad, but relevant. The breadth adds depth.
- The hands-on exercises are designed to test problem solving skills
- “Tough but fair” is the comment we most often hear after the GSE lab.
Rumor/Myth – I can’t register without knowing lab schedule

- FALSE – We’ve never had a single person pay for the lab who we couldn’t accommodate
- Pre-qualified GSE candidates actually have more influence over GIAC lab schedule than anyone else
GSE Preparation

- Anything you can do to gain more hands-on experience will help you prepare for the GSE
- Re-work or simulate all hands-on exercises for relevant SANS courses
- Use vmware workstation to simulate a network environment at home and practice with focus on the GSE certification objectives
GSE Preparation (2)

- Configure a sniffer outside your home network firewall and analyze traffic
- Generate and analyze malicious and normal traffic on your own
- Sign-up for dshield and follow incidents.org closely
GSE Preparation (3)

- Attack a vulnerable test network at home, harden it and repeat
- Consider netwars and other hands-on challenges to sharpen skills
  [http://www.sans.org/netwars](http://www.sans.org/netwars)
- Tackle a GIAC Gold project
GSE Preparation (4)

- Practice hardening different Windows and Unix systems
- Practice configuring firewalls, encryption technologies, and using the most common security tools
- Play with the technology!
Current GSE Lab Configuration

- Exercises are open book
- Internet access allowed on GIAC-provided community machines for research
- Using your own Windows laptop using GIAC issued VMs and tools
- Work is graded independently
Current GSE Lab Configuration (2)

- Backtrack 4
  - most of the security tools you need
- Windows – your choice
- Fedora Core 12
- Numerous un-known hosts
- GIAC provides all VMs.
GSE - Conclusions

- Not for everyone
- Designed for top tier technical professionals
- Demand has always been high
- How many does the world need?
- Expect it to become hot!
Questions?

- E-mail Jeff Pike at jpike@giac.org
- Check out http://www.giac.org/gse.php