The Hacker Profiling Project
general overview

Project Leaders
Raoul Chiesa
raoul@ISECOM.org
Dr. Stefania Ducci
stefania@ISECOM.org

Document Keywords

HPP General Overview, HPP Introduction, Cybercrime, Hacker Profiling, Criminal Profiling, Honeypots, Honeynets, Computer Intrusion, IT & ICT Attack Anatomy, IT & ICT fraud.

Disclaimer

- The use of this document is under ISECOM's document licensing.
- The information contained within this presentation does not infringe on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- Quoted trademarks belongs to registered owners.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

Hackers Profiling Grid

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

Project Leaders

Raoul Chiesa

- ***Director of Communications*** at ISECOM
  - **Institute for Security and Open Methodologies** (Est. 2002)
  - Originally called the Ideahamster Organization (Est. 2001)
  - **Non Profit Organization** Registered in Spain and U.S.A.
  - **Open Source Community** Registered OSI
- **Project Manager for H.P.P., OSSTMM Key Contributor**
  - OPST, OPSA, ISECOM Authorized International Trainer
- ***Professor of IT Security*** at various Universities & Masters (Italy)
- ***Board of Directors Member*** for I**SECOM**, **CLUSIT**, **Telecom Security Task Force** (TSTF.net)

Project Leaders

Dr. Stefania Ducci

Stefania has a **University degree in Law** (University of Bologna - 2002), and a **Master degree in Criminology** (University of Turin - 2003).

She works for **UNICRI** (United Nations Interregional Crime And Justice Research Institute), a UN agency, dealing with crime and criminal justice.

In 2004 she began collaborating with Raoul Chiesa on **personal basis**. The studies carried out in team formed the core of H.P.P. Project.

For the Hacker's Profiling Project, Stefania has used an **independent research approach**, providing her support and cooperation during her spare time, fascinated by the huge research possibilities and professional evolution offered by the Project.

Her principal interest consists in reading hacking and "classic" criminal profiling books.

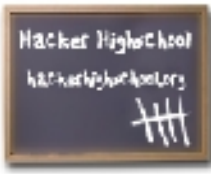
The ISECOM Mission

- Our Mission:
  - **To provide global, practical, useable security knowledge and knowledge-tools to solve problems caused by insecurity, privacy violations, ethical violations, and poor safety measures.**
- Our Audience:
  - **Governments, Corporations, Organizations (OSSTMM, HPP)**
  - **Professionals and quasi-professionals (Rules of Engagement, Metrics)**
  - **College students (Academic Alliance Program)**
  - **Teens and pre-teens (Hacker Highschool)**

The ISECOM Projects

- **OSSTMM** – The Open Source Security Testing Methodology Manual
- **HSM** – The Home Security Methodology
- **BIT** – Business Integrity Testing Methodology Manual
- **BPP** – Bad People Project
- **SPSMM** – The Secure Programming Standards Methodology M
- **STICK** – Software Testing Checklist
- **SOMA** – Security Maturity Model
- **HHS** – Hacker High School
- **HPP** – Hacker's Profiling Project

New!



Scope

- **This presentation will intentionally focus on a general introduction to the Hacker's Profiling Project (HPP).**
- **Further public versions of the HPP are already available upon request and identification, since we are still covering the project's core-development phases.**
- **At this time, the following releases of the HPP presentation have been developed:**
  - ✓ Basic (this one)
  - ✓ Compact
  - ✓ Standard
  - ✓ Full
  - ✓ HPP Book # 1 (under development; expected JAN 2007)
- **The HPP Presentations and Questionnaires are available in the following languages:**
  - ✓ English
  - ✓ Italian
  - ✓ Greek (translation in progress)
  - ✓ Rumenian (translation in progress)
  - ✓ German (under development)
  - ✓ Russian (partnership in progress)
  - ✓ Spanish (under development)
  - ✓ French (partnership in progress)

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

Hackers Profiling Grid

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

The “cybercrime”

Dealing with “hacking-related” security problems from more than a decade, in the last years we observed with attention series of phenomenon defined by us “worrying”:

- A dramatic decrease of the so called “window of exposure”, which is the time between the elaboration of “0-day” exploits and their use in massive attacks and/or distributed at world level;
- Dangerous synergies among technologically advanced personalities, classic criminality (national and transnational) and terrorism;
- Continuous increase of the dependence between national stability (critical national infrastructures, homeland security, telecommunications, fundamental services, etc.) and the ICT Security issues.

Nevertheless, often the cybercrime and hi-tech crime phenomena are analyzed in a wrong manner.

The H.P.P. Project

In this connection, we want to analyze the "cybercrime problem" by using an approach completely different from the ones used till now, going directly to the source.

In fact, the H.P.P. Project is aimed at:

- Analysing the hacking phenomenon – technological, social and economic – in its several aspects, through both technical and criminological approaches.
- Understanding the different motivations and identifying the actors involved;
- Observing "in the field" the (true) criminal actions;
- Applying the profiling methodology to the collected data;
- Learning by the acquired knowledge and disseminating it.

The H.P.P. Phases

The H.P.P. Project started in September 2004 and became an official ISECOM project on June 2006. Till now, we have identified 8 different project phases.

Phase 1 **THEORICAL COLLECTION**
Elaboration and Distribution of the questionnaire, in different forms and towards different targets

Phase 2 **OBSERVATION**
Participation to "IT underground security" events (EU, Asia, USA, Australia)

Phase 3 **FILING**
Creation of a Data-base for the classification elaboration of data collected during Phase 1

Phase 4 **"Live" COLLECTION**
Elaboration and activation of Honey-Net Systems of new generation and highly customized

Phase 5 **G&C ANALYSIS**
Gap-Analysis and Correlation among datas collected through the questionnaire, Honeynets and profiles deducted from the existing literature on the topic

Phase 5/A **HCP "live" ASSESSMENT (24X7)**
Continuous assessment of profiles and correlation of modus operandi, through data collected in Phase 4

Phase 6 **FINAL REPORTING**
Redefinition and fine-tuning of different hacker and profiles previously used as a "standard de-facto"

Phase 7 **DIFFUSION OF THE MODEL**
Final elaboration of results, drafting and publication of the methodology, raising awareness (white papers, lectures, company awareness, training)

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

Hackers Profiling Grid

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

The HPP Questionnaire

- **Module "A"**

Personal data (gender, age, social status, family context, study/work)

- **Module "B"**

Relational data (relationship with: the Authorities, teachers/employers, friends/colleagues, other hackers)

- **Module "C"**

Technical and criminological data (target, hacking techniques and tools, motivations, ethics, perception of the illegality of their own activity, crimes committed, deterrence)

All the questions allow anonymous answers

HPP QUESTIONNAIRE - the delivery

✓ **3 questionnaire typologies:**

- **Level 1**: Full Release

  25 pages, Modules A, B and C expected as "fully completed" (all fields are mandatory)

- **Level 2**: Compact Release

  10 pages, Modules A, B and C to be partially completed (some fields are mandatory)

- **Level 3**: Basic Release

  3 pages, Modules A and C to be partially completed, often uncorrected (few mandatory fields.)

✓ **3 delivery levels:**

- **Known and/or verified, "directly" or not (the QoQ is extremely high), IRL and on-line.**
- **Underground/hacking general contacts (the QoQ is medium), on-line.**
- **Focused Magazines, Other (the QoQ is low), hard-copy and on-line.**

The questionnaire: excerpts

a) Sex:

Male

Female

b) Age:

c) Title of study (please, indicate the last):

Primary school leaving-certificate
Secondary school leaving-certificate
Professional qualification
Degree
Beyond (master, PhD, specialisation, etc.)

d) Country and place of residence (if you don't wish to specify your city, please, indicate the geographical area of residence). Specify also if you live in a city or in a village and, in the latter case, if this is far or not from a big urban centre.

(a) There are other persons in your family who are (or were)interested in IT?

Yes

No

(b) Are there other persons in your family who practise (or have practised) hacking/phreaking?

a) Awareness of your hacking/phreaking activity:

1)

(a) Among your acquaintances, who is (or was) aware of your hacking/phreaking activity? (teachers, employer(s), schoolmates, colleagues, friends, other members of the underground world, partner, and so on).

d) Hacking, phreaking, carding:

1) Do (or Did you) practise:

- hacking Yes No

- phreaking Yes No

e) Kinds of data nets, technologies and operative systems targeted and tools used:

1) On what kind of data nets and technologies do (or did) you practise hacking/phreaking? For example: Internet, X.25, PSTN/ISDN, PBX, Wireless, "mobile" nets (GSM/GPRS/EDGE/UMTS), VoIP.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

Hackers profiling Grid

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

HPP Grid: yesterday

Know your Enemy: preferred targets

PSYCOLOGICAL PROFILE	TARGET
Wannabe Lamer	**End-user**
(I'd like to be an hacker, but I can't…)	
Script Kiddie	**SME/specific security flaws**
(The script boy)	
Cracker	**Big Companies/PA/Finance/Telco**
(Burned ground, the Destructer)	
Ethical Hacker	**Vendor/System Integrator/Telco**
(The "ethical" hacker's world)	
Quiet, paranoid, skilled hacker	**Big Companies/PA/Finance/Telco/R&D**
(The very specialized and paranoid attacker)	
Cyber-Warrior	**Multinationals "symbol"**
(The soldier, hacking for money)	
Industrial Spy	**Multinationals, ICT companies**
(Industrial espionage)	
Government agent	**Multinationals/Governments**
(Governative agent: CIA, Mossad, FBI, etc.	Cuckoo's Egg docet)

(c) 2004, @ Mediaservice.net Srl.
DSDLAB

16

HPP Grid: today

PROFILE	RANK	IMPACT LEVEL	TARGET	
Wanna Be Lamer	Amateur	NULL	End-User	
Script Kiddie		LOW	SME	Specific security flaws
Cracker	Hobbiest	MEDIUM / HIGH	Business company	
Ethical Hacker		MEDIUM	Vendor	Technology
Quiet, Paranoid, Skilled Hacker		MEDIUM / HIGH	On necessity	
Cyber-Warrior	Professional	HIGH	"Symbol" business company	End-User
Industrial Spy		HIGH	Business company	Corporations
Government agent		HIGH	Government	Suspected Terrorist
			Strategic Company	Individual
Military Hacker		HIGH	Government	Strategic Company

Level of technical skills

Wannabe Lamer Script Kiddie Cracker

Ethical hacker
Q.P.S. Hacker
Cyber-Warrior
Industrial spy
Government Agent
Military Hacker

Level of dangerousness

Wannabe Lamer

Script Kiddie

Ethical Hacker

Q.P.S. Hacker

Cracker

Cyber-Warrior

Industrial spy

Government Agent

Military Hackers

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

Evaluation and Correlation standards

- This release of HPP presentation does not cover this chapter.
- The Evaluation and Correlation standards have been based, as for now, on the following fields:
  - ✓ Modus Operandi
  - ✓ Lone Hacker or as a Member of a Group
  - ✓ Motivations
  - ✓ Main Targets
  - ✓ Hacker career and selected targets
  - ✓ Relations between targets and motivations
  - ✓ Fundamentals principles of the so-called "Hacker Ethics"
  - ✓ Crashed or Damaged Systems
  - ✓ Perception pf the illegality of the own activity
  - ✓ Deterrence effect of Laws, Convictions and Technical Difficulties
- The Evaluation and Correlation standards are available to the public, upon identified request.

Hacker top-level typologies view

1. Wannabe Lamer
2. Script kiddie: under development (Web Defacers, ….)
3. Cracker: under development (Web Defacers, malicious hackers)
4. Ethical hacker: under development (security researcher, hacker groups)
5. Quiet, paranoid, skilled hacker
6. Cyber-warrior: to be developed
7. Industrial spy: to be developed
8. Government agent
9. Military hacker

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Conclusions

Bibliography and references

Contacts

Conclusions

The hacking world has not always been linked to criminal actions;

The researches carried out till today have not depicted properly a so complex, hierarchical and in continuous evolution phenomenon as the underground world;

The application of a profiling methodology is possible, but it needs a 360° analysis of the phenomenon, by analysing it from four principal point of views: Technological, Social, Psychological, Criminological;

We still have a lot of work to do and we need support: if by ourselves we have reached these results, imagine what we can do by joining our forces and experiences !

The Hacker's Profiling Project is open to collaborations and research partnerships.

HPP Next Steps

GOALS

- ✓ Data-base delivery
- ✓ Honey-Net systems delivery

WHAT WE NEED

- ✓ Looking for contributors (attack logs, hacking tales, experience)
- ✓ Looking for volunteers (log analysis, forensics analysis, reverse engineering)
- ✓ Researching of sponsors and funds raising

CHALLENGES

- ✓ Identification and evaluation of vectors, techniques and attack-tools
- ✓ Data-correlation and identification of patterns
- ✓ Release of the methodology at a *draft* level and starting of the HPP_IRP (Hackers Profiling Project Internal Review Process)
- ✓ Public release of the HPP 1.0 methodology

Considerations

✓ **The whole HPP Project** is self-funded and based on independent research methodologies.

✓ Despite many problems, we have been carrying out the Project for **two years**.

✓ The final methodology is going to be released under **GNU/FDL** and distributed through the ISECOM.

✓ **It is welcomed** the research centres, public and private institutions, and governmental agencies' interest in this research project.

✓ We think that we are **developing something beautiful**...

…**something that does not exist**…

…and it seems – really – **to have a sense** ! :)

✓ It is not a simply challenge. However, **we think to be on the right path**.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Bibliography and References (1)

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **The H.C.P. Questionnaires (2004-2005)**
- **Stealing the Network: How to 0wn a Continent**, (AA.VV), Syngress Publishing, 2004
- **Stealing the Network: How to 0wn the Box**, (AA.VV.), Syngress Publishing, 2003
- **Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier**, Suelette Dreyfus, Random House Australia, 1997
- **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, Clifford Stoll, DoubleDay (1989), Pocket (2000)
- **Masters of Deception: the Gang that Ruled Cyberspace**, Michelle Stalalla e Joshua Quinttner, Harpercollins, 1995
- **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997
- **Takedown: sulle tracce di Kevin Mitnick**, John Markoff e Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
- **The Art of Deception**, Kevin D. Mitnick and William L. Simon, Wiley, 2002
- **The Art of Intrusion**, Kevin D. Mitnick and William L. Simon, Wiley, 2004
- **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998
- **The Hacker Diaries: Confessions of Teenage Hackers**, Dan Verton, McGraw-Hill Osborne Media, 2002
- **Cyberpunk: Outlaws and Hackers on the Computer Frontier**, Katie Hafner, Simon & Schuster, 1995
- **SecurityFocus.com** (BugTraq, VulnDev), **Mitre.org** (CVE), **Isecom.org** (OSSTMM), many "underground" web sites & mailing lists, private contacts & personal friendships, the Academy and Information Security worlds

Bibliography and References (2)

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **Compendio di criminologia**, Ponti G., Raffaello Cortina, 1991
- **Criminalità da computer**, Tiedemann K., in "Trattato di criminologia, medicina criminologica e psichiatria forense", voumel X, "Il cambiamento delle forme di criminalità e devianza", Ferracuti F. (by), Giuffrè, 1988
- **United Nations Manual on the Prevention and Control of Computer-related Crime**, in International Review of Criminal Policy – Nos. 43 and 44
- **Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale**, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001
- **Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques**, Turvey B., Knowledge Solutions Library, January, 1998
- **Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro

Acknowledgements

The H.P.P. Project's Authors would like to thank for their contribution, support and time:

• **Key People:** Sentinel, Dr. Elisa Bortolani, Job De Haas, Kevin D. Mitnick, Mayhem, Venix.

• **Events, Associations and Organizations**: HITB, *SecWest, Italian Hackmeeting, SysCan, MOCA, BLACKHAT, RUXCON, EUROSEC, CLUSIT, ISACA (Italian Chapter), OWASP meetings (Italian Chapter), ISO 27001 IUG (Italian Chapter), BellUA, Telecom Security Task Force, Phrack, 2600 Magazine, Xcon/Xfocus Team, Security Task Force Consortium.

• **Mailing lists**: SecurityFocus.com, Full-Disclosure, sikurezza.org,, italian LUGs, private m.ls.

• **Gurus**: Raist, Raptor, Inode, Synack, Cla'75, Lamerone, Dialtone, Pete Herzog, Stefano Chiccarelli, Emmanuel Gadaix, Dr. Gabriele Faggioli, Trek/3K, Phlippe Langlois, Gabriella Mainardi, Antonis Anagnostopoulos, Marco Tracinà, Sentinel, Vittorio Pasteris, Pietro Gentile, Fabrizio Ciraolo, Alessandra Vitagliozzi, Jim Geovedi, Anthony Zboralski, the Grugq, Fabrice Marie, Roelef9 from SensePost, Dhillon Kannabhiran.

Special thanks to:

Daniele Poma, Andrea "Pila" Ghirardini, Andrea Barisani, Fabrizio Matta, Marco Ivaldi, Dr. Angelo Zappalà, Anna Masera, D.ssa Angela Patrignani, Prof. Ernesto Savona, Dr. Andrea Di Nicola, Patrizia Bertini, Dr. Mario Prati, Dr. Raffaella D'Alessandro, Ettore and Federico Altea, Vincenzo Voci, Massimiliano Graziani, Dr. Mimmo Cortese, Lapo Masiero, Simona Macellari, Amodiovalerio "Hypo" Verde, Paolo and Giorgio Giudice, Salvatore Romagnolo, Avv. Annarita Gili, Raffaela Farina, Enrico Novari, Laura Casanova De Marco, Fabrizio Cirilli, Eleonora Cristina Gandini, Dr. Alessandro Scartezzini, Stavroula Ventouri, Rosanna and Francesca D'Antona, Dr. Alberto Pietro Contaretti, Dr.ssa Alicia Burke, Andrey Buikis, Flaminia Zanieri and "the nano", Giovanni Lo Faro, Carla Fortin, Mirko "Mitch" Arcese, Lidia Galeazzo, Freddy "Seabone" Awad, Margherita Bo, Matteo Curtoni and Maura Parolini, Veronica Galbiati, Maya and Barbara "Wolf", Loren Goldig, Alessandro "Cyberfox" Fossato, Laura Di Rauso, Silvia Luzi.

HPP Partnerships

- Here we list the HPP signed partnerships as of July 2006.

✓ Supporting Organizations

✓ Project Sponsors

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Contacts & Links

Hacker's Profiling Project home page:

- **http://www.isecom.org**

Project Leaders:

- Raoul Chiesa, Director of Communications

raoul@ISECOM.org

- Dr. Stefania Ducci, Independent Criminal Researcher

stefania@ISECOM.org