GIAC Exam Preparation

Understanding the Rules

- Exam is open book (and open notes)
- You have four months to take the exam from date authorized
- You can purchase retakes
- You can purchase extensions

Understanding Your Skills

- GIAC is the hands-on certification
- If the subject matter is new, then you may need more time to study
- If have 10 years experience in the field, then you have an advantage
- Use practice exams to assess your skills.

Fire Hose Method

- SANS is famous (or infamous) for the fire hose method of instruction
- So if you only retain 10% of class instruction how do you get the other 90%?
- Study – smartly, efficiently

Indexes, Tabs, Highlighters

- Open book – use an index and tabs
- Start creating index during class
- Highlight important concepts keywords
- Highlight or tab areas you need to go back to

Index Guidelines

- Not too granular, but not too general.
- Insert tabs in books at module breaks.
- 2-3 Pages total
- A word of caution -- You can't lookup every question!

Example Index

502.1 Perimeter Concepts: Threats, services, what attacker do, Layered Security, Decoying, OS vs Commercial Tools

IP Refresher and Beyond: tcpdump and windump, Link Layer, ARP Poisoning, Defeat Sniffing, IP Layer, IP Fields, Idle Scan, IP Route Options (Source Routing)

Fragmentation: Normal Fragmentation, MTU, tcpdump and fragmentation, packet filtering and frag, DF flag, Malicious Fragmentation, ping o' death, teardrop, missing fragment,

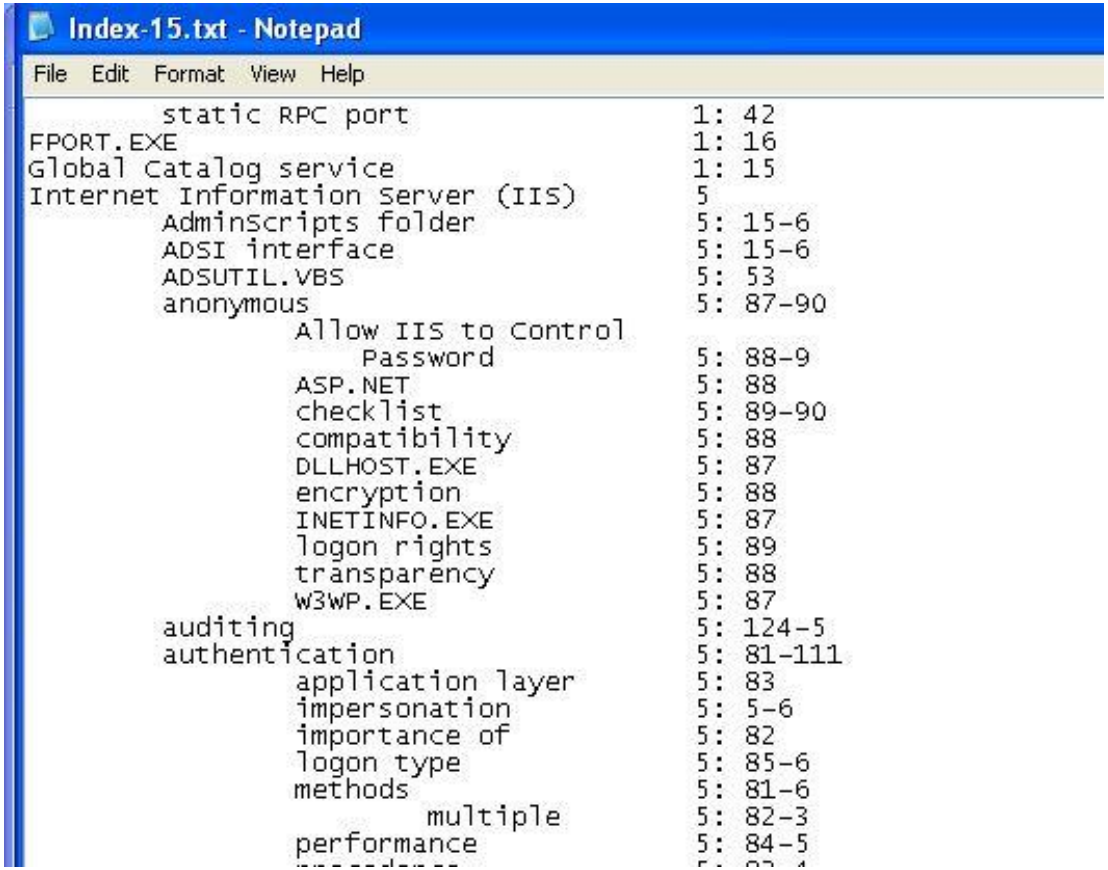
TCP/UDP/ICMP: UDP Stimulus/Response, UDP Port Scanning, TCP Header Fields/Flags, TCP connections, TCP Options, TCP Stimulus/Response, ICMP Header/Errors, Windows/Unix Traceroute, tcptraceroute,

Tearing Into Packets: tcpdump/windump switches, bitmasking, filtering, Echo sequence number (windows/linux), hijacking with ettercap, p0f fingerprinting.

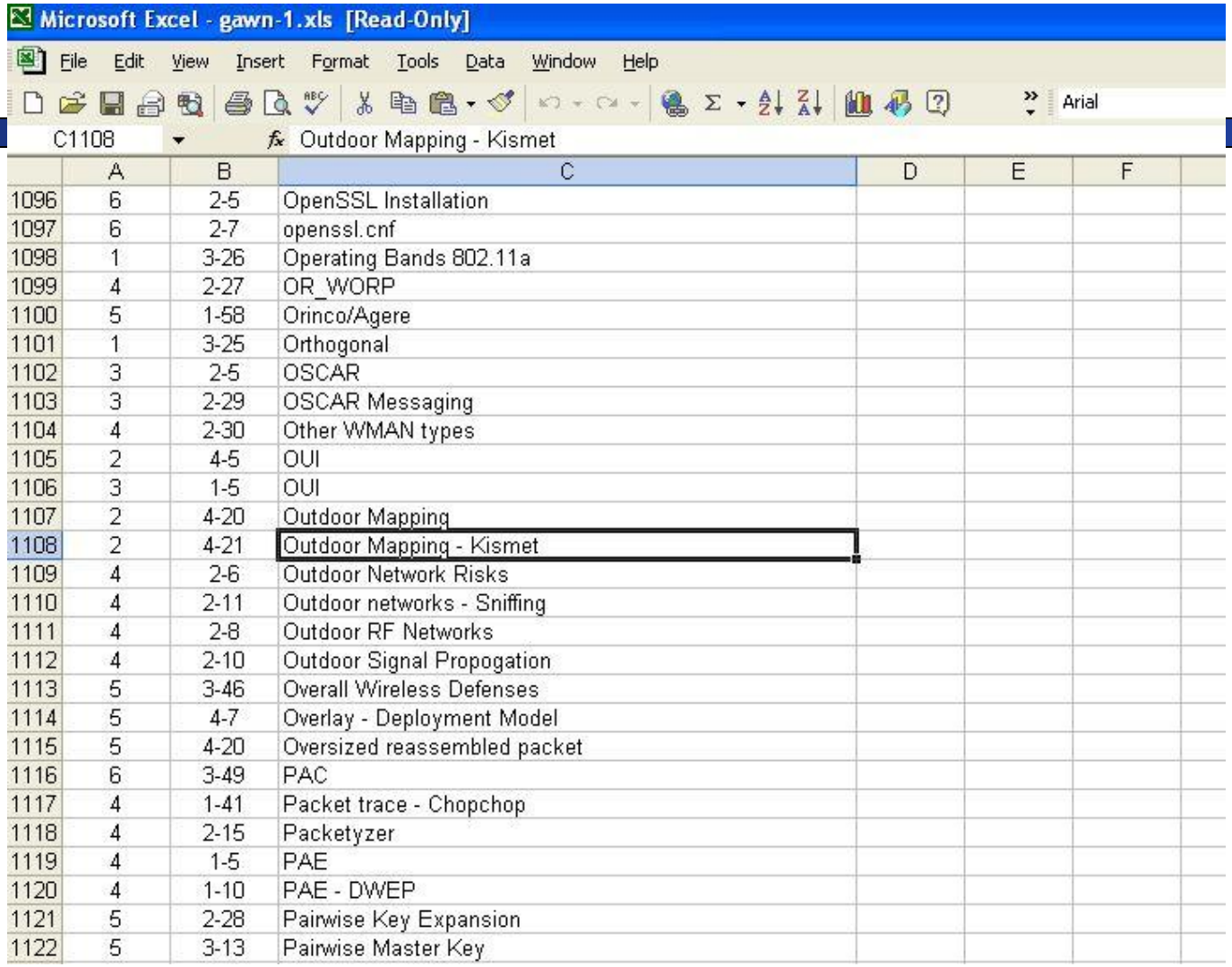
IPv6: changes, history, header, missing fields, extension headers, address convention, 48bit MAC to EUI 64, types of IPv6 addresses, multicast, jumbo payloads, ICMPv6, security issues, and privacy concerns.

502.2 Static and Stateful Packet Filters: Ingress/Egress Filtering, State Table, What gets evaluated, Difference in implementations

Example Index (2)



Example Index (3)


Microsoft Excel - gawn-1.xls [Read-Only]

File Edit View Insert Format Tools Data Window Help

C1108 Outdoor Mapping - Kismet

	A	B	C	D	E	F
1096	6	2-5	OpenSSL Installation			
1097	6	2-7	openssl.cnf			
1098	1	3-26	Operating Bands 802.11a			
1099	4	2-27	OR_WORP			
1100	5	1-58	Orinco/Agere			
1101	1	3-25	Orthogonal			
1102	3	2-5	OSCAR			
1103	3	2-29	OSCAR Messaging			
1104	4	2-30	Other WMAN types			
1105	2	4-5	OUI			
1106	3	1-5	OUI			
1107	2	4-20	Outdoor Mapping			
1108	2	4-21	Outdoor Mapping - Kismet			
1109	4	2-6	Outdoor Network Risks			
1110	4	2-11	Outdoor networks - Sniffing			
1111	4	2-8	Outdoor RF Networks			
1112	4	2-10	Outdoor Signal Propogation			
1113	5	3-46	Overall Wireless Defenses			
1114	5	4-7	Overlay - Deployment Model			
1115	5	4-20	Oversized reassembled packet			
1116	6	3-49	PAC			
1117	4	1-41	Packet trace - Chopchop			
1118	4	2-15	Packetyzer			
1119	4	1-5	PAE			
1120	4	1-10	PAE - DWEP			
1121	5	2-28	Pairwise Key Expansion			
1122	5	3-13	Pairwise Master Key			

About practice tests

- Roughly same difficulty as exam
- Questions are written by the same subject matter experts
- First practice exam is best gauge of your skills. Questions may be repeated on subsequent practice exams
- Follow the same single exam format as certification exam

An Ideal Study Plan

- Read all SANS courseware twice (using a highlighter and tabs)
- Prepare a good index of course material
- Listen to audio files at least once
- Familiarize yourself with the certification objectives (COs)
- When you think you know your stuff, take the first practice exam simulating live exam conditions.

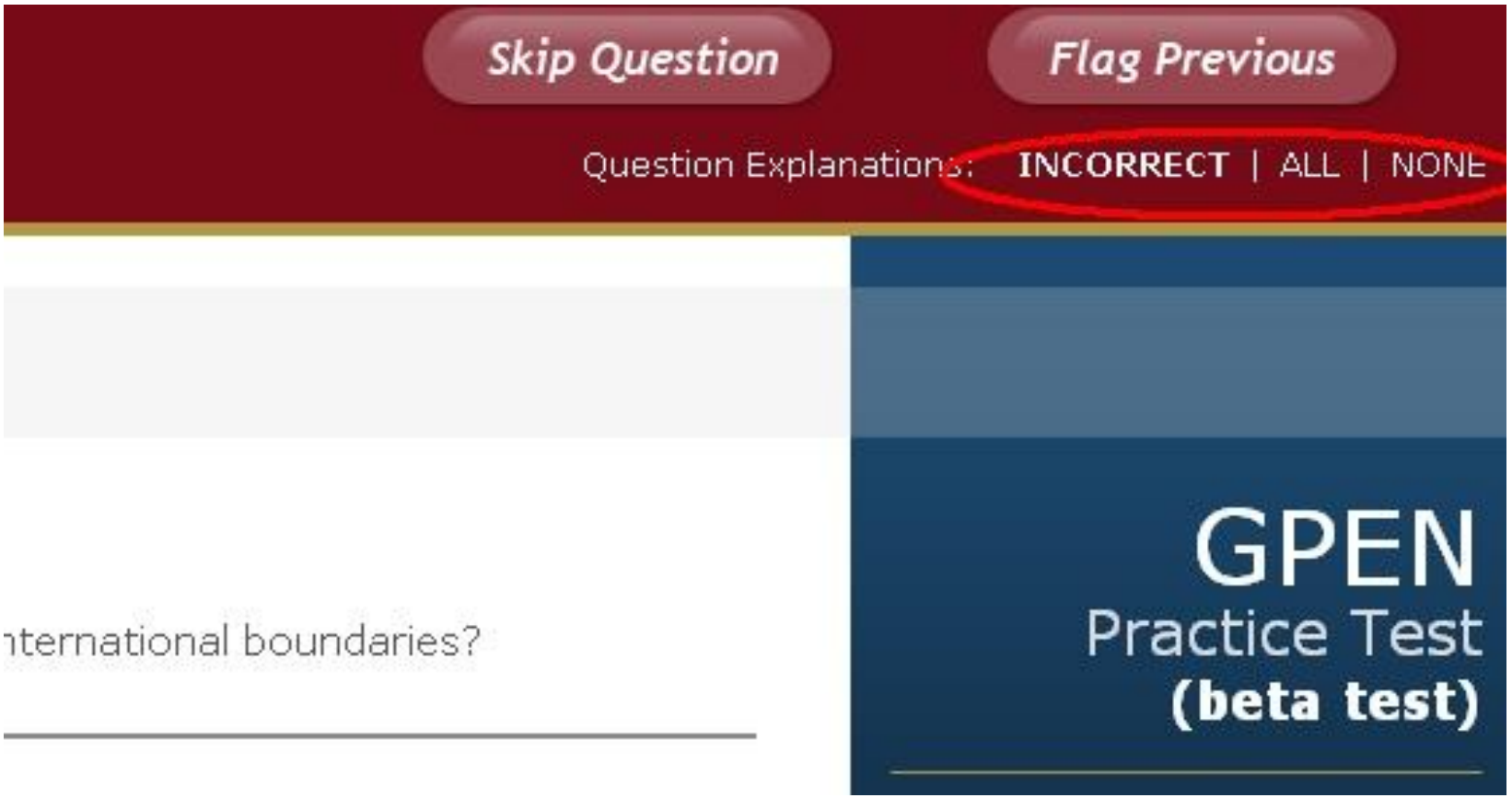
Study plan in ideal world (2)

- Assess deficient areas based on practice exam results (printed report ranks your knowledge of cert objectives)
- Additional study to address deficiencies
- Second practice exam
- One more round of addressing deficiencies
- Certification Exam

Condensed Study Plan

- Index the courseware
- Be familiar with cert objectives
- Take first practice test
- Honest assessment of your own skills + additional study as required
- Take cert exam (if ready)

Practice Exam Question Explanations



Sample STAR/CO Report

GPEN Practice Test

Score: 83.33% Status: Passed

Cain	★★★☆☆
Command Injection	★★★★★
Command Shell vs. Terminal Access	★★★☆☆
Cross Site Request Forgery	★★★★★
Cross Site Scripting	★★★★★
Enumerating Users	★★★★★
Exploitation Fundamentals	★☆☆☆☆
Finding Vulnerabilities with Search Engines	★★☆☆☆
John the Ripper	★★★★☆

STAR/CO Report Always Available

(Recent Practice Tests)

Exam ▲	Certification	Status
GCIM - 0407 Exam – ID 427176	--	Failed — 8.00% (view summary)
Automated Math Test Exam – ID 654416	--	Passed — 100.00% (view summary)
Automated Math Test Exam – ID 665636	--	Passed — 100.00% (view summary)
Automated Math Test Exam – ID 668016	--	Passed — 100.00% (view summary)
Automated Math Test Exam – ID 668021	--	Passed — 100.00% (view summary)
Automated Math Test Exam – ID 668616	--	Passed — 100.00% (view summary)
Automated Math Test Exam – ID 672624	--	Passed — 100.00% (view summary)

Test timing

- Set waypoints. Example: 40/1hr, 80/2hr, 120/hr
- Simulate exam timing with practice tests
- Don’t watch the clock at all unless you are near a waypoint.

Question Reading

- Read the question, all answer options, then read the question again
- Understand what the question is asking and don't make assumptions
- Beware of NOT/FALSE questions

Preparation – Tying It Together

- Course Material
- Practice Exams
- Certification Objectives

Combating Psychological Issues

- Stay in the moment
- Trust yourself if you know the answer
- Relax (retakes available)
- Chance favors the prepared mind
- The power of positive thinking

More info

- http://www.giac.org/overview/faq.php
- http://www.giac.org/certbulletin/gsec.php
- http://www.giac.org/proctor/
- http://www.giac.org/information/
- exam-support@giac.org