Appendix B: Survey Questions and Response Rate

This year's "Under the Hoodie" is built on an entirely new set of 93 questions, and garnered 180 total responses. Those questions are reproduced below, along with the response rates to each question. We utilize a fair amount of question skip logic to ensure that penetration testers are only answering the questions relevant to their specific engagement, so all respondents will normally only see a small fraction of these questions.

SECTION	QUESTION	RESPONSE	% OF N=180
Start	What kind of assessment was this? (Pick only one)	180	100.00%
Question	About how much of the engagement time did you spend on planning and recon?	4	2.22%
Responses	Did you need to gain Domain Admin / Enterprise Admin in order to achieve the objective of the engagement?	4	2.22%
% of n=180	Did you need to use well-known, off-the-shelf exploits, such as MS17-10 (EternalBlue) to achieve the objective of the engagement?	4	2.22%
Red Team Attack Simulation	Were you detected and caught or blocked by the blue team, SOC, or physical security before gaining internal access?	4	2.22%
Red Team Attack Simulation	Were you detected and caught or blocked by the blue team, SOC, or physical security after gaining internal access?	4	2.22%
Red Team Attack Simulation	Which component of the red team engagement did you work on? (Just pick one for now)	4	2.22%
Social Engineering	About how much of the engagement time did you spend on planning and recon?	10	5.56%
Social Engineering	Were you detected and caught or blocked by the blue team, SOC, or physical security before gaining internal access?	9	5.00%
Social Engineering	Were you detected and caught or blocked by the blue team, SOC, or physical security after gaining internal access?	9	5.00%
Social Engineering	Which component of the SE engagement did you work on? (Just pick one for now)	11	6.11%
External Pentest	About how much of the engagement time did you spend on planning and recon?	52	28.89%
External Pentest	How many hosts were in scope?	71	39.44%
External Pentest	Which external network components did you work on?	71	39.44%
Internal Pentest	About how much of the engagement time did you spend on planning and recon?	41	22.78%
Internal Pentest	About how many IP addresses were in scope?	61	33.89%

SECTION	QUESTION	RESPONSE	% OF N=180
Internal Pentest	How many domains were in scope?	62	34.44%
Internal Pentest	Were you detected and caught or blocked by the blue team or SOC before gaining internal access?	63	35.00%
Internal Pentest	Were you detected and caught or blocked by the blue team or SOC after gaining internal access?	62	34.44%
Internal Pentest	Which internal components did you work on?	63	35.00%
Code Review	What kind of code review was this?	6	3.33%
Something Else	Are you sure?	19	10.56%
External Network Compromise	What vulnerabilities did you find? (Check any that apply)	33	18.33%
External Network Compromise	Did you gain internal network access?	33	18.33%
Webapp Compromise	How many applications were in scope?	39	21.67%
Webapp Compromise	Were any of these webapps live and in production?	39	21.67%
Webapp Compromise	Were you given credentials?	39	21.67%
Webapp Compromise	What technology was the application built on? (Check all that apply)	31	17.22%
Webapp Compromise	What JavaScript frameworks were used? (Check all that apply)	30	16.67%
Webapp Compromise	Where was the application hosted?	38	21.11%
Webapp Compromise	What vulnerabilities did you find? (Check all that apply)	38	21.11%
Webapp Compromise	Did you escalate privileges to site admin or root?	39	21.67%
Vuln Assessment	What tools did you scan with? (Check all that apply)	1	0.56%
Vuln Assessment	Was this an authenticated scan or unauthenticated?	1	0.56%
Vuln Assessment	What kinds of vulnerabilities and exposures were found? (Check all that apply)	1	0.56%
Vuln Assessment	Was host exploitation in scope?	1	0.56%
Vuln Assessment	Did you end up popping any shells?	1	0.56%

SECTION	QUESTION	RESPONSE	% OF N=180
DoS / DDoS Assessment	How many endpoints were being attacked? (Pick one)	0	0.00%
DoS / DDoS Assessment	What layer was the attack traffic? (Pick all that apply)	0	0.00%
DoS / DDoS Assessment	How much traffic was sent? (Pick one)	0	0.00%
DoS / DDoS Assessment	Did the customer have DoS / DDoS protection in place? (Pick one)	0	0.00%
DoS / DDoS Assessment	How did the targets respond to the DoS test? (Pick one)	0	0.00%
Physical Social Engineering	How many locations were in scope? (Pick one)	3	1.67%
Physical Social Engineering	How did you get in? (Choose all that apply)	3	1.67%
Physical Social Engineering	What sensitive stuff did you get access to? (Check all that apply)	2	1.11%
Physical Social Engineering	Once inside, did anyone question you? (Check any that apply)	3	1.67%
Physical Social Engineering	Did you plant any devices? (Pick all that apply, using their closest equivalents)	3	1.67%
Electronic Social Engineering	Did you use an email component?	11	6.11%
ESE: Email Details	So, what happened?	11	6.11%
ESE: Emails	Email is cool, but phone-based ESE is a thing, too. Did you call, text, or dial an interactive voice response (IVR) system?	11	6.11%
ESE: Phones	Who was the target of your calls or texts? (Check all that apply)	4	2.22%
ESE: Phones	So, what happened?	4	2.22%
WiFi	Was there a guest network?	11	6.11%
WiFi: Guest Network Details	Did the guest network have a password?	10	5.56%
WiFi: Guest Network Details	Which security protocols were in use?	10	5.56%
WiFi: Guest Network Details	Did the guest network have proper isolation?	10	5.56%
WiFi: Corporate Network	Were you able to access the corporate network?	11	6.11%

SECTION	QUESTION	RESPONSE	% OF N=180
WiFi: Corporate Network Details	How many access points were in scope?	7	3.89%
WiFi: Corporate Network Details	How many users were on the WiFi during the assessment?	7	3.89%
WiFi: Corporate Network Details	Which security protocols were in use?	7	3.89%
WiFi: Corporate Network Details	Was a certificate required for access to the corporate network?	7	3.89%
WiFi: Corporate Network Details	How did you gain access the corporate network?	7	3.89%
WiFi: Corporate Network Details	Did you get administrator privileges in the corporate network?	7	3.89%
WiFi: Corporate Network Details	What vulnerabilities did you find? (Check all that apply)	7	3.89%
Internal Network Compromise	Were you invited to go onsite or provided an ingress point on the network, or did you have to first break in?	56	31.11%
Internal Network Compromise: Initial Access	How long did it take to gain internal access?	8	4.44%
Internal Network Compromise: Initial Access	What was your *primary* method for attempting to gain internal access?	7	3.89%
Internal Network Compromise: The Nitty Gritty	Did you obtain Domain or Enterprise Administrator access?	54	30.00%
Internal Network Compromise: The Nitty Gritty	Were any hosts vulnerable to MS17-010 (Eternal Blue)?	55	30.56%
Internal Network Compromise: The Nitty Gritty	Were any hosts vulnerable to MS08-067 (Conficker)?	54	30.00%
Internal Network Compromise: The Nitty Gritty	Did any domain controllers have null sessions enabled?	55	30.56%
Internal Network Compromise: The Nitty Gritty	Did you find some sensitive data? This can be either a red team objective, or some other sensitive data.	55	30.56%
Internal Network Compromise: The Nitty Gritty	What vulnerabilities did you find? (Check all that apply)	54	30.00%

SECTION	QUESTION	RESPONSE	% OF N=180
Internal Network Compromise: The Nitty Gritty	What lateral movement technique did you leverage THE MOST?	55	30.56%
Mobile Application Assessment	Were you given the source code?	5	2.78%
Mobile Application Assessment	What platform was the mobile application built for? (Check all that apply)	5	2.78%
Mobile Application Assessment	What vulnerabilities did you find?	5	2.78%
Keep Going?	Did you want to report on any other component of the engagement?	148	82.22%
Credential Capture	Did you capture any credentials?	153	85.00%
Credential Details	How did you gather usernames? (Check all that apply)	82	45.56%
Credential Details	How did you obtain passwords or password hashes? (Check all that apply)	86	47.78%
Credential Details	Were any of these creds privileged accounts? (Privileged just means "more rights than the usual user," not necessarily Domain Admin. Use your best judgement.)	87	48.33%
Privileged Account Details	Were any of these privileged accounts, in fact, Domain Admin?	48	26.67%
Privileged Account Details	How did you find privileged accounts? (Check all that apply)	49	27.22%
Credential Control: Account Lockouts	How effective were account lockouts? (Check all that apply)	109	60.56%
Credential Control: 2FA / MFA	Was 2FA enabled on any services you tested?	120	66.67%
2FA Encountered	Were you able to bypass or compromise 2FA?	26	14.44%
2FA Defeated	How did you compromise 2FA? (Check all that apply)	9	5.00%
Password Cracking	Did you try to crack any passwords?	120	66.67%
Password Cracking Details	What kind of hashes did you collect?	63	35.00%
Password Cracking Details	How many password hashes did you get?	63	35.00%
Password Cracking Details	About what percentage of the passwords did you crack?	63	35.00%
Password Cracking Details	Did you see any of these? (Select all that apply)	49	27.22%

In the interest of space, we have not provided the multiple-choice answers, since reproducing answers would add another 15 or so pages to this report. That said, we are happy to share the entire survey, including possible multiple choice answers with any interested practitioners or researchers—just drop us a line at research@rapid7.com and we'll get those to you.

As a matter of fact, if you're part of a penetration testing organization and would like to participate in the next survey, also get in touch with us at that address. While we absolutely do not want to encourage anyone to violate NDAs or otherwise expose sensitive client information, we very much want to get more anonymized sample data in our analysis. Our survey is nearly entirely multiple-choice and collects only broad demographic data such as the client's company size and industry vertical, and never company names or specifics about individual assessments or individuals. We'll be reaching out to penetration testing organizations around the world over the next few months, but if you can't wait to get started and help to advance public understanding of penetration testing, let us know!