The Script Bulletin

JUNE 2018

UPDATES:

Tickets available now for CRESTCon Asia

CRESTCon Asia is a unique event that brings together leading technical and business information security professionals in this industry.

Date and time: Friday, 20 July 2018
09:00 to 17:30

Venue: Suntec Singapore Convention & Exhibition Centre, 1 Raffles Boulevard, Room 303-304, Singapore 039593

CREST Members in Asia are entitled to two free tickets per Member Company. Admission is strictly by pre-registration only. To purchase your tickets or claim your free member tickets, please go to:
https://crestconasia2018.eventbrite.sg

Infosecurity Europe 2018

CREST had a very busy and successful three days at Infosecurity Europe 2018 once again and as it is every year, it was great to see so many of our members exhibiting.

Along with members and potential new members visiting the stand we had a lot of interest in our academic partner program and from people in the public sector.

The photo shows Sam Alexander and Sara Cox welcoming Immersive Labs to the stand who had just announced they had become a CREST Approved Training Provider.

The Institute of Coding has launched

CREST is proud to be part of a consortium of leading universities, professional bodies and businesses that is championing digital skills. It is important that CREST is engaged with initiatives such as this, to ensure that cyber security is firmly on the mainstream agenda.
You can find out more from the Institute of Coding website: **https://instituteofcoding.org/** or read about the launch here: **https://www.standard.co.uk/tech/institute-of-coding-uk-digital-skills-a3869311.html**

Training provider meeting

On 21 June CREST held a Training Provider meeting at the BSI Milton Keynes offices. The meeting was held following the launch of the Approved Training Provider Scheme to gather feedback. The addition of mobile rigs for CREST's exam capability was discussed and how this can link to the training. The attendees then discussed further improvements to the scheme for the future. A full report on the feedback from the attendees is currently being written up but it they did agree that the new scheme was an improvement.

We would like to take this opportunity to thank BSI for the use of its office. The homemade rocky road was a big hit in the afternoon break!

CREST Events | **CREST Workshops** | **Industry Events**

UPDATES:

What makes a good CREST report workshop – Context Information Security offices, 19 June

Thank you to everyone who attended what proved to be a very lively and interesting workshop and to Context for hosting us. This was the first in a series of workshops held to help define a CREST Test. It was certainly very useful to get the perspectives from the buying community on pen test reporting via members of the CREST Senior Advisory Panel who attended.

SAVE THE DATE – CRESTCon 2019 will be on 14 March 2019 at Royal College of Physicians

Planning is already well underway for next year's event and we are always looking for suggestions for how we can improve on how we do things. Please email **allie.andrews@crest-approved.org** with any ideas you have.

Early bird sponsorship packages are available now.

For details of these packages please contact **debbie.jones@crest-approved.org** as soon as possible. Only six are available and three have already reach contract negotiation stage as this newsletter goes to press!

CREST members are entitled an additional discount

CRESTCon 2018 presentation summaries

Several students attended CRESTCon from CREST academic partners. They each wrote summaries of the presentations they attended; 3 of which are attached below:

Presenter: Saurabh Harit
I know what you installed last summer. Written by Jordan Watson from UCL
In this presentation, Saurabh Harit from Spirent discussed vulnerabilities that exist in many 3rd party web applications and demonstrated a tool he has written to aid in their discovery. These vulnerable applications can allow attackers to gain access to and compromise the back-end server. Using his custom tool yasuo, Saurabh showed how to find these applications.

Saurabh discussed how negligence and forgetfulness surrounding uninstalling 3rd party web applications, that have often been installed around a testing and trial phase, are often left weakly configured and lead to vulnerabilities. Although many of the vulnerabilities of web applications like Tomcat and Hudson Jenkins can be things like remote code execution, SQL injections and file inclusion vulnerabilities, Saurabh explained how a lot of issues arise because of users and how some of the vulnerabilities occur because of weak passwords. It's also an issue from the users when failing to uninstall or properly configure 3rd party web application during any trial and testing periods. Saurabh asserts that this lack of care is what ultimately leads to the vulnerabilities discussed in this presentation. Ultimately Saurabh emphasised that it's not about what shells come from, it's where. To solve this, he went on to explain an open source tool written in Ruby that he has been writing to aid penetration testers.

>>

UPDATES:

Yasuo is a ruby script that scans for vulnerable and exploitable 3rd party web applications on a network. This tool can drastically speed up a penetration test by automating the process of discovering vulnerable web applications on a network. Yasuo is also compatible with nmap and can use output files generated via nmap. Because of this, the tool will be able to easily fit into a penetration tester's arsenal of tools. Interestingly the tool has capabilities of alleviating the stress placed on a host from constant scanning.

Saurabh's presentation addressed common vulnerabilities, how they arise and presented a tool to aid in securing a host. Also its compatibility with commonly used tools makes it an incredibly value contribution to the open source community and cybersecurity in general.

Presenters: Andrew Davies and Jon Medvenics
Common traps and pitfalls in red teaming. Written by Connor Roberts from Bournemouth University
Presented by Andrew Davies (Director at Netscylla) & Jon Medvenics (Lead Incident Manager at Netscylla), they set out a presentation outlining ways to catch a red-teamer. In this presentation Andrew was talking from the point of the red-teamers and Jon the blue.

Straight from the get go they mention testing from your own IP (this being corporate or home), and by carrying out a simple Who is command and simply blocking the hole block, in effect catching the red-teamers before they've started. Jon touches on the legalities of purchasing domains and making it mimic a third party and how this can put the red-teamer in very murky water. To add to this point, purchasing the domains with a personal credit card, your details are stored and can be passed on to the authorities.

Jon mentions that if phishing is an initial start of your assessment, it is important to understand headers, and worth sending emails to yourself to see what the header looks like and in turn putting on a blue-teamer hat and working out what would catch you out so you can carry out a much more efficient assessment. Presenters mentioned that this has been a common mistake from red-teamers.

Both mention the importance of understanding artefacts that are left with the tools you are using, an example of this was when cloning a website with HTTrack, a header and footer is left stating that it has been cloned and where from. Another example was the use of Beef, the default session name being BEEFSESSION gives a very simple win for the blue team.

Andrew highlighted the use of formatting your prompts with a simple [Date] [Time] [Drive & Path]> system, which allows you to grep with ease. By doing this when challenged with what happened on a certain day you don't have to search through logs.

Andrew gave insight that a lot of plays he is seeing within the industry within the last six months have come from the "Advanced Penetration Testing: Hacking the world's most secure networks" book. Jon also stated that this book has great ideas which can be relayed into your red-teaming.

To end the presentation, they gave a comical list of what's not safe for work, this involved the red team changing their MAC address to have the vendor-id to appear as the NSA. Another being making everyone a domain admin… who's going to want to give that up?

Overall the presentation gave evidence that when a red-team rushes, they can make costly errors which causes them to waste more time. Simple things like not leaving your hostname as Kali can save a red-teamer from looking silly before they've even begun!

Presenter: Daniel Carter
Hacking a home router from the web
In this presentation Daniel Cater explained how he was able to gain access to a home network from the web by exploiting vulnerabilities in a specific router. During the presentation Daniel explained how he gained access, from initial hypothesis to gaining control of all functionality, including some that was not provided to the administrator.

The router used had many security measures, including; unique SSID, unique SSID key, unique admin password

and no access to settings from the internet by default. Despite what these measures may imply, a teardown of the hardware suggested there was a hidden account on the router. This lead to Daniel capturing the password using the following method:

Mirror traffic on the WAN side of the router

Set up wireshark to capture data being sent to the router

Call up customer support and say the WiFi isn't working

Capture credentials for the root account

The credentials for the root account were found to be the same for all routers of that model, in addition to this the root account could activate certain options the admin account couldn't. Despite these vulnerabilities it was not possible to use these vulnerabilities to reach the web interface remotely, due to CSRF protection preventing web pages from submitting requests.

This protection could be bypassed using a malicious webpage that takes advantage of DNS rebinding. This could allow a malicious attacker to; modify DNS server settings, drop firewall rules, enable FTP to internet (to read files off a memory stick), plus reading the SSID and SSID key.

The final flaw that was explained, was the way the router is managed using TR-069. This works by the router checking in with the ISP once a day to check for updated firmware etc. The URL that the server looks for can be changed to point to a malicious server, thanks in part to; no certificate validation, no mutual authentication and the router must use a HTTP keep alive request, plus a single TCP connection. The point of this is that only with this method could telnet be enabled.

To finish the presentation Daniel made several recommendations as to how these vulnerabilities could have been fixed. These included strong and unique credentials for the hidden account, or removing it entirely, a check of the HTTP host header and a valid ACS certificate.

CRESTCon 2018 Video content

More video content from 2018 content has been uploaded to the CREST YouTube channel at: **www.youtube.com/crestadvocate**

CREST Approved Training Provider Request

CREST Approved Training Provider, InfoSec Skills is looking for CRIA qualified individuals for following:

- CPIA-CRIA Training Provider sign off
- CPIA-CRIA Authors
- CPIA-CRIA Instructors

If you would like more information about these flexible opportunities to help people with their personal professional development, contact Terry Neal **terry@infosecskills.com** or call him on +44 (0)20 8144 2303 for details.

CREST Member Offer for IAAC Annual Symposium

Friday, 14 September 2018, BT Centre, London, EC1A 7AJ

IAAC is offering people who work at CREST Member companies 20% off the commercial rate, bringing the cost of a ticket down to £80.

Members please email **allie.andrews@crest-approved.org** for the discount code.

The theme of the day is Digital Resilience - for individuals, communities, organisations and society.

There is more information on the day in the main event section.

CREST Diary

CREST Diary:

Month	Event	Type	Date
2018			
July	Pitch the Ship – ISSA	Exhibiting & Supporting	5 July
	OWASP AppSec Europe	Exhibiting & Supporting	5-6 July
	CRESTCon Asia	Annual Event	20 July
	Threat categories of connected vehicles	Workshop	30 July
Aug	Bsides Manchester	Exhibiting & Supporting	16 Aug
	BlackHat/Defcon	Member Meet-Up	TBD
Sept	44CON	Exhibiting & Supporting	12-14 Sept
	IAAC Annual Symposium	Supporting	14 Sept
	UK Health Show	Exhibiting & Supporting	25-26 Sept
Oct	IP EXPO Europe	Exhibiting & Supporting	3-4 Oct
	Cloud Security Expo, Singapore	Supporting	10-11 Oct
Nov	Infosecurity North America (New York)	Presenting, Exhibiting & Supporting	14-15 Nov
	Cyber Security Summit and Expo	Exhibiting & Supporting	15 Nov
	CREST Fellowship 2018	Annual Event	22 Nov
	International Security Expo 2018	Exhibiting & Supporting	28-29 Nov
Dec	Black Hat 2018	Supporting	3-6 Dec
2019			
Mar	CRESTCON	Annual Event	14 Mar

Event Diary

CREST Events:

Ask the Assessor Session

15 Jul, Hong Kong
Venue: Applied Science & Technology, Hong Kong

Following a successful session over webinar on 15th June, CREST Assessor Stuart Morgan will be at Hong Kong Applied Science and Technology on 17 July. This will be an in person interactive session where CREST examination candidates or potential candidates will get the opportunity to discuss the skills, techniques and learning required in the CREST practical examination.

For more information on this contact **josephng@astri.org**

WORKSHOP: CREST Threat categories for autonomous vehicles

30 Jul
Venue: TBA, UK

The second workshop looking at threat categories for autonomous vehicles has been scheduled. More information will follow by email.

If you are interested in attending please contact **debbie.jones@crest-approved.org**

Member Meet-Up at BlackHat/Defcon

Date: TBD

A meet up for members is being arranged in Las Vegas to take place during BlackHat/Defcon in August. More details will follow but to register your interest in taking part please contact **allie@crest-approved.org**

Event Diary

Industry Events:

CREST Webinars:

CREST has a BrightTalk channel for hosting webinars and other videos and we will be stepping up our program of webinars in 2018 globally. See **https://www.brighttalk.com/channel/13519/crest**. If you are interested in presenting a technical webinar or would like us to host your content, then please submit your ideas for consideration to **allie@crest-approved.org**. We will promote, run and record on the CREST channel.

'Pitch on the Ship' ISSA Event

5 Jul
Venue: HQS Wellington, London

https://www.eventbrite.co.uk/e/pitch-on-the-ship-onboard-hqs-wellington-tickets-42354115299

In the 'Security Solutions in the Spotlight' event, ten security software/solution vendors battle it out for the Best Supplier and Best Product prizes, as voted by the audience. The event offers each vendor a 10 minute speaking pitch to explain what makes their product the best, in a fast-paced and lively environment. This unique format enables delegates to understand existing and emerging technologies on the market, and each vendor will have a stand so you can find out more about their solutions. There will be four special keynotes throughout the day, it is sure to be a great day!

CREST is supporting and exhibiting at the event.

OWASP AppSec Europe 2018

5-6 Jul
Venue: The Queen Elizabeth II Centre (QEII)

https://2018.appsec.eu/?gclid=EAIaIQobChMI8rnl3fCW2wIVb7ftCh0EswSsEAAYASAAEgJhk_D_BwE

AppSec EU provides attendees with insight into leading speakers for application security and cyber security, training sessions on various applications, networking, connections and exposure to the best practices in cybersecurity. The main conference spans two days from 5-6 July 2018, offering four full tracks of talks, for pen-testers and ethical hackers, developers and security engineers, DevOps practices and GRC/risk level talks for managers and CISOs. This year's conference program will focus on the bottom to the top and top to the bottom in application security.

CREST is supporting and exhibiting at the event.

Event Diary

Industry Events:

Bsides Manchester 2018

16 Aug
Venue: Manchester Metropolitan University Business School, Manchester, M15 6BH

https://www.bsidesmcr.org.uk/

BSides Manchester is one of the UK's premier technical cybersecurity conferences. It is run under a Community Interest Company (CIC) and is a not for profit company and event. It is an inclusive event for everyone in the InfoSec community and organised by a handful of dedicated Security Professionals volunteers who give up their own time, skills and knowledge for free.

CREST is supporting and exhibiting at the event.

44CON 2018

12-14 Sept
Venue: ILEC Centre, London

https://44con.com/

It will kick off on Wednesday 12 September at 18:00 at the ILEC Conference Centre with a Community Evening. Entry to the Community Evening is free but you will have to register beforehand. Registration will open at 6pm.

CREST is supporting, exhibiting & participating at the event.

IAAC Annual Symposium

14 Sept 2018

https://www.eventbrite.co.uk/e/iaac-symposium-2018-digital-resilience-for-individuals-communities-

BT Centre, London , EC1A 7AJ. The theme of the day is **Digital Resilience - for individuals, communities, organisations and society.**

Registration will be from 08:30 for a 09:30 start. Drinks reception is from 16:30.

The symposium will look at security and information assurance, adding design, engineering, education, preparedness and learning, to explore digital resilience. At the heart of the event will be an examination of individual, community, organisational and societal digital resilience.

Individual digital resilience is often framed in terms of young people and their ability to have fulfilling personal and professional lives on and off line. Much of the cyber security awareness work undertaken in schools is discussed as digital resilience. Community and organisational digital resilience situates cyber in a wider context of hazards that might affect a smart-city or business's ability to continue to operate and adapt. We'll assess the extent to which the balance of factors is changing with our increasingly connected and interdependent world. At the societal level, we look to government for strategy and to keep the country running. We'll examine the resilience issues shaping thinking on cyber in government and critical infrastructure.

Industry Events:

We are running our usual poster competition for universities and businesses who wish to showcase their current research and projects. Please contact **info@iaac.org.uk** for details or visit our website at **www.iaac.org.uk**

The symposium includes:

- Opening and closing keynote speakers
- Panel discussions
- Government updates
- Poster competition
- Networking opportunities

Speakers confirmed include:

Robert Hall, Executive Director, Resilience First

Carolyn Bunting, CEO, Internet Matters

Martin Howelett, Director Youth Federation and IAAC Ambassador in the North West

Mike St John Green, Independent Consultant on critical infrastructure and cyber security

Shavana Musa, International law and security, Manchester University and founder Ontogeny Global

DCMS speaker confirmed.

Lord Arbuthnot of Edrom, Chairman IAAC

With thanks to BT, this year's symposium will once again be held in the excellent BT Centre in central London.

Who can attend? This is conference is open to anyone who registers, subject to capacity.

"What we have seen in financial markets should bring home to us all that the central organising principle of this 21st century is interdependence. For the century just past, interdependence may have been one option among many. For the century that is to come, there is no longer an alternative." Kevin Rudd, Former Australian Prime Minister

With sincere thanks to IAAC's National Sponsors: O2, GSK, Reliance ACSN, Sopra Steria, QinetiQ, BT, Northern Trust, Fortinet and Northrop Grumman; and to our NW Regional Sponsors, Bank of America Merrill Lynch and Raytheon.

UK Health Show 2018

25-26 Sept

Venue: Olympia, London

https://ukhealthshow.com/

Now in its third year, Cyber Security in Health (CSIH) is the vital source of cyber security information for the healthcare sector. Attracting senior level cyber security professionals from across the UK healthcare sector, CSIH provides the pivotal platform for all those involved in setting the strategy for their organisation's security, thus protecting critical data against the growing threats facing the industry.

CREST is supporting and exhibiting at the event.

Event Diary

Industry Events:

Cyber Security Chicago

26-27 Sept
Venue: McCormick Place, Chicago

https://www.cybersecurity-chicago.com/#null

Cyber Security Chicago launched in 2017 as part of the fastest growing cyber security event series that uniquely covers the entire security landscape.

Now in its 2nd year, Cyber Security Chicago offers invaluable security insight from industry experts on all facets of cyber security and risk mitigation, right in the center of Chicago.

The Chicago area is home to more than 10,000 IT security professionals. Talent from universities and colleges, such as DePaul University & Illinois State University have become the main drivers of cyber security research in the state and are transforming the Chicago area into a cyber security hub.

CREST is supporting, exhibiting & participating at the event.

IP EXPO Europe

3-4 Oct
Venue: ExCel, London

http://www.ipexpoeurope.com/

The event showcases brand new exclusive content and senior level insights from across the industry, as well as unveiling the latest developments in IT. IP EXPO Europe now incorporates Cloud Europe, Cyber Security Europe, Networks & Infrastructure Europe, AI, Analytics & IOT Europe, DevOps Europe and Open Source Europe.

CREST is exhibiting & supporting at the event.

Infosecurity 2018 North America

14-15 Nov
Venue: New York, USA

https://www.infosecuritynorthamerica.com/

With more than 22 years of experience creating marketleading information security events around the globe, Infosecurity Group launched Infosecurity North America in Boston for fall 2017. Industry professionals looking for everything under one roof joined companies showcasing innovation from around the globe, bringing the Boston community together.

CREST is presenting, supporting and exhibiting at the event.

Cloud Security Expo

10-11 Oct
Venue: Marina Bay Sands Expo and Convention Centre Singapore

https://www.cloudexpoasia.com/

Cloud Expo Asia is a two day business event, held at the Marina Bay Sands Expo and Convention Centre in Singapore. It is for the partners, technical experts, management, policy makers, practitioners and cloud service providers. It will be an ideal business platform where you will be provided with an excellent opportunity to facilitate new business leads while getting close to your clients and customers. It is an efficient and effective way of profitably marketing to this ever growing dynamic market. Security and governance, hosted solutions, cloud security and service, cloud back up, hosting and cloud storage will be some of the major topics of concern.

CREST is supporting and exhibiting at the event.

Event Diary

Industry Events:

Cyber Security Atlanta

17-18 Oct
Venue: Georgia World Congress Center Building C, C4 Hall, Atlanta, USA

http://www.cybersecurity-atlanta.com/

Cyber Security Atlanta is part of the fastest growing cyber security event series that launched in 2017, providing events that uniquely cover the entire security landscape.

Cyber Security Atlanta will offer invaluable security insight from industry experts on all facets of cyber security and risk mitigation, right in the heart of Atlanta, Georgia.

Atlanta is one of the fastest growing high-tech metro areas in the US, home to more than 115 information security companies accounting for 25% of the global security revenue market share.

Atlanta also places third for the city with the most Fortune 500 HQ's and produces sensational talent from leading educational institutions, making it a true cyber security powerhouse. Cyber Security Atlanta allows you to keep up to date with all things cyber security without having to travel to the West Coast.

CREST is exhibiting, supporting and participating at the event.

Cyber Security Dallas 2018

31 Oct - 1 Nov
Venue: Gaylord Texan Resort & Convention Center, Dallas, USA

Cyber Security Dallas is part of the fastest growing cyber security event series. Providing events that uniquely cover the entire security landscape.

Cyber Security Dallas will offer invaluable security insight from industry experts on all facets of cyber security and risk mitigation, right in the heart of Dallas, Texas.

Texas is now a major player in the US tech scene, Cyber Security Dallas allows you to keep up to date with all things cyber security without having to travel to the West Coast. Texas is home to 52 companies on the Fortune 1,000 list, third only to New York & California. With over 10,000 corporate headquarters in the Dallas/Fort Worth Metroplex alone, Dallas has the largest corporate headquarters concentration in the United States.

CREST is exhibiting, supporting and participating at the event.

Event Diary

Industry Events:

Cyber Security Summit and Expo, London

15 Nov
Venue: Business Design Centre, London

https://cybersecuritysummit.co.uk/

The Cyber Security Summit and Expo is the UK's largest one-day event dedicated to cross-sector learning for cyber preparedness across government, the public sector, critical national infrastructure and industry. Connecting senior-level business, security, technology and data leaders – this event provides a unique platform to debate national leadership priorities and share best practice solutions to achieve cyber resilience in a fast-moving digital world.

CREST is supporting and exhibiting at the event.

International Security Expo 2018

28-29 Nov
Venue: Olympia, London

https://www.internationalsecurityexpo.com/

UK Security Expo is a major scale event that tackles some of the most challenging threats to our citizens, borders and infrastructure. The event provides a unique and secure environment for security experts to come together to buy products, share experience and gain the knowledge needed to address current and emerging security challenges. The show delivers 10,000+ International Visitors to London from Government, Transport & Borders, Major Events, Military, Law Enforcement, Emergency Services, CNI and the public and Private Sectors.

CREST is supporting and exhibiting at the event.

Black Hat Europe 2018, London

3-6 Dec
Venue: ExCel, London

https://www.blackhat.com/upcoming.html

Black Hat is the most technical and relevant global information security event series in the world. For more than 18 years, Black Hat has provided attendees with the very latest in information security research, development, and trends in a strictly vendor-neutral environment. These high-profile global events and Trainings are driven by the needs of the security community, striving to bring together the best minds in the industry. Black Hat inspires professionals at all career levels, encouraging growth and collaboration among academia, world-class researchers, and leaders in the public and private sectors.

CREST is supporting the event.