Cybersecurity Solutions for Small Businesses

The Hidden Threat:

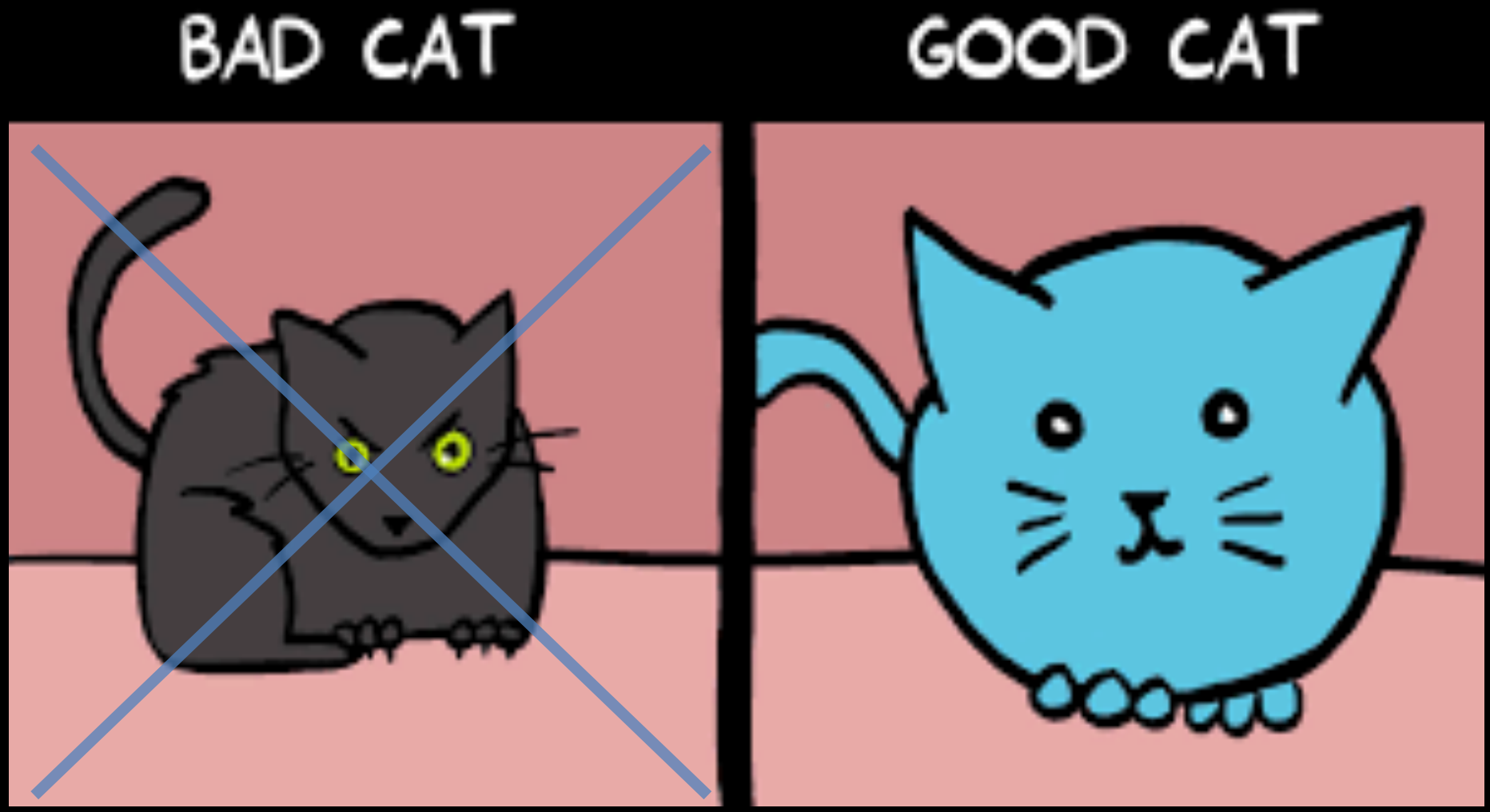
Security attacks that small businesses need to worry about

April C. Wright

ArchitectSecurity.org


problemsolver
applications
knowledge
automation
complex
assessment
riskmanagement
consistent
certified
innovative
information
blueteam
preventative
leadership
evangelist
remediation
projects
creativity
assurance
defense
proactive
architecture
design
platforms
development
infosec
networks
initiatives
manager
frameworks
systems
evaluator
technical
lifecycle
safeguards
hybrid
senior
ITIL
expert
impact
security
analyst
redteam
GRC
cloud
guidance
unix
cyberz
global
author
web
enterprise
largescale
programs
shell
auditor
federal
solutions
speaker
cats
awareness
customers
planning
database
integration
operations
industry
experience
datacenter
diplomat
generalist
compliance

1. Certified Master's Level Social Engineer
2. CISSP (Certified Information Systems Security Professional)
3. CSSLP (Certified Secure Software Lifecycle Professional)
4. CCSP (Certified Cloud Security Professional)
5. SSCP (Systems Security Certified Practitioner)
6. CISA (Certified Information Systems Auditor)
7. CCSK (Certificate of Cloud Security Knowledge)
8. ITIL version 3 Fundamentals
9. QualysGuard Certified Specialist
10. Vulnerability Management - Qualys
11. FedRAMP System Security Plan (SSP) 200-A
12. Oracle Certified Security Administrator
13. Oracle Certified Network Administrator
14. Oracle Certified Systems Administrator
15. CompTIA Network+
16. CompTIA Security+
17. Infra CMDB Certified Developer – EMC
18. Microsoft Certified Professional (MCP)



@aprilwright

e-mail

In 2017, 66% of malware was installed via malicious email attachments

61% of data breach victims in 2017 were companies with less than 1000 employees

Social attacks are the vector utilized in 43% of all breaches

28% of phishing breaches were *targeted* at specific individuals

You cannot buy a product to protect your business against social and physical attacks

Awareness is your primary defense

Wi-Fi

SSID Pool

Refresh

GuestWiFi
The Network
acme-guest
Concourse-B
Free WiFi
University Open
acme-floor3
Tenant 201
default
FreeWifi
mobileAP
wireless
cablewifi
Home
no_ssid

Hak5 WiFi Pineapple

Configuration

- [x] Allow Associations
- [x] Log Probes
- [x] Log Associations

PineAP Daemon: Enabled | Switch

- [x] Capture SSIDs to Pool
- [x] Beacon Response
- [x] Broadcast SSID Pool

Beacon Response Interval: Normal

Broadcast SSID Pool Interval: Normal

Source MAC: 00:C0:CA:8B:3A:XX

Target MAC: FF:FF:FF:FF:FF:FF

Save PineAP Settings

DWall Settings

DWall is currently running.

Disable | Stop Listening

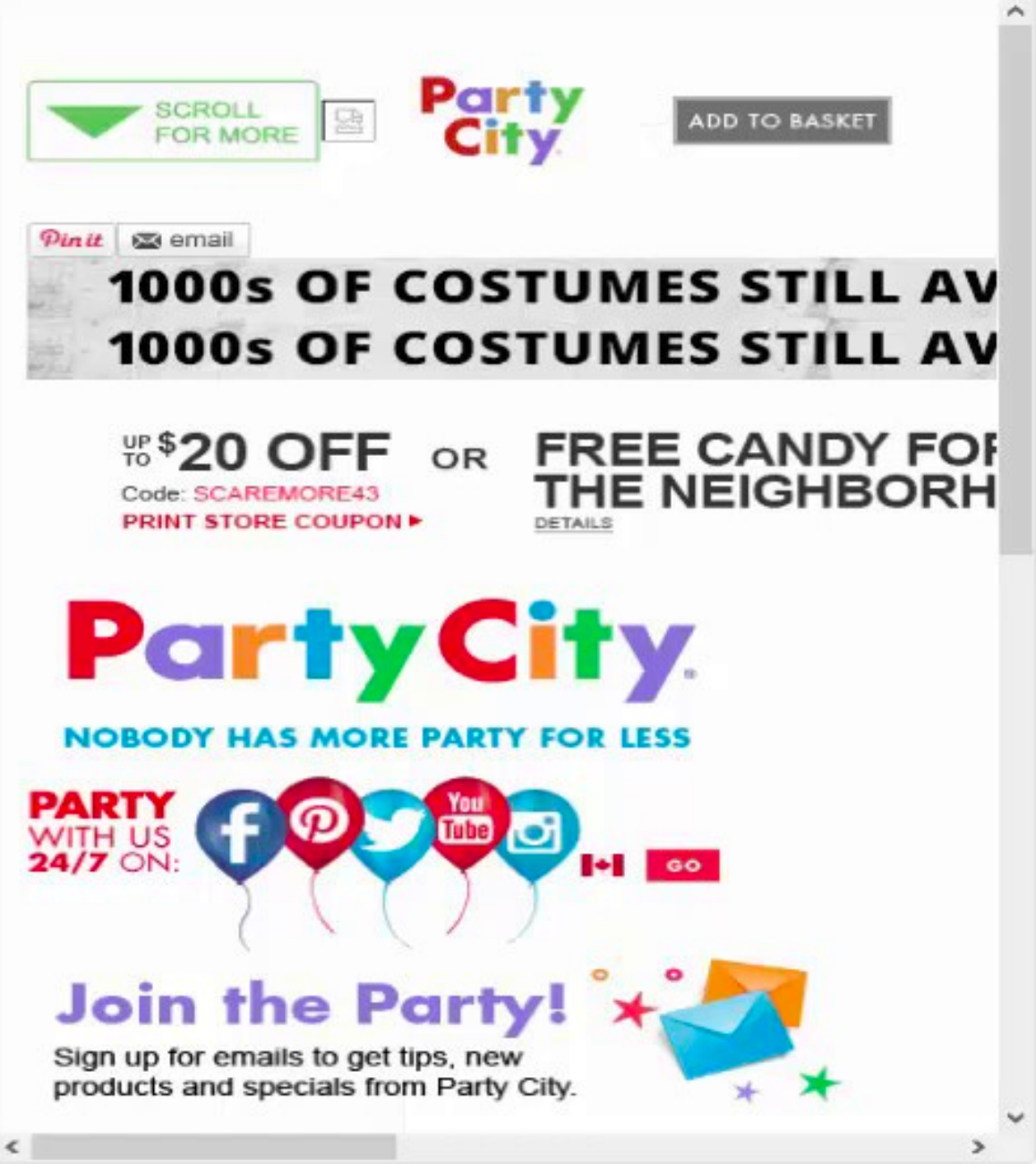
URLs

Client	URL
172.16.42.179	http://w88.go.com/b/ss/wdgdsec,wdgdoldhom/1/H.25.. t=29%2F9%2F2016%2013%3A36%3A12%206%202 a624-4811-aded-bf0b0da3bb41&c12=dcom%7Cdhor v40=dcom%7Cdhome%7Chomepage%7Chomepage c62=www.disney.com&v62=www.disney.com&c63=www v73=5946c0b2-a624-4811-aded-bf0b0da3bb41&c74 bh=704&AQE=1
172.16.42.179	http://ctologger01.analytics.go.com/cto/?app=w88_dc lSessId=1477762531046-8908025050695&lVisId=14 fullPgNm=dcom%7Cdhome%7Chomepage%7Chome cod=32&adPgNm=/7046/dcom-mobile/homepage&ad

Cookies

Client	Cookie
172.16.42.179	carousel_firstIndex=155%3B%3BP687272%3B%3B2' JSESSIONID=F14143A5796DB9BD4CE453F756FFB customer=none, basket=none, EMAIL_PAGE_CNT=1 dtm_token=AQEG9CKLNLnmlgFR-MDTAQElHwE; __ __utmz=5991724.1477762554.1.1.utmcsr=(direct)|ut __utmb=5991724.1.10.1477762554;

Images



USB Thumbdrives

“Staff secretly dropped computer discs and USB thumb drives in the parking lots of government buildings and private contractors. Of those who picked them up, 60 percent plugged the devices into office computers, curious to see what they contained. If the drive or CD case had an official logo, 90 percent were installed.

“There’s no device known to mankind that will prevent people from being idiots,” said Mark Rasch, director of network security and privacy consulting for Falls Church, Virginia-based Computer Sciences Corp. (CSC)

https://www.wired.com/2011/06/the-dropped-drive-hack/


confidential
upcoming
layoffs
employee
bonuses

Why is USB So Dangerous?

USB RUBBER DUCKY

$44.99

The USB Rubber Ducky is a keystroke injection tool disguised as a generic flash drive. Computers recognize it as a regular keyboard and accept pre-programmed keystroke payloads at over 1000 words per minute.

Payloads are crafted using a simple scripting language and can be used to drop reverse shells, inject binaries, brute force pin codes, and many other automated functions for the penetration tester and systems administrator.

Since 2010 the USB Rubber Ducky has been a favorite among hackers, penetration testers and IT professionals. With origins as the first IT automation HID using an embedded dev-board, it has since grown into a full fledged commercial Keystroke Injection Attack Platform. The USB Rubber Ducky captured the imagination of hackers with its simple scripting language, formidable hardware, and covert design.

Quantity

1

ADD TO CART

https://hakshop.com/products/usb-rubber-ducky-deluxe

EMULATE COMBINATIONS OF TRUST DEVICES.
CARRY MULTIPLE PAYLOADS.

CHOOSE ATTACKS WITH THE FLICK OF A SWITCH.

It opens up attack surfaces that weren't possible before in one single device. Penetration testing attacks and IT automation tasks are all delivered in seconds with the Bash Bunny. By emulating combinations of trusted USB devices — like gigabit Ethernet, serial, flash storage and keyboards – computers are tricked into divulging data, exfiltrating documents, installing backdoors and many more exploits.

It features a simple scripting language that you can write in any text editor like notepad. The growing collection of payloads are hosted in a single library – so finding the right attack is quick and easy. Setting up Bash Bunny attacks is just a matter of flicking its switch to arming mode and copying a payload file. It's the same as you would for an ordinary flash drive — it's literally that convenient.

Carrying multiple payloads and getting feedback on each attacks is effortless. Slide the switch to your payload of choice, plug the Bash Bunny into the victim computer and watch the multi-color LED. With a quad-core CPU and desktop-class SSD it goes from plug to pwn in 7 seconds.

Plus, the Bash Bunny is a full featured Linux box with shell access from a dedicated serial console – so all of the pentesting tools you've come to know and love are just keystrokes away.

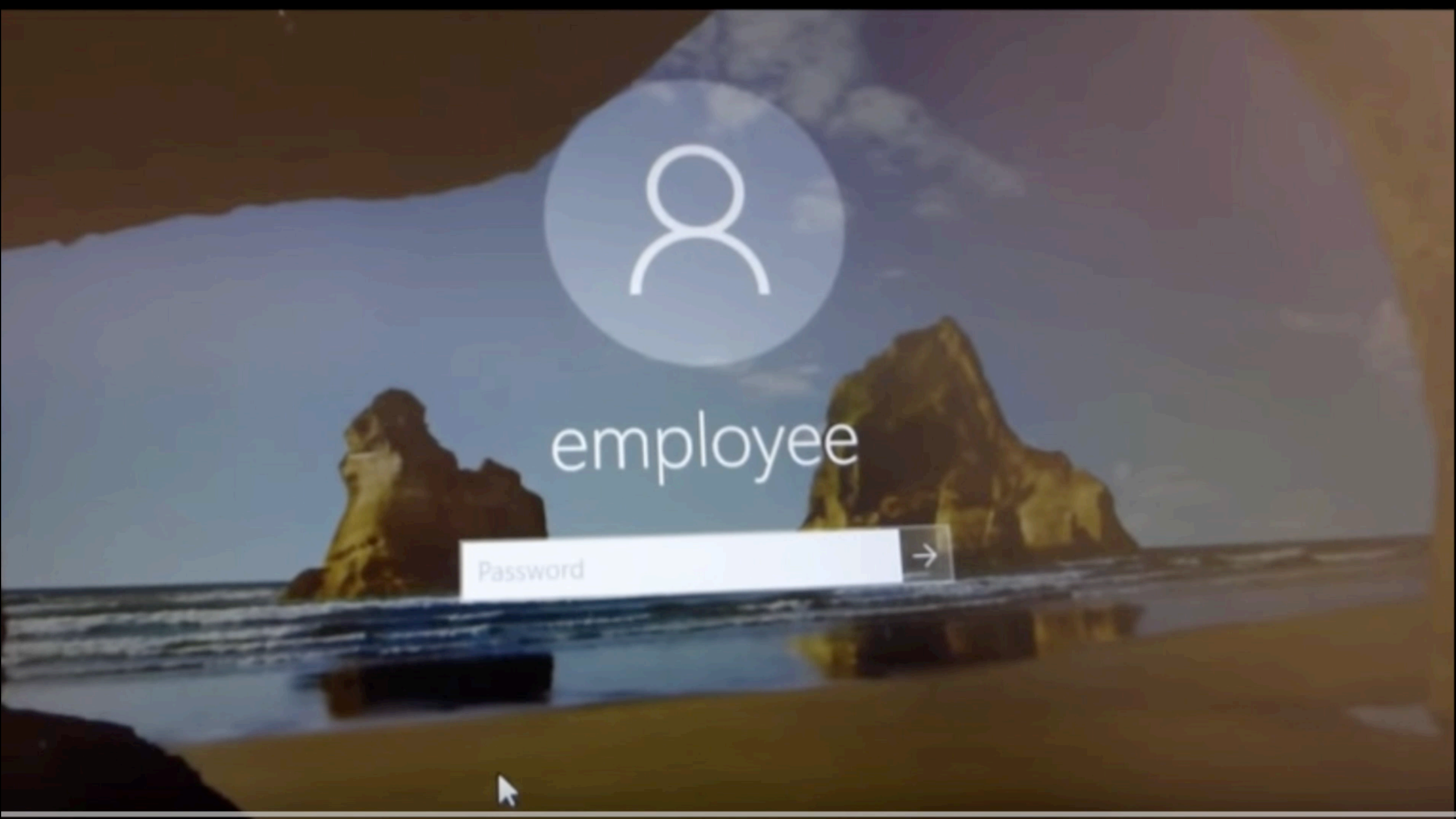
Branch: master ▾ bashbunny-payloads / payloads / library /

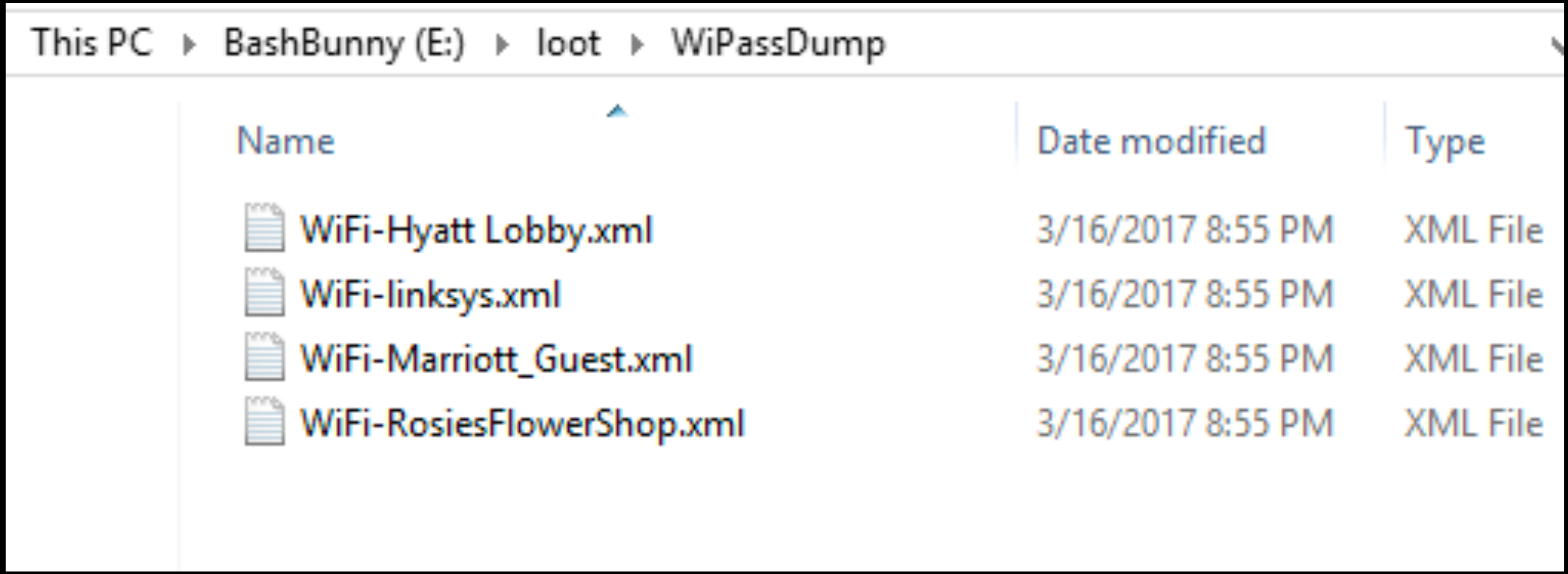
Create new file | Find file | History

Thorsten-Sick committed with sebkinne Added "Info Grabber for Linux" payload (#299) — Latest commit fae8746 3 days ago

..

Incident_Response	Update and fix payloads (#277)	2 months ago
android	Update and fix payloads (#277)	2 months ago
credentials	Added "Bushings blue turtle" payload (#263)	19 days ago
execution	Add RevShellBack payload (#265)	2 months ago
exfiltration	Added SmartFileExtract payload (#296)	14 days ago
exploitation/Metasploit-Autopwn	Metasploit Autopwn Bash Bunny Payload (#242)	3 months ago
general	Add BlueTeamPCAudit payload (#261)	18 days ago
phishing	Update and fix payloads (#277)	2 months ago
prank	Violation of CoC (#294)	20 days ago
recon	Added "Info Grabber for Linux" payload (#299)	3 days ago
remote_access	Updated "Linux Reverse Shell" to v1.2 (#262)	19 days ago
sFTP Directory Grabber	Update and fix payloads (#277)	2 months ago


employee
Password



https://www.blackhillsinfosec.com/pull-wireless-credentials-bash-bunny/

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>linksys</name>
        <SSIDConfig>
                <SSID>
                        <hex>6C696E6B737973</hex>
                        <name>linksys</name>
                </SSID>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPAPSK</authentication>
                                <encryption>AES</encryption>
                                <useOneX>false</useOneX>
                        </authEncryption>
                        <sharedKey>
                                <keyType>passPhrase</keyType>
                                <protected>false</protected>
                                <keyMaterial>verylongandboringpassword</keyMaterial>
                        </sharedKey>
                </security>
        </MSM>
</WLANProfile>
```

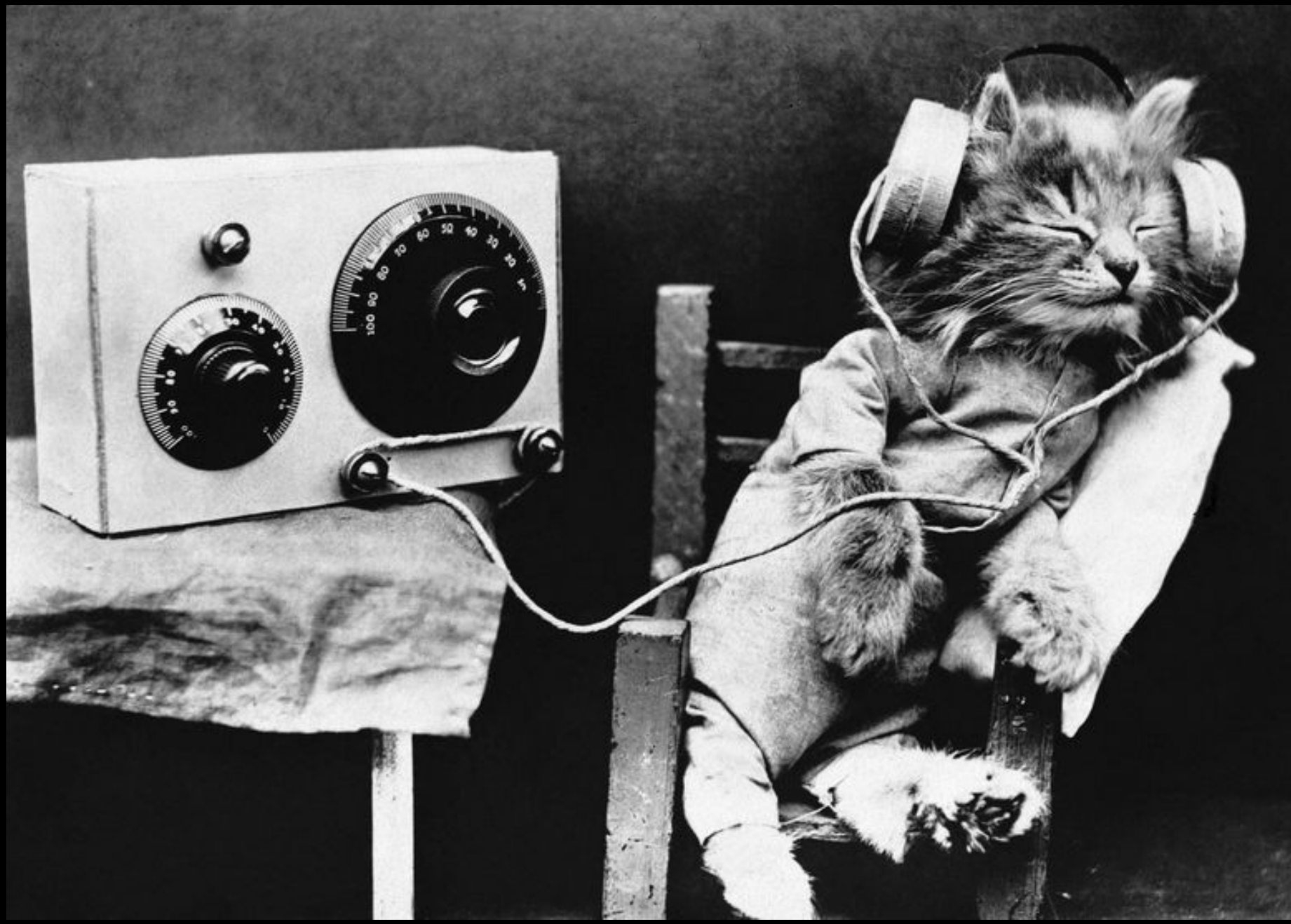
SSID

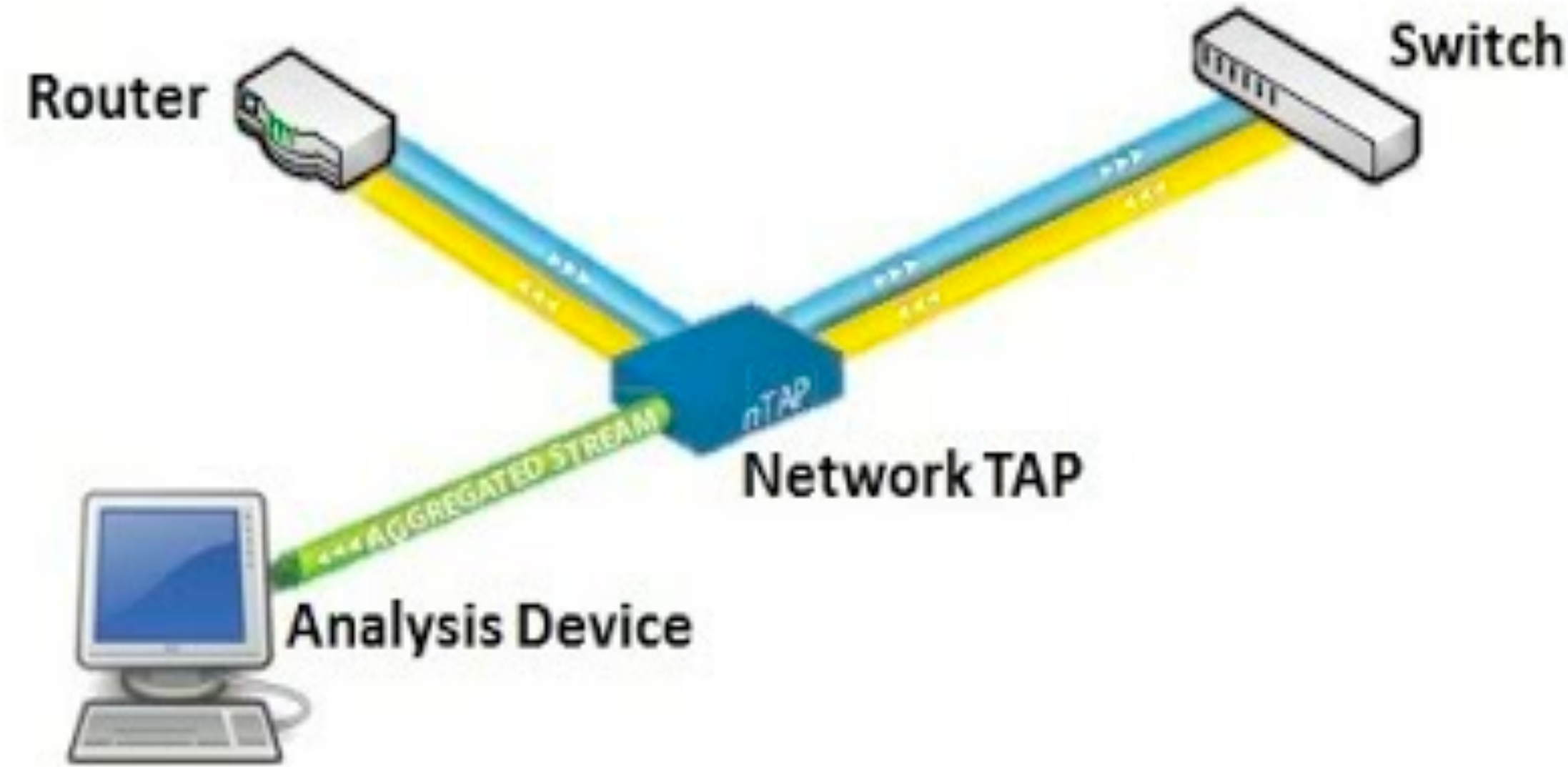
Encryption Algorithm

Passphrase

https://www.blackhillsinfosec.com/pull-wireless-credentials-bash-bunny/

Network Taps




Router
Switch
nTAP
Network TAP
AGGREGATED STREAM
Analysis Device

THROWING STAR LAN TAP

$14.99

The Throwing Star LAN Tap is a passive Ethernet tap, requiring no power for operation. There are active methods of tapping Ethernet connections (e.g., a mirror port on a switch), but none can beat passive taps for portability. To the target network, the Throwing Star LAN Tap looks just like a section of cable, but the wires in the cable extend to the monitoring ports in addition to connecting one target port to the other.

The monitoring ports (J3 and J4) are receive-only; they connect to the receive data lines on the monitoring station but do not connect to the station's transmit lines. This makes it impossible for the monitoring station to accidentally transmit data packets onto the target network.

Quantity

1

ADD TO CART

https://www.amazon.com/Throwing-Star-LAN-Tap-communications/dp/B01N3POABX

LAN TURTLE

LAN Turtle

$249.99

DROP A LAN TURTLE. GET A SHELL.

The LAN Turtle is a covert Systems Administration and Penetration Testing tool providing stealth remote access, network intelligence gathering, and man-in-the-middle surveillance capabilities through a simple graphic shell.

Housed within a generic "USB Ethernet Adapter" case, the LAN Turtle's covert appearance allows it to blend into many IT environments.

Title

LAN TURTLE CLASSIC | LAN TURTLE SD | LAN TURTLE 3G

Quantity

1

ADD TO CART

https://hakshop.com/products/lan-turtle?variant=429651787785

https://www.hak5.org/wp-content/uploads/2017/10/banner2.jpg

Hidden Cameras & Other Cloak and Dagger Devices

LOCK PICKS

Pen Pick Set

$40

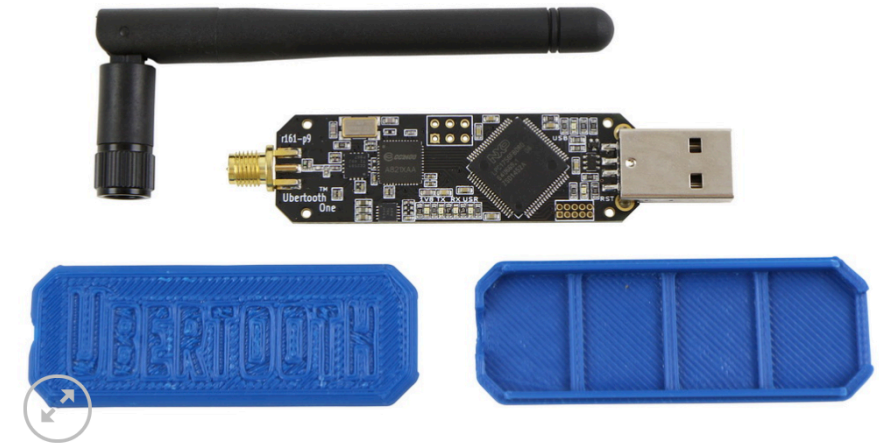
- 1 +

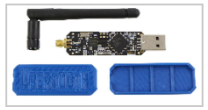
ADD TO CART

SKU: LP-D212

Category: Lock Picks

Tag: Penetration Testing





NETWORKING / WIRELESS NETWORKING

Ubertooth One Kit

$135

- 1 + ADD TO CART

SKU: GSG-U1-C

Category: Wireless Networking

Tags: Bluetooth, Debugging, Penetration Testing

DESCRIPTION

The Ubertooth One is an open source 2.4 GHz wireless development platform suitable for Bluetooth experimentation. Commercial Bluetooth monitoring equipment can easily be priced at over $10,000 , so the Ubertooth was designed to be an affordable alternative platform for monitoring and development of new BT, BLE, similar and wireless technologies.

The Ubertooth One was created by Mike Ossmann at Great Scott Gadgets in 2011 when he realized that there was not an off-the-shelf BT adapter that offered the capabilities he required. A great video from his talk at ShmooCon 2011 tells the whole story and can be found on YouTube. The Ubertooth One is open source hardware designed in KiCad, and all the hardware specs, design files, and additional information can be found at the GitHub Repo

The device is designed primarily as an advanced Bluetooth receiver, offering capabilities beyond that of traditional adapters, which allow for it to be used as a BT signal sniffing and monitoring platform. Although the device hardware will accommodate signal broadcasting, the firmware currently only supports receiving and minimal advertising channel transmission features.

Coffee Cup Travel Mug Hidden Camera

Pretend to drink while the hidden camera in the middle records everything in stunning 1080p video. Our most popular portable spycam!

Zoom the image with the mouse

PRODUCT HIGHLIGHTS:

- Stunning 1920x1080p HD Video
- Crisp 2560x1920 Photos
- Motion Activated Recording
- 32 Hours Continuous Recording
- Loop Recording
- Rechargeable 8 Hour Battery
- Time/Date Stamp
- Fill With Actual Liquid
- Record Hours Of Video
- 1 Minute Post Recording
- Works w/ PC or Mac
- Super Quick & Easy On / Off
- Lifetime Warranty
- Lifetime Support

(No reviews yet) | Write a Review

SKU: MG-OmniCoffeeLid

Retail Price: ~~$439.00~~

Sale Price: $370.00

(You save $144.00)

In Stock

Free Shipping

SELECT AVAILABLE OPTIONS:

Memory Upgrade:

64 MB Memory Upgrade (+75)

Audio Upgrade | Police, Gov't & Outside USA Only:

No Audio

Quantity:

1

ADD TO CART

Add to Wish list

LawMate 720P CMOS HD Button Color Camera Kit

HD LawMate Button Camera Kit. Works with all our DVR's. It's covert design gives you the ability to record anywhere while wearing the button like camera.

(No reviews

$399.00

SELECT AVAILABLE

Quantity:

1

Lawmate Power Bank Hidden Camera w/ Wi-Fi Remote Viewing

Charge your gadgets and record hidden video while watching remotely simultaneously on your smartphone or tablet. Long lasting battery lets you live stream virtu
in seconds.

PRODUCT HIGHLIGHTS:

- Stunning 1080p HD Video
- HD Snap Shot Photos
- 2MP Camera
- Wi-Fi Remote Viewing
- Free Phone / Tablet App
- Motion Activated Recording
- 16 Hours Recording Time
- 6 Hour Battery While Recording
- 8 GB Included
- Loop Overwrite Recording
- Time/Date Stamp
- 6800mA Lithium Battery
- Works w/ PC or Mac
- Lawmate PV-PB20I
- 1 Year Warranty
- Lifetime Support

(No reviev

Retail Price:
~~$399.00~~

(You save $50.00)

SELECT AVAILABI

SD Card Storage:

SD Card Storage (8GB I

Add Audio + 3-Day Cu

No Audio

Quantity:

1

UltraMax 2K Video Spy Pen Hidden Camera

Covertly record up hours of STUNNING 2k quality video from this spy pen with a simple one-button control. You'll enjoy easy-to-use operation from an actual functioning pen that discreetly captures crisp, impressive footage.

PRODUCT HIGHLIGHTS:

- Sharp, Crisp 2k HD Video + Audio
- 4352 x 3264 Snapshots
- 30FPS Recording Rate
- Capture Hours Of Footage
- Continuous or Motion Activated
- Time & Date Stamp
- 60 Minute Battery Life
- Actual Functioning Pen
- Easy, One-Touch Recording

★★★★★ (3 reviews) | Write a Revie

~~$250.00~~ $169.00

(You save $81.00)

SELECT AVAILABLE OPTIONS:

Quantity:

1

Water Bottle Hidden Spy Camera w/ Motion Detection

You can fill it with real water to drink while the hidden camera in the middle records everything. Our most popular portable spycam!

Zoom the image with the mouse

PRODUCT HIGHLIGHTS:

- Stunning 1920x1080p HD Video
- Motion Activated Recording
- Continuous Recording
- Time/Date Stamp
- Fill With Actual Water
- Record Hours Of Video
- 1 Minute Post Recording
- Works w/ PC or Mac
- Rechargeable 8 Hour Battery
- Super Quick & Easy On / Off
- 1 Year Warranty

(No revi

Retail Price:
~~$499.00~~

(You save $150.00)

SELECT AVAILAI

Memory Upgrade:

16 MB Memory Includ

Audio Upgrade | Pol

No Audio

Quantity:

1

Mini USB Charger 1080P HD Hidden Camera w/ Motion Activated Recording

Simply plug & spy! This real functioning wall plug will charge your gadgets while recording hours of HD video on a continuous loop. By far the smallest HD spy camera ever made that works with both PC or Mac

PRODUCT HIGHLIGHTS:

- Stunning 1920x1080p HD Video
- Plug & Play
- 32 GB Built-In Memory
- Motion Activated Recording
- AC Powered
- Functional Charger
- Loop Recording
- Time/Date Stamp
- Works w/ PC or Mac
- Lifetime Warranty
- Lifetime Support

(1 review) | Write a Review

SKU: MG-HCMiniCharge-Black

~~$239.00~~ **$148.98**

(You save $90.02)

In Stock

Free Shipping

SELECT AVAILABLE OPTIONS:

Quantity:

1

ADD TO CART

Add to Wish list

Keychain Car Remote Hidden Camera

Keep an eye on your family with this inconspicuous device that records motion activated HD video

Zoom the image with the mouse

(No

~~$250.00~~

(You save $71.00)

SELECT AVAIL

Quantity:

1

Physical & Social Attacks


HID
ProxCard® II

Merry Auzmas 🎄
@Auzranium

Follow

Well it is official...I now work at the hospital!!! There is my ID Badge with my real face. I know it is volunteer but it is like a job.

7:19 PM - 13 Sep 2017 from Vermont, USA

1 Retweet **4** Likes


Ryan

Where to Focus

Train users about phishing with an education plan that:

- Empowers users to alert on “phishy” emails
- Teaches users how to spot a phishy email
- Teaches users where to report phishy emails

Implement and test a phishing "response plan" that:

- Identifies recipients who clicked links or opened a file
- Changes credentials on compromised hosts
- Investigates post-click communications from infected hosts
- Isolates a system so that the malware cannot spread
- Identifies and removes the malware
- Considers the use of sandboxing technologies that separate the mail client application from the host OS

Phishing

- Prepend *external* email subjects with **[External]** or **[E]** in the subject header to help users detect spoofed messages purporting to be coming from a someone internal
- Have a process for approving payments that includes some form of communication *other than* email
- Train the employees who are able to approve money transfers that they will never ever be asked over email to transfer funds outside of the documented approval policy
- Work with your banking institution to block and alert on large or anomalous transfers of funds

Wi-Fi

- Use a VPN when connected to ANY Wi-Fi network
- Turn off VPN on your devices when you're not using it
- Delete previously connected Wi-Fi from your "known networks" when you don't need it anymore
  - When you go to a hotel, "Forget Network and remove the hotel's Wi-Fi when you aren't staying there - it's easy to re-add
- Don't use WPA/2-PSK on corporate networks

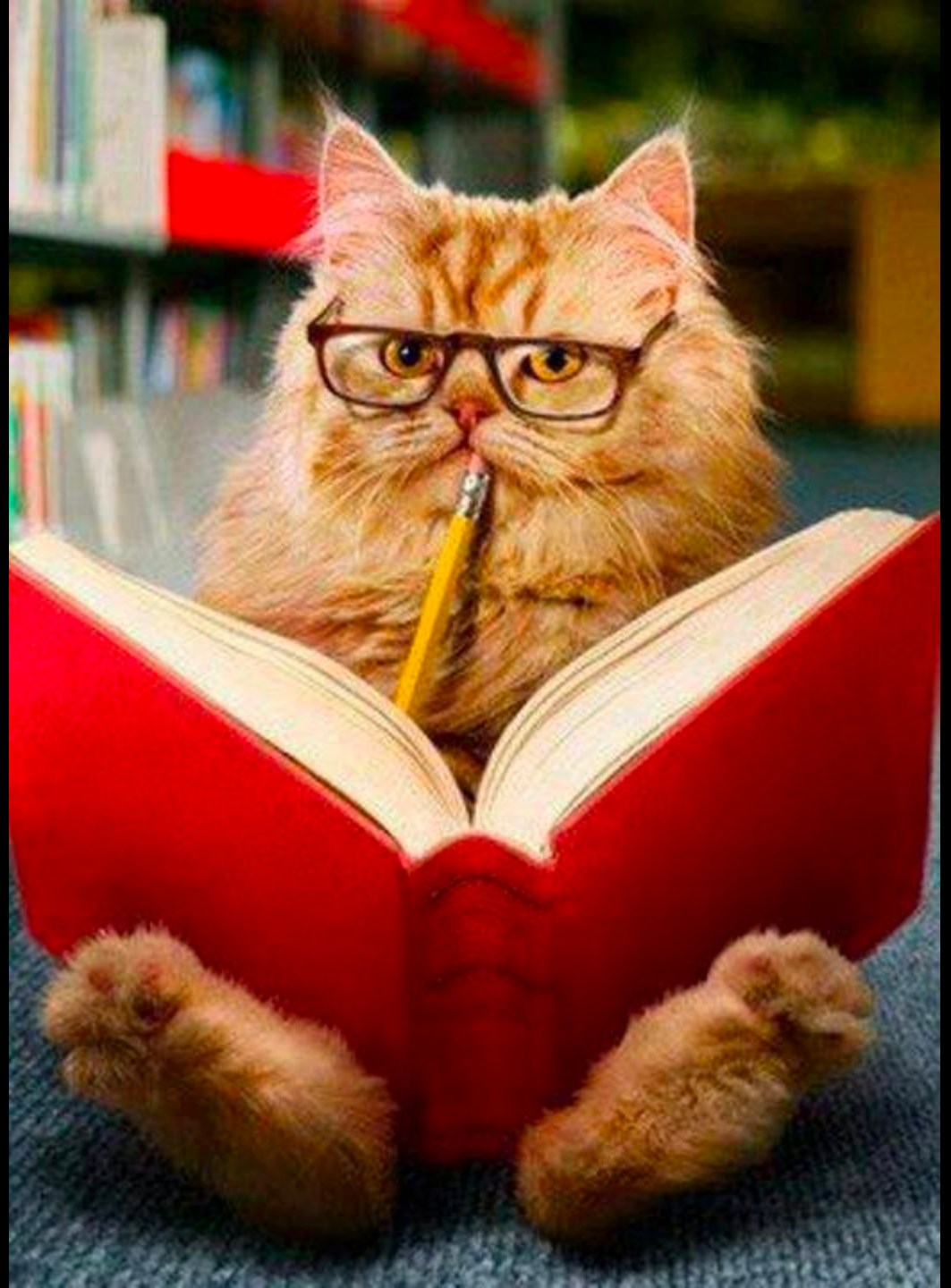
USB

- Don’t leave workstations unlocked / unattended
- Use full disk encryption
- Disable USB access on company-owned computers or limit to specific, known devices
- Don’t allow anyone to touch your computers
- Never insert media you receive in snail mail
- Don’t post photos of your badge on social media

Physical Attacks

- Question anyone you don't recognize
- Validate credentials
  - Verify via known pathways, not via a number they give you
- Social attacks often come from people in uniforms
  - Uniforms make us assume something about someone
  - Uniforms can be a suit and tie or a jumpsuit or a hard hat.
  - Just because someone is carrying a ladder does not mean they are authorized to be there.
  - Don't trust anyone! - Delivery people, New Hires, Auditors, Inspectors, Technicians, HVAC, Repair people, Cleaning crew, …even customers/potential customers!

Putting It All Together



Segula Camera Pen

Product Code: EL733

DESCRIPTION | RETURNS & REFUNDS | DELIVERY INFORMATION

Segula Pen Camera. An elegant ballpoint pen with a hidden accessory... a minicamera with a micr record up to three hours of video footage, with sound, within 15 square metres. This multi-purpo dictation machine. Please be aware of local photography restrictions in certain destinations.

Timewerk HD Night-vision Video Camera Watch

Product Code: EL698

Your Price

£99

Quantity

1

ADD TO SHOPPING BAG

Share This Product

DESCRIPTION | RETURNS & REFUNDS | DELIVERY INFORMATION

This watch with HD video, camera and microphone allows you to shoot videos – even at night – take photos or make audio recordings then download them via USB cable. It also features a titanium carbide-plated, stainless steel case and leather strap. Please be aware of local photography restrictions in certain international destinations. Two-year warranty

Please observe local laws and restrictions on usage in sensitive public areas.


WARNING:
May contain Dormant Cyber Pathogens
Packet Squirrel
TX
AP
upcoming layoffs
This is my burner $device
HACK THE PLANET
adafruit
SONY
WarSoller

Takeaways

- **Humans Must Be vigilant** - Log files and change management systems can give you early warning of a breach.
- **Make people your first line of defense** - Train staff to spot the warning signs. Only keep data on a "need to know" basis and only grant minimal required access to systems
- **Patch promptly** - This could guard against many attacks
- **Encrypt sensitive data** - Make your data next to useless if it is stolen
- **Use two-factor authentication** - This can limit the damage that can be done with lost or stolen credentials
- **Don't forget physical security** - Not all data theft happens online.

2017 Verizon Data Breach Investigations Report (DBIR)

https://verizonenterprise.com/verizon-insights-lab/dbir/2017/

“The freedom to connect to the world anywhere at anytime brings with it the threat of unscrupulous predators and criminals who mask their activities with the anonymity the Internet provides to its users”

-- Mike Fitzpatrick

April C. Wright

ArchitectSecurity.org

@aprilwright